Как цитировать: Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 316 с. EDN: XVINGO. DOI: http://dx.doi.org/10.21202/978-5-8399-0815-4_2_316

For citation: Digital Technologies and Law: collection of scientific articles of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 2. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 316 p. EDN: XVINGO. DOI: http://dx.doi.org/10.21202/978-5-8399-0815-4_2_316

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 2

Казань ■ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2023

DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22
Kazan

In 6 volumes
Volume 2

Kazan ■ KIU "POZNANIYE" PUBLISHERS ■ 2023

УДК 004:34(063)
ББК 67с51я43
Ц75

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

Ц75 **Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции** (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 316 с. EDN: XVINGO. DOI: http://dx.doi.org/10.21202/978-5-8399-0815-4_316.
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0815-4 (Том 2)

Вошедшие в сборник научные труды приурочены к II Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 22 сентября в Казани в рамках Международного форума Kazan Digital Week 2023, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

Широкий круг рассмотренных на конференции теоретико-методологических и практико-ориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, нормативным регулированием цифровой среды, перспективами правового воздействия на формирующиеся и новые общественные отношения, когнитивно-поведенческие паттерны в условиях цифровизации и алгоритмизации социального программирования, автоматизированного принятия правовых решений операционно-интеллектуальными системами, доминирования цифровых платформ на цифровом рынке, технологических инноваций и многим другим.

Научные труды представленного тома систематизированы по современным трендам развития цифровых технологий в системе уголовно-правовых отношений.

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 достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0815-4 (Том 2)

UDC 004:34(063)
LBC 67c51я43

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

Digital Technologies and Law: collection of scientific papers of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 2. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 316 p. EDN: XVINGO. DOI: http://dx.doi.org/10.21202/978-5-8399-0815-4_316
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0815-4 (Vol. 2)

The scientific works included in the collection are timed to coincide with the II International Scientific and Practical Conference "Digital Technologies and Law", held on September 22 in Kazan as part of the International Forum "Kazan Digital Week 2023", organized by the Government of the Russian Federation jointly with the Cabinet of Ministers of the Republic of Tatarstan.

A wide range of theoretical, methodological and practice-oriented, interdisciplinary and sectoral issues discussed at the conference are related to the priorities of the legal development of digital technologies, regulatory regulation of the digital environment, prospects for legal influence on emerging and new social relations, cognitive-behavioral patterns in the context of digitalization and algorithmization of social programming, automated legal decision-making by operational-intelligent systems, the dominance of digital platforms in the digital market, technological innovation and much more.

The scientific works of the presented volume are systematized according to modern trends in the development of digital technologies in the system of criminal legal relations.

The ideas and proposals reflected in the multi-volume publication in their entirety are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies, practicing lawyers, representatives of law-making and law enforcement bodies, government officials and participants in the real sector of the economy, including developers and manufacturers of products of digital technology achievements, young student researchers, undergraduates and graduate students, everyone interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0815-4 (Vol. 2)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ

DIGITAL TECHNOLOGIES IN THE SYSTEM CRIMINAL LEGAL RELATIONS

А. А. Антонов,
преподаватель,
Финансовый университет при Правительстве Российской Федерации
(Владикавказский филиал),
адвокат,
Адвокатская палата Республики Северная Осетия – Алания

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ РЕСОЦИАЛИЗАЦИИ ЛИЧНОСТИ ПОСРЕДСТВОМ ОБРАЗОВАНИЯ В СИСТЕМЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ИСПОЛНЕНИЯ НАКАЗАНИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассматривается проблема ресоциализации личности в условиях становления искусственного интеллекта в системе образования Федеральной службы исполнения наказаний Российской Федерации в форме персонализации обучения и обучения навыкам. В социальных сетях искусственный интеллект создает определенные группы по интересам, в том числе и деструктивные, в которых управляет процессом персонализации и обеспечивает наивысшую эффективность манипулирования человеком в современном мире. Рассмотрено понятие «искусственный интеллект», а также его основные характеристики. Развитие искусственного интеллекта в образовательной среде требует подготовку преподавателей, обладающих знаниями в сфере новых технологий, в том числе с привлечением содержащихся в местах лишения свободы осужденных – специалистов. Показано особенности и примеры внедрения технологий искусственного интеллекта в современную систему образования ФСИН. Перечислены проблемы и перспективы применения искусственного интеллекта в местах лишения свободы.

Ключевые слова: новые технологии, цифровые устройства, ресоциализация, искусственный интеллект, система образования, персонализация обучения, обучение навыкам

ARTIFICIAL INTELLIGENCE AS A TOOL FOR RESOCIALIZATION OF PERSONALITY THROUGH EDUCATION IN THE SYSTEM OF THE FEDERAL PENALTY SERVICE OF THE RUSSIAN FEDERATION

Abstract. The article deals with the problem of personality resocialization in the conditions of the formation of artificial intelligence in the education system of the Federal Penitentiary Service of Russia in the form of personalization of education

and skills training. In social networks, artificial intelligence creates certain interest groups, including destructive ones, in which it manages the personalization process and ensures the highest efficiency of human manipulation in the modern world. The article discusses the concept of «artificial intelligence», as well as its main characteristics. The development of artificial intelligence in the educational environment requires the training of teachers with knowledge in the field of new technologies, including with the involvement of convicted specialists in places of deprivation of liberty. The author showed the features and examples of the introduction of artificial intelligence technologies into the modern education system of the Federal Penitentiary Service. The problems and prospects of using artificial intelligence in places of detention are listed.

Keywords: skills training, digital devices, resocialization, artificial intelligence, education system, personalization of learning

Ресоциализация осужденных наряду с их исправлением является основной целью функционирования пенитенциарной системы. В Российской Федерации вопросом подготовки к ресоциализации осужденных исправительные учреждения занимаются с момента попадания заключенного в места лишения свободы, наиболее оптимизируя реабилитацию за полгода до освобождения. В российской пенитенциарной системе приняты социально-медицинская, социально-психологическая, социально-экономическая и социально-педагогическая виды реабилитации лиц, осужденных к отбыванию наказания в местах лишения свободы [5].

Ресоциализация осужденных в местах лишения свободы включает обширную программу социальных норм и культурных ценностей, предусмотренных для лиц, не овладевших или слабо овладевших прежде, направленных на развитие новых концепций общественного развития. Ресоциализация – это реабилитация не освоенных ранее социальных норм, с помощью которого зрелая личность обновляет прежние отношения или развивает новые.

Социально-экономическая и социально-педагогическая реабилитации тесно связаны и предполагают право и обязанность осужденного не только осуществлять трудовую деятельность на производстве исправительного учреждения, но и улучшать профессиональные компетенции, получать профессию.

В настоящее время в нашей стране активно развивается тенденция непрерывного образования, дающего человеку больше возможностей для смены видов трудовой деятельности, достижения высоких карьерных результатов и обеспечения достойного уровня жизни.

Предоставить возможность получить образование и профессию при ее отсутствии на момент осуждения или получить новую профессию в процессе отбывания наказания упрощает понимание дальнейшей трудовой деятельности осужденных.

Современная пенитенциарная система стремительно развивается и претерпевает ряд изменений. В Уголовно-исполнительном кодексе Российской Федерации от 08.01.1997 № 1-ФЗ установлена обязательность получения общего образования для осужденных, не достигших возраста 30 лет [3].

Направление получаемых профессий соответствует специфике видов производства, функционирующих в колониях. После освобождения бывший осужденный имеет возможность выйти в социум с прикладной специальностью.

Однако, имея ввиду важность практически применимой, востребованной специальности для освобождающихся из мест лишения свободы, стоить отметить, насколько в 2020–2023 гг. все более популяризуются специальности, обусловленные внедрением искусственного интеллекта. Работа с использованием «достижений прогресса» позволяет россиянам работать дистанционно, самостоятельно реализовывать собственные проекты.

Стремительное развитие инновационных технологий расширяет сферы деятельности искусственного интеллекта, что требует определения его правового статуса в общественных отношениях.

В настоящее время никого не удивляют технологические изменения, происходящие в развитых странах и бурными темпами применяющих искусственный интеллект роботов, беспилотный транспорт, цифровые устройства в различных сферах деятельности.

Необходимость в повторной социализации может возникать вследствие длительного нахождения в исправительных учреждениях и кардинального изменения окружающей действительности. Ресоциализация личности, требующей введения образовательного процесса, включает в себя обучение цифровым навыкам учащегося. Процесс базируется на создании индивидуальных программ, предусматривающих основные подходы в применении искусственного интеллекта.

Искусственный интеллект создан человеком как интеллектуальный разум, обладающий глобальными возможностями в различных сферах науки и техники. Под ними подразумевают сложные программы, предоставляющие возможность автономно решать сложные вопросы.

Внедрение искусственного интеллекта в образовательную систему Федеральной службы исполнения наказаний (далее – ФСИН) через социальные сети позволит увеличить компетенции в формировании личности, прежде всего воспитания осужденных, которые благодаря искусственному интеллекту, смогут реализовать себя в творческой сфере.

Практика искусственного интеллекта в местах лишения свободы – это так называемое навыковое обучение, т. е. овладение социальными, когнитивными и эмоциональными навыками. Это предполагает переход к проектной деятельности, а потом овладение цифровыми навыками: конструирование продуктов, цифровой архитектуры, «общение» с искусственным интеллектом.

Данным навыкам будут обучать машина, робот – они обеспечат массовое обучение. В этом сила искусственного интеллекта, который позволит обучаемому получить быстрый и свободный доступ к любым данным, к любой нужной информации и как поводырь подведет к нужному решению. Но знание как признак избранности, как признак индивидуального таланта будет заменено практическими навыками, на которые будет исключительный спрос.

Практика использования искусственного интеллекта в учреждениях пенитенциарной системы показывает, что искусственный интеллект может быть репетитором, автоматизировать оценку знаний, анализировать поведение обучающихся. Главным контролером образовательного процесса будет искусственный интеллект [2. С. 194].

Процесс обучения социальным, мыслительным и эмоциональным навыкам требует полного раскрытия обучающимся своего творческого потенциала, способ-

ности конструктивно мыслить и решать сложные задачи. Но без основного звена образовательного процесса преподавателя, обладающего профессиональными качествами, и использования знаний обучаемого с применением технологий искусственного интеллекта достижение желаемого результата невозможно. Без специалиста в данной сфере приобретаемые обучающимися знания не смогут конструктивно применяться, и учащиеся будут напоминать роботов, которые не способны самостоятельно мыслить. Опытный преподаватель, пользующийся авторитетом и знающий историю России, привьет любовь к своей родине обучающимся, в том числе находящимся в местах лишения свободы.

Искусственный разум может помочь приобрести общепрофессиональные навыки, направленные на приобретение базовых знаний, но искусственный интеллект еще не скоро заменит преподавателя, способного не только обучить подопечных творческому мышлению, творческим решениям, но и передать им практический опыт разрешения сложных жизненных ситуаций.

Необходимость развития новой модели образования назрела давно. Поставленная цель заключается в воспитании свободных индивидов с интеллектуальными способностями, позволяющими заниматься творчеством, с высокой личной социальной ответственностью, готовых своей деятельностью к решению важных задач, являющихся актуальными для общества.

Как известно искусственный интеллект помогает решить важные вопросы в учебном процессе, в частности психоэмоциональные навыки. Вполне возможно создание проектов и цифровых программ, позволяющих общаться с искусственным интеллектом.

В частности, нейросеть позволит обеспечить массовое обучение в местах лишения свободы, что предоставит учащимся доступ к важной и необходимой информации с применением новых направлений деятельности. Теоретические знания как критерий, определяющий индивидуальные способности, перейдут в практическую плоскость с приобретенными навыками, которые будут востребованы в современном обществе.

Поэтому важную роль среди множества направлений развития образования занимает вопрос создания комплексного проекта подготовки специалистов. В настоящее время преподавателю учебного заведения отводится ключевая роль в формировании личности обучающегося в ходе его профессиональной подготовки.

Для конструктивного результата необходимо готовить специалистов, способных заниматься исследованиями современных направлений науки и техники. Крупных специалистов можно подготовить только в непосредственном общении, создавая при исправительных учреждениях специальные научные центры. Преподаватель обязан владеть современными технологиями обучения и создания научных парадигм программирования в общеобразовательной практике. Из этого следует вывод, что педагогические технологии занимают буферное положение между наукой и практикой.

Очевидно, что обучение с применением искусственного интеллекта решает многие проблемы, так как при традиционном обучении много избыточного материала, он не разделен на основной и второстепенный. Искусственный интеллект позволяет это сделать, обеспечивает обратную связь и главное открывает большие возможности для индивидуализации процесса обучения.

Бурный технологический рост в России направлен на ускоренное внедрение искусственного интеллекта в научно-производственные области с использованием роботов, беспилотного транспорта, сферы нанопроизводства, цифровых устройств, редактирование генома и т. д. Это позволит России не только удерживать уже имеющиеся позиции, но и опережать развитые в данной сфере страны.

Как известно нейросети, в которых преобладает фактор персонализации в системе образования, являются одним из основных инструментов манипулирования человеком в современных реалиях жизни. Искусственный интеллект, управляющий процессом влияния на человека, путем получения информации о типе личности управляет ее поведением и сознанием, позволяя совершать действия как в виртуальной, так и в реальной области. Таким образом, применение искусственного интеллекта в образовательном процессе осужденных в указанной концепции будет способствовать их воспитанию и исправлению как граждан интеллектуального социума. В настоящее время при данном обучении все зависит от квалификации и мастерства педагога, и возникает сложность в обеспечении всех специалистами такого уровня. Программированное обучение позволит комплексно решить данную проблему.

Необходимо отметить, что в целях сокращения рецидивизма и улучшения экономико-технологического развития в стране, стоит сосредоточить внимание на привлечении осужденных еще на этапе отбывания наказания к программированию и работе с искусственным интеллектом.

Первые шаги в данном направлении уже сделаны. «ФСИН России рассматривает возможность привлечения осужденных ИТ-специалистов, которые отбывают наказание в исправительных центрах, к удаленной работе по специальности в коммерческих компаниях» [4].

В марте 2020 г. Сбербанк первым стал использовать труд отбывающих наказание преступников для развития искусственного интеллекта. Осужденные помогали ИИ распознавать рукописный текст и детали изображений [1].

«Искусственный интеллект как источник воздействия на человека, распознает психотип личности и управляет ее поведением, мотивируя на определенные поступки не только в виртуальной, но и в реальной сфере. Персонализированное управление человеком и есть особенность манипулирования группами в социальных сетях. Результативность в достижении поставленной цели путем манипулирования учащимися на основе разработанных алгоритмов зависит от управляющей команды программистов, их профессиональных знаний в различных областях» [2].

«Существует несколько аспектов, позволяющих отрицательно реагировать на идею внедрения лиц, отбывающих наказание, в IT-системы страны. Причинами опасений могут стать: совершение экономического преступления, отсутствие желания и мотивации осужденного к исправлению и ресоциализации, нарушение устойчивого психологического строя внутри системы исполнения наказаний. Именно поэтому таким реформам должно сопутствовать внедрение усиленного кадрового отбора, представляющего собой проверку квалификации и реальных мотивов со стороны осужденного» [5]. Проверку и подготовку работников эффективнее всего осуществлять с помощью искусственного интеллекта.

Искусственный интеллект позволит проводить собеседование со специалистами, отбывающими наказание, авторитетными компаниями без вынужденного изъятия их из мест лишения свободы, что требует задействования большого количества сотрудников ФСИН. Искусственный интеллект может стимулировать и развивать образовательные компетенции, позволяющие раскрыть творческий потенциал индивида как личности, обладающей приобретенными практическими технологиями. Как сказано, стимулирующие обучающих процессы манипулирования на основе образовательных программ образуют интеллектуальные способности программистов, знаний контингента, с которым предстоит работать.

Обучение осужденных с применением искусственного интеллекта улучшит социальное и экономическое состояние страны. Для этого необходимо создавать при Министерстве юстиции РФ научные образовательные центры, состоящие из квалифицированных ИТ-специалистов, с целью обучения находящихся в местах лишения свободы осужденных дистанционно.

Такое образование позволит увеличить количество специалистов в востребованной в настоящее время сфере применения искусственного интеллекта. Например, после освобождения из мест лишения свободы гражданин будет иметь неоценимый опыт работы по актуальной специальности.

Заключение. Результаты нашей работы в известной мере подтвердили рабочую гипотезу о том, что программированные пособия, в которых реализованы принципы программированного обучения посредством применения искусственного интеллекта, эффективны, так как:

1. Повышают интерес к новым формам обучения, внося разнообразие в учебный процесс, а поэтапный самоконтроль создает дополнительную мотивацию осужденных в обучении.

2. Программированное обучение очень эффективно при индивидуальной деятельности обучающихся, так как применяется концепция управления познавательной деятельностью учащихся, а материал предоставляется небольшими частями с программой, способствующей восприятию каждой темы.

3. При программированном обучении с применением искусственного интеллекта увеличивается в сравнении с традиционным процессом обучения заинтересованность осужденных в получении практического результата.

Таким образом, применение искусственного интеллекта в рамках социально-педагогической и социально-экономической реабилитации является важным направлением в развитии пенитенциарной системы России.

Список литературы

1. Греф назвал пять принципов современного образования (2021) // РИА «Новости». 14 января. URL: https://ria.ru/20210114|obrazovanie-1593065352.html

2. Макаревич Э. Ф. Искусственный интеллект как инструмент формирования личности в системе образования и социальных сетях / Московский гуманитарный университет // Знание, понимание, умение. 2022. С. 192–203.

3. Уголовно-исполнительный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Российская газета. № 249. 22.12.2001.

4. ФСИН собрался привлекать осужденных АТ-шников к работе по специальности. Москва SNuws.ru // 2022.27.04. URL: https://www.cnews.ru/news/top/2022–04–27_fsin_sobralas_privlekat

5. Кравцова Е. А. Искусственный интеллект – новый инструмент ресоциализации осужденных / Российский государственный социальный университет // Перспективное применение НБИК-технологий: синергия искусственного интеллекта с информационным обществом. 2022. С. 78–83.

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

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИХ ВЛИЯНИЕ НА РАЗВИТИЕ УГОЛОВНОГО ПРАВА

Аннотация. Цифровизация общественных отношений порождает потребность в совершенствовании нормативной правовой базы, в том числе уголовного законодательства. Это обусловлено использованием цифрового пространства и цифровых технологий при совершении преступлений. Поставлена цель выявить влияние цифровых технологий на развитие уголовного права. Для достижения этой цели в статье был проведен обзор видов преступлений, совершаемых в цифровом пространстве или с использованием цифровых технологий, приведены данные официальной статистической отчетности, раскрыты преимущества совершения таких преступлений, показано влияние изменения механизма совершения преступлений на качество уголовного закона. Делается вывод, что еще не сложилось целостное представление о формировании уголовно-правовой политики в сфере противодействия преступлениям, совершаемым в цифровом пространстве или с использованием цифровых технологий.

Ключевые слова: цифровые технологии, цифровое пространство, информационно-телекоммуникационная сеть, электронная сеть, Интернет, механизм преступления, криминализация, общественная опасность

DIGITAL TECHNOLOGIES AND THEIR IMPACT ON THE DEVELOPMENT OF CRIMINAL LAW

Abstract. The digitalization of public relations gives rise to the need to improve the regulatory legal framework, including criminal law. This is due to the use of digital space and digital technologies in the process of committing crimes. The author set himself the goal of identifying the impact of digital technologies on the development of criminal law. To achieve this goal, the article reviewed the types of crimes committed in the digital space or using digital technologies, provides data from official statistical reporting, reveals the benefits of committing such crimes, and shows the impact of changing the mechanism for committing crimes on the quality of criminal law. It is concluded that there has not

yet been a holistic view of the formation of criminal law policy in the field of combating crimes committed in the digital space or using digital technologies.

Keywords: digital technologies, digital space, information and telecommunications network, electronic network, Internet, crime mechanism, criminalization, public danger

Введение. Развитие цифровых технологий оказывает существенное влияние на механизм преступления, то есть процесс его совершения, в том числе способ применения орудий и средств, а также все иные деяния субъекта, в результате которых образуются материальные и нематериальные следы.

Вместе с тем при изучении преступлений, совершаемых в цифровом пространстве, необходимо задаться вопросом, следует ли рассматривать такую преступность как совершенно новую форму правонарушений, что требует обновления набора криминологических инструментов, или следует преуменьшить преувеличение окружающей ее новизны и сосредоточиться на естественной эволюции преступности. Данный вопрос актуален, в том числе в связи с тем, что уголовно-правовые нормы все чаще дополняются квалифицирующими / особо квалифицирующими признаками «с использованием СМИ либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»», с публичной демонстрацией, в том числе в СМИ или информационно-телекоммуникационных сетях (включая сеть «Интернет»)». Но всегда ли использование цифровых технологий может привести к изменению степени общественной опасности преступления? Этот вопрос пока не получил однозначного ответа.

Виды преступлений, совершаемых в цифровом пространстве или с использованием цифровых технологий. Цифровые технологии используются в процессе и с целью причинения вреда / ущерба на неопределенно широкой территории, за пределами их предполагаемого использования. Чаще всего такие технологии применяются при совершении мошенничеств, компьютерных преступлений (распространение вредоносных компьютерных программ и др.), преступлений террористической, диверсионной, экстремистской направленности, для «хищения» персональных данных, сексуальных домогательств и т. д.

По данным Главного управления правовой статистики и информационных технологий Генеральной прокуратуры РФ, регистрируется рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, в 2018 г. было зарегистрировано 174 674 таких преступления, в 2019 г. – 294 409 (+68,5 %), в 2020 г. – 510 396 (+73,4 %), в 2021 г. – 517 722 (+1,4 %), в 2022 г. – 522 065 (+0,8 %).

В 2018 г. было зарегистрировано 108 016 преступлений, совершаемых в сети «Интернет» (61,8 % от всех зарегистрированных преступлений совершаемых с использованием цифровых технологий); в 2019 г. – 157 036 (53,3 %); в 2020 г. – 300 337 (58,8 %); в 2021 г. – 351 463 (67,9 %); в 2022 г. – 381 112 (73 %). Чаще всего такие преступления совершаются с использованием средств мобильной связи: в 2018 г. зарегистрировано 61 299 преступлений (35,1 % от всех зарегистрированных преступлений совершаемых с использованием цифровых технологий); в 2019 г. – 116 154 (39,5 %); в 2020 г. – 218 739 (42,9 %); в 2021 г. – 217 552 (42 %); в 2022 г. – 212 963

(40,8 %). Достаточно большой процент преступлений совершается с использованием расчетных (пластиковых) карт: в 2018 г. зарегистрировано 16 427 преступлений (9,4 % от всех зарегистрированных преступлений, совершаемых с использованием цифровых технологий); в 2019 г. – 34 383 (11,7 %); в 2020 г. – 190 167 (37,3 %); в 2021 г. – 165 658 (32 %); в 2022 г. – 127 149 (24,4 %); реже с использованием компьютерной техники: в 2018 г. зарегистрировано 15 027 преступлений (8,6 % от всех зарегистрированных преступлений, совершаемых с использованием цифровых технологий); в 2019 г. – 18 261 (6,2 %); в 2020 г. – 28 653 (5,6 %); в 2021 г. – 27 519 (5,3 %); в 2022 г. – 29 140 (5,6 %).

Данные статистической отчетности свидетельствуют о том, что наибольшее количество регистрируемых деяний – это преступления против собственности: в 2019 г. было зарегистрировано 98 798 краж (ст. 158 УК), 119 903 мошенничества (ст. 159 УК), 16 119 мошенничеств с использованием электронных средств платежа (ст. 159^3 УК) и 970 мошенничеств в сфере компьютерной информации (ст. 159^6 УК); в 2020 г. – 173 416 (прирост к АППГ на 75,5 %), 210 493 (+75,6 %), 25 820 (+60,2 %), 761 (10,8 %); в 2021 г. – 156 792 (снижение на 9,6 %), 238 560 (+13,3 %), 10 258 (–60,3 %), 431 (–43,4 %); в 2022 г. – 113 565 (–27,6 %), 249 984 (+4,6 %), 7 288 (–29 %), 334 (–22,5 %) преступления соответственно.

Развитие цифрового пространства и цифровых технологий способствовало и росту незаконной торговли различными предметами (наркотическими средствами; психотропными веществами; лекарственными препаратами; дикой флорой и фауной, в том числе находящейся под угрозой исчезновения; оружием и др.) с использованием данного цифрового пространства. К примеру, в 2018 г. было зарегистрировано 18 805 преступлений, предусмотренных ст. 228^1 УК (незаконный оборот наркотиков с целью сбыта); в 2019 г. – 24 677 (+31,2 %); в 2020 г. – 47 060 (+90,7 %); в 2021 г. – 51 444 (+9,3 %); в 2022 г. – 62 209 (+21 %).

Отмечается, что цифровое пространство стало активно использоваться для распространения идеологии насилия; пропаганды и финансирования террористической, экстремистской, диверсионной деятельности; вербовки новых членов террористических, экстремистских, диверсионных формирований и их обучения и в процессе приготовительной и непосредственной террористической, экстремистской, диверсионной деятельности [1. С. 251–269]. Многие террористы радикализируются именно в цифровом пространстве. Специалисты по безопасности подчеркивают даже, что террористические формирования используют Интернет не только для обращения в свою веру, но и для максимальной огласки своей деятельности. В этом плане Интернет стал неуправляемым пространством, требующим более жесткого регулирования [21. P. 57–75], поскольку под угрозу ставится не только национальная безопасность государства, но нередко мир и безопасность всего человечества.

Существует серьезная обеспокоенность по поводу распространения «фейковых» новостей (дезинформации) через социальные сети. Это происходит как в политических, так и иных целях (например, медицинская или научная дезинформация, касающаяся вакцинации или изменения климата) и способна повлечь за собой негативные последствия для общества. Исследования показывают, что многие люди в настоящее время считают «выдуманные новости и информацию» критической

проблемой: опрос исследовательского центра Pew Research Center показал, что значительное количество респондентов оценили это как «очень большую проблему для страны», чем насильственные преступления, изменение климата или терроризм [13].

Кроме того, появились такие новые деяния, которые стали обозначаться терминами «груминг», «секстинг», «сексуальное вымогательство», «порнография из мести», «киберфлэшинг», «сексуальное насилие с использованием изображений», «принудительный контроль». Несмотря на то, что данные виды насилия являются бесконтактными, они могут повлечь за собой долгосрочные психологические травмы для жертвы [17, p. 871–892]. Такие последствия характерны не только для насильственных, но и иных преступлений, совершаемых в цифровом пространстве или с использованием цифровых технологий. Исследования последних лет показывают, что наряду с возможным экономическим ущербом жертвы таких преступлений могут испытывать пагубные последствия для своего эмоционального и психологического благополучия, включая симптомы, сходные с симптомами посттравматического стрессового расстройства, а также признаки дистресса, такие как тревога, соматизация, гнев и плохое настроение. У лиц, однажды столкнувшихся с такими преступлениями, повышается страх повторно стать жертвой, что порождает потерю доверия к другим и обществу [18].

Представленные выше данные не показывают в полном объеме всей проблемы, поскольку официальная статистика преступности неадекватно отражает конкретные данные таких деяний, и их львиная доля остается вне поля зрения правоприменителя. Одной из очевидных причин является высокий уровень их латентности.

Кроме того, уголовный закон больше внимания уделяет существу преступления, а не технологическим средствам, используемым для его совершения. Многие преступления включают в себя онлайн- и офлайн-компоненты. В результате регистрация таких правонарушений остается проблематичной или фрагментарной, и можно сделать лишь предварительные оценки о ее глобальности. Существует даже мнение о том, что криминологи находятся во власти фирм по кибербезопасности и аналитических центров, которые производят сомнительные опросы и статистику в качестве маркетингового материала, часто сильно преувеличивая распространенность киберпреступности и причиняемый ею финансовый ущерб [15. P. 76–92].

Некоторые специалисты в области IT-технологий отмечают, например, что преступность в цифровом пространстве растет не только по частоте, но и в процентах от всех преступлений. По некоторым данным интернет-провайдеры ежедневно регистрируют около 80 млрд автоматических сканирований со стороны онлайн-преступников с целью выявления целей для киберпреступлений [14]. По данным специалистов Positive Technologies наибольшему риску кибератак подвергаются компании, оказывающие онлайн-услуги и предоставляющие возможность онлайн-оплаты (атакующие могут встраивать в сайты вредоносный код для перехвата персональных и платежных данных) [11].

Увеличение количества совершаемых преступлений в цифровом пространстве и с использованием цифровых технологий вполне объяснимо.

Во-первых, увеличивается количество людей, которые пользуются данным пространством и соответствующими технологиями. Так, по данным Global Digital 2023, на начало 2023 г. 5,44 млрд человек (68 % от общей численности населения

мира) пользуются мобильными телефонами; 64,4 % мирового населения имеют доступ в Интернет; социальные сети насчитывают 4,76 млрд пользователей (60 % от мирового населения) [7].

Во-вторых, большое количество пользователей цифровым пространством не обладают достаточными цифровыми знаниями.

Специалисты отмечают, что основной причиной инцидентов кибербезопасности является человеческая ошибка. Злоумышленники часто пользуются и плохой «гигиеной» кибербезопасности (слабыми паролями) [19. P. 140–149].

В-третьих, внеюрисдикционный, транснациональный характер Интернета и простота глобальной цифровой связи (устройства, с помощью которых совершаются преступления, могут находиться в другой стране), а также повсеместное распространение цифровых устройств в обществе [12. P. 451–473].

Кибератаки не предприятия, которые могут даже разрушить бизнес, обусловлены целым рядом факторов, в частности низкой осведомленностью персонала о кибербезопасности; неадекватной защитой критической и конфиденциальной информации; отсутствием бюджета; нехваткой специалистов по кибербезопасности; отсутствием подходящих руководств по кибербезопасности и др. [19. P. 140–149].

Кроме того, росту рассматриваемых преступлений способствует эволюция цифровых технологий. Для совершения преступлений используются новые компьютерные устройства, технологии искусственного интеллекта, облачные и туманные вычисления, интернет вещей, промышленный интернет, т. е. технологии, работающие автономно без участия человека и в режиме «самообучения», что также выводит данную преступность из-под контроля человека и общества [5. С. 21]. К сожалению, правоприменительная сфера существенно отстает от данных технических новшеств, что серьезно затрудняет процесс раскрытия и расследования преступлений.

Преимущества преступлений, совершаемых в цифровом пространстве или с использованием цифровых технологий. Для обозначения преступного поведения с использованием информационно-телекоммуникационной сети, в том числе сети «Интернет», чаще всего используют термины «киберпреступность», «онлайн-преступление», «интернет-преступление» или «цифровое преступление» [12. P. 451–473]. При этом выделяют как традиционные киберпреступления, которые совершаются для усиления существующих форм правонарушений (например, онлайн-мошенничество, распространение материалов о сексуальной эксплуатации детей и др.), и киберзависимые преступления, т. е. преступления, которые невозможно совершить в отсутствие Интернета, и охватывающие вредоносные действия, которые не существуют за пределами цифровой сферы (например, программы-вымогатели, кибератаки и др.) [14]. Кроме того, выделяют преступления, совершаемые с использованием цифровых технологий, когда они не имеют непосредственного отношения к преступлению (например, когда торговцы наркотиками обмениваются сообщениями через Интернет с помощью инструментов шифрования) [15. P. 76–92].

Киберпреступления могут быть направлены против конкретных лиц (например, преследование в сети), групп лиц (например, преступления на почве ненависти), компьютерных систем или сетей (например, взлом), (больших) групп пользователей

компьютеров (например, вирусные инфекции), виртуальных объектов (например, виртуальное изнасилование), критических инфраструктур (например, кибератаки на электростанции) и т. д. [20. P. 480–497].

Среди преимуществ совершения данных преступлений выделяют следующие моменты:

– более широкое использование технологий социальных сетей и большой охват аудитории. Это способствует тому, что один преступник теперь может охватить большее количество жертв [14];

– снижение затрат и уровня навыков, необходимых для совершения киберпреступлений [14];

– анонимность Интернета. Люди могут выходить в сеть под вымышленными именами, используя аватары или даже без необходимости сигнализировать о своем присутствии в сети [16. P. 98–117];

– доступность. С различных сайтов можно бесплатно получить личную (конфиденциальную) информацию как отдельного индивидуума, так и целых предприятий. Бесплатно можно загрузить и различные письменные, звуковые или визуальные материалы [16. P. 98–117], в том числе деструктивного свойства (например, порнографические материалы; призывы к действиям террористического характера и др.);

– скорость распространения информации;

– возможность использования цифровых технологий на любых территориях, в том числе представляющих опасность (зоны военных конфликтов, чрезвычайных экологических ситуаций или экологического бедствия и др.) [2. С. 31–39];

– возможность совершения преступлений из любого места (например, места жительства, работы, учебы, отдыха и др.);

– источник опасности и объект посягательства могут быть удалены друг от друга на большое расстояние (они могут находиться не только в разных районах одного и того же населенного пункта, но и в разных регионах страны и даже за ее пределами), что создает сложность в раскрытии и расследовании таких преступлений;

– физическая безопасность субъектов, применяющих цифровые технологии (например, при использовании опасных предметов – химических, отравляющих, взрывчатых веществ и др.), и сложность их обнаружения [2. С. 31–39].

Влияние изменения механизма совершения преступлений в связи с развитием цифрового пространства и цифровых технологий на качество уголовного закона. Происходящие изменения должны своевременно отражаться и в нормах уголовного законодательства, в котором все чаще в составах преступлений можно обнаружить соответствующие криминообразующие или квалифицирующие / особо квалифицирующие признаки.

Отметим, что в настоящее время российский законодатель не ограничивается внесением изменений только в нормы о преступлениях в сфере компьютерной информации (гл. 28 УК). Соответствующие квалифицирующие признаки можно обнаружить в целом ряде составов преступлений против личности (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2, ч. 2 ст. 128^1, п. «б» ч. 3 ст. 133, п. «в» ч. 2 ст. 151^2); против собственности (п. «г» ч. 3 ст. 158, ст. 159^3, 159^6) и в сфере экономической деятельности (ст. 171^2, 185^3); против общественного порядка и общественной безопасности (ст. 205^2, п. «в» ч. 3 п. «в» ч. 5 ст. 222, п. «в» ч. 3 п. «в» ч. 5 ст. 222^1, п. «в»

ч. 3 п. «в» ч. 5 ст. 222^2, п. «б» ч. 2 ст. 228^1, п. «д» ч. 2 ст. 230, ч. 11 ст. 238^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2, п. «г» ч. 2 ст. 245, ч. 11, п. «б» ч. 2 ст. 258^1); против основ конституционного строя и безопасности государства (ч. 2 ст. 280, ч. 2 ст. 280^1, п. «в» ч. 2 ст. 280^4, ст. 282), против мира и безопасности человечества (п. «в» ч. 2 ст. 354^1).

При этом следует констатировать тот факт, что в настоящее время процесс внесения соответствующих изменений в уголовный закон носит хаотичный, бессистемный характер, что не может не сказаться на его качестве и нередко порождает существенные проблемы в правоприменительной практике.

Ярким примером, на наш взгляд, является внесение изменений в ст. 258^1 УК, в которой законодатель предусмотрел в ч. 11 ответственность за незаконные приобретение или продажу особо ценных диких животных и водных биологических ресурсов, их частей и дериватов (производных) с использованием СМИ либо электронных или информационных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а в п. «б» ч. 2 этой же нормы за совершение этих же деяний с публичной демонстрацией, в том числе в СМИ или информационно-телекоммуникационных сетях (включая сеть «Интернет»). В данном случае существует сложность в разграничении этих признаков. Это приводит к тому, что правоприменитель в идентичных ситуациях квалифицирует деяние по разным частям нормы. Как следствие – нарушение принципа справедливости, тем более что законодатель увидел разницу в степени общественной опасности данных признаков, и поэтому описанное в ч. 11 нормы преступление относится к категории средней тяжести (до 5 лет лишения свободы), а в ч. 2 – тяжкого (до 6 лет лишения свободы). Что интересно, добавление иных квалифицирующих признаков к названным (таких как совершение этих же деяний с использованием служебного положения, в соучастии) увеличивает степень общественной опасности деяний, описанных в ч. 11 нормы (см. ч. 21, 3, 31), что также вызывает вопросы.

Возникает вопрос о степени общественной опасности и в ситуации хищений чужого имущества. Так, если виновный похищает денежные средства, например, в размере 3000 руб., деяние квалифицируется по ч. 1 ст. 158 УК (до двух лет лишения свободы). Если эта же сумма похищается из одежды, сумки или другой ручной клади, находившихся при потерпевшем, содеянное квалифицируется по п. «г» ч. 2 ст. 158 УК (до пяти лет лишения свободы), а если речь идет о хищении этой же суммы с банковского счета, а равно в отношении электронных денежных средств, то ответственность наступает по п. «г» ч. 3 ст. 158 УК (до шести лет лишения свободы). Таким образом, цифровой способ совершения кражи существенно влияет на степень ее общественной опасности, но всегда ли это оправдано?

По мнению некоторых ученых, в данном случае распространенность такого деяния само по себе не является основанием для установления роста их общественной опасности [2, с. 11–16]. Мы также придерживаемся мнения о том, что совершение преступлений в цифровом пространстве или с использованием цифровых технологий не во всех случаях увеличивает степень общественной опасности деяний. Считаем излишним добавлять рассматриваемый признак во все составы преступлений, которые могут быть совершены в цифровом пространстве или с использованием

цифровых технологий. На современном этапе считаем достаточным дополнить ст. 63 УК частью 12 в следующей редакции «12. Судья (суд), назначающий наказание в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать отягчающим обстоятельством совершение преступления с использованием информационно-телекоммуникационных технологий».

Кроме того, введение квалифицирующего признака в п. «г» ч. 3 ст. 158 УК и нового состава преступления, предусмотренного в ст. 159^3 УК, повлекло за собой сложности в разграничении этих деяний и противоречивой судебной практике [8. С. 159–165].

Следует констатировать, что еще не сложилось целостное представление о том, как должна формироваться и развиваться уголовно-правовая политика в сфере противодействия преступлениям, совершаемым в цифровом пространстве или с использованием цифровых технологий.

Законодатель пытается решить сиюминутные проблемы, вводит новые статьи, модернизирует старые, но системного регулирования (охраны) не наблюдается [10. С. 225]. Но важно помнить о том, что точечные изменения в уголовном законе, как указывает Р. И. Дремлюга, уже исчерпали свои возможности. Необходим пересмотр доктринально-политических основ охраны общественных отношений, сложившихся в процессе «цифровой трансформации» экономики и общества [3. С. 37].

Конструируя нормы о преступлениях, совершаемых в цифровом пространстве или с использованием цифровых технологий, необходимо соблюдать правила законодательной техники, выяснять социальную обусловленность этих норм и четко оценивать основания криминализации деяний.

Подчеркнем, что ключевым основанием криминализации деяния или изменения интенсивности его пенализации является общественная опасность. Поэтому, внося изменения в уголовный закон, законодатель должен внимательно отнестись к вопросу оценки данного критерия. Чаще всего законодатель безальтернативно оценивает использование цифровых технологий в процессе совершения преступлений как отягчающее обстоятельство без учета его влияния на степень общественной опасности.

Следует констатировать и факт использования законодателем разной терминологии при конструировании соответствующего признака преступления. Чаще всего такой признак формулируется, как «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»», в отдельных составах – совершенные «через … электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»)» (ст. 185^3) или «с использованием … электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»» (ст. 205^2, п. «б» ч. 2 ст. 228^1, ч. 11 ст. 258^1, ч. 2 ст. 280, п. «в» ч. 2 ст. 280^4), либо «с публичной демонстрацией, в том числе в … информационно-телекоммуникационных сетях (включая сеть «Интернет»)» (п. «г» ч. 2 ст. 245, п. «б» ч. 2 ст. 258^1). Сложность толкования данных признаков заключается в том, что на законодательном уровне раскрывается только понятие «информационно-телекоммуникационная сеть» и не раскрываются категории «электронные сети» и «Интернет», что следует расценивать как пробел российского законодательства. В научной литературе высказывается предположение о том, что термин «электронный» является дополнительной

характеристикой самих информационно-телекоммуникационных сетей [6. С. 257]. Но для единообразия применения норм уголовного закона требуется легальное определение данных категорий.

Согласимся с мнением и о том, что криминализации подлежат лишь те деяния, которые можно обнаружить и расследовать [9. С. 78]. Поэтому, как справедливо отмечается в научной литературе, увеличение круга деяний против цифровой экономики и информационного общества должно сопровождаться широкомасштабным повышением квалификации и увеличения числа сотрудников органов уголовной юстиции в сфере информационно-коммуникационных технологий [4. С. 23].

В настоящее же время большой процент рассматриваемых преступлений остается нераскрытыми. Так, по данным указанной выше статистической базы, в 2018 г. осталось нераскрытыми 119 811 таких преступлений (68,6 % от всех зарегистрированных преступлений совершаемых с использованием цифровых технологий); в 2019 г. – 206 694 (70,2 %); в 2020 г. – 379 830 (74,4 %); в 2021 г. – 388 607 (75 %); в 2022 г. – 370 179 (71 %).

Заключение. Полагаем, что преступления, совершаемые в цифровом пространстве или с использованием цифровых технологий, являются естественной эволюцией преступности, обусловленной цифровизацией общественных отношений. Конечно, развитие цифрового пространства и цифровых технологий оказывает влияние на механизм совершения преступлений, в отдельных случаях это влияет и на степень общественной опасности содеянного, но не всегда. Поэтому корректировка уголовного закона, которая осуществляется путем криминализации новых деяний или добавления в уже существующие нормы криминообразующих и квалифицирующих / особо квалифицирующих соответствующих признаков, не всегда положительно влияют на его качество. Законодательный процесс должен сопровождаться строгим соблюдением выработанных в доктрине уголовного права правил. Только в этом случае можно сконструировать социально обусловленные нормы, способные выполнить основную задачу уголовного законодательства – удержание преступности в контролируемых государством рамках.

Кроме того, следует констатировать, что одних мер уголовно-правового характера недостаточно для снижения уровня преступлений, совершаемых в цифровом пространстве или с использованием цифровых технологий. Требуется продолжать работу по повышению цифровой грамотности и осведомленности о кибербезопасности, а также повышения квалификации и увеличения числа правоприменителей в области цифровых технологий.

Список литературы

1. Антонова Е. Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию / Е. Ю. Антонова // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 251–269. DOI: 10.21202/jdtl.2023.10. EDN HFPMTN.

2. Антонова Е. Ю. Технологии искусственного интеллект. субъект преступления или орудие / средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 1. С. 31–39. DOI 10.31429/20785836–14–1–31–39.

3. Вельтмандер А. Т. Общественная опасность преступлений, совершенных с использованием информационно-коммуникационных (цифровых) технологий // Уголовная политика в условиях цифровой трансформации: сборник статей материалов II Всероссийской научно-практической конференции, Казань, 27 апреля 2023 года. Казань: Отечество, 2023. С. 11–16.

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

5. Евдокимов К. Н. Противодействие технотронной преступности: теория, законодательство, практика: монография. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры РФ, 2023. 171 с.

6. Иванов С. А., Ковалева О. Н., Прокопенко Н. А. Значение современных технологий в совершении преступления // Современный ученый. 2022. № 4. С. 255–260.

7. Интернет и соцсети в начале 2023 год. главные цифры Global Digital 2023 // VC.ru. URL: https://vc.ru/marketing/596126-internet-i-socseti-v-nachale-2023-goda-glavnye-cifry-global-digital-2023

8. Клименко А. К. Проблемы квалификации хищений, совершенных с использованием технологии бесконтактной оплаты // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 года. М.: Федеральное государственное казенное образовательное учреждение высшего образования «Университет прокуратуры Российской Федерации», 2021. С. 159–165.

9. Коробеев А. И. Уголовно-правовая политика России: от генезиса до кризиса. М.: Юрлитинформ, 2019. 352 с. (Уголовное право).

10. Трансформация права в цифровую эпоху: монография / Министерство науки и высшего образования РФ, Алтайский государственный университет; под ред. А. А. Васильева. Барнаул: Изд-во Алт. ун-та, 2020. 432 с.

11. Число кибератак в России и в мире // TAdviser. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru (дата обращения: 14.08.2023).

12. Brants C., Jackson A., Wilson T. J. A Comparative Analysis of Anglo-Dutch Approaches to ‘Cyber Policing’: Checks and Balances Fit for Purpose? // The Journal of Criminal Law. 2020. Vol. 84, Is. 5. Pp. 451–473. DOI: 10.1177/0022018320952561.

13. Buchanan T., Benson V. Spreading Disinformation on Facebook: Do Trust in Message Source, Risk Propensity, or Personality Affect the Organic Reach of “Fake News”? // Social Media + Society. 2019. Vol. 5, Is. 4. DOI: 10.1177/2056305119888654.

14. Curtis J., Oxburgh G. Understanding cybercrime in ‘real world’ policing and law enforcement // The Police Journal. 2022. Vol. 0(0). DOI: https://doi.org/10.1177/0032258X221107584.

15. Dupont B., Whelan C. Enhancing relationships between criminology and cybersecurity // Journal of Criminology. 2021. Vol. 54, Is. 1. Pp. 76–92. DOI: 10.1177/00048658211003925.

16. Goldsmith A., Wall D. S. The seductions of cybercrime: Adolescence and the thrills of digital transgression // European Journal of Criminology. 2022. Vol. 19, Is. 1. Pp. 98–117. DOI: 10.1177/1477370819887305.

17. Killean R., McAlinden A.-M., Dowds E. Sexual Violence in the Digital Age: Replicating and Augmenting Harm, Victimhood and Blame // Social & Legal Studies. 2022. Vol. 31, Is. 6. Pp. 871–892. DOI: 10.1177/09646639221086592.

18. Palassis A., Speelman C. P., Pooley J. A. An Exploration of the Psychological Impact of Hacking Victimization // SAGE Open. 2021. Vol. 11, Is. 4. DOI: 10.1177/21582440211061556.

19. Tasheva I. Cybersecurity post-COVID-19: Lessons learned and policy recommendations // European View. 2021. Vol. 20, Is. 2. Pp. 140–149. DOI: 10.1177/17816858211059250.

20. Wagen W., Pieters W. The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory // European Journal of Criminology. 2020. Vol. 17, Is. 4. Pp. 480–497. DOI: 10.1177/1477370818812016.

21. Zedner L. Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism // Common Law World Review. 2021. Vol. 50, Is. 1. Pp. 57–75.

А. М. Ахатова,
ассистент,
Удмуртский государственный университет

ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКУЮ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В СЕТЕВОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОГО И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА

Аннотация. Развитие сетевого информационного пространства обусловило появление новых и изменение существующих видов преступлений, связанных с использованием компьютерной информации и информационно-телекоммуникационных сетей. В целях дестабилизации общественно-политической ситуации в стране расширяются масштабы оказания негативного информационно-психологического воздействия на индивидуальное, групповое и общественное сознание. Нарушение сознательной деятельности лица приводит к принятию им бессознательных решений, к психологической зависимости и деструкции личности. Тем не менее на практике возникают вопросы относительно квалификации действий лиц, совершивших преступление в результате информационно-психологического воздействия. Раскрываются понятие информационно-психологической безопасности личности в сетевом информационном пространстве, основные угрозы, способные оказать влияние на психику человека с анализом судебной практики. Внесены предложения относительно квалификаций действий лиц, совершивших преступления в результате информационно-психологического воздействия.

Ключевые слова: экстремизм, терроризм, сетевое информационное пространство, информационная безопасность, информационно-психологическая безопасность, компьютерная информация, информационно-телекоммуникационная сеть, уголовное право, квалификация преступлений

THE IMPACT ON THE INFORMATION AND PSYCHOLOGICAL SECURITY OF A PERSON IN THE NETWORK INFORMATION SPACE IN ORDER TO COMMIT EXTREMISM AND TERRORISM

Abstract. The article analyzes the problem of the emergence of new types of crimes committed in the network information space. Criminals have a negative information-psychological impact on individual, group and public consciousness. The purpose of such an impact is to destabilize the political situation. Violation of the conscious activity of a person leads to the adoption of unconscious decisions by him, to psychological dependence and destruction of personality. In judicial practice, questions arise regarding the qualification of the actions of persons who have committed a crime as a result of information and psychological influence. The article reveals the concept of information-psychological security of the individual in the network information space, information threats. Proposals have been made to qualify the actions of persons who have committed crimes as a result of information-psychological influence.

Keywords: extremism, terrorism, network information space, information security, information-psychological security digital information, telecommunication network, criminal law, qualification of crimes

Возможности трансграничного оборота компьютерной информации в сетевом информационном пространстве в последнее время используются для совершения преступлений экстремистского и террористического характера, где в качестве объектов посягательства выступают общественная безопасность, основы конституционного строя и безопасность государства.

В целях дестабилизации общественно-политической ситуации в стране расширяются масштабы оказания негативного информационно-психологического воздействия на индивидуальное, групповое и общественное сознание. В эту деятельность вовлекаются религиозные, правозащитные и иные организации, а также отдельные группы граждан. Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики нашего государства [21].

Для определения сферы данного исследования необходимо раскрыть понятие сетевого информационного пространства, под которым следует понимать совокупность глобальных (GAN), региональных (MAN), локальных (LAN) и иных информационно-телекоммуникационных сетей, связывающих или способных связывать информационные системы посредством использования комплексов сетевых протоколов, главной целью которого является предоставление возможности реализации различных форм и видов коммуникации.

Сетевое информационное пространство не ограничивается только одной сетью и может включать в себя и иные сети. Например, «закрытые» сети Darknet (даркнет), «Шелковый путь» (Silk Road), «Гидра» («Hydra»), корпоративные сети (Enterprise Network), сети связи (5G) и др [23]. Наиболее часто преступными террористическими и экстремистскими формированиями используются месседжеры Telegram, Whatsapp, Viber, Skype с целью навязывания радикальных идеологических и политических взглядов, акцентируя внимание на несправедливости в обществе [8].

Уровень восприятия информации у людей различен и зависит от индивидуальных психологических и психических особенностей, образования, возрастной категории, жизненного опыта и иных факторов. Ознакомление психически нездоровых лиц, несовершеннолетних, лиц пожилого возраста, а также лиц, характеризующихся повышенной эмоциональной возбудимостью, неустойчивой психикой с негативной цифровой информацией, способна побудить их к совершению преступлений [3]. Нередко признаки лица, совершившего противоправное деяние, связаны с отсутствием в силу определенных обстоятельств и возможностей оценить поступающую информацию. Уровень критического анализа постепенно заменяется «клиповым мышлением», фрагментарное визуальное восприятие становится преобладающим.

Недостоверная информация в сетевом информационном пространстве способствует искажению чувства реальности. Это приводит деструктивному поведению человека, росту психологических, психических заболеваний, разрушению сложившихся норм нравственности, провоцирует противоправное поведение.

Еще в 2004 г. было проведено исследование в университетской психиатрической больнице в Вене относительно влияния виртуального контента на психику человека. По итогам работы был сделан вывод о прямом психологическом воздействии цифровой информации на психику человека и опубликованы в статье «Быть веб-камерой» [1].

Методы целенаправленного информационно-психологического воздействия могут быть переданы с помощью изменения яркости экрана на цифровом устройстве, звуков, которые могут вызвать негативные реакции организма. Широко известен случай, произошедший в Японии, под названием «Dennō senshi Porygon», когда во время просмотра мультфильма «Покемон» («Карманные монстры») у детей возникли головные боли, судороги, слепота и конвульсии, многие из них были госпитализированы в больницу [2].

Кандидат психологических наук П. В. Цыганкова выделяет основные психологические угрозы, возникающие в информационном пространстве, способные оказать влияние на психику человека:

1. *Угрозы, связанные с цифровой продукцией* [28]. В данную группу относится информация, оказывающая деструктивное воздействие на психику человека. Например, размещение в социальных сетях, мессенджерах, YouTube-каналах, интернет- и иных ресурсах материалов, возбуждающих ненависть либо вражду, размещение «фейковой» информации. Примером может являться распространение недостоверной информации в социальных сетях о планировании террористических актов в России Службой безопасности Украины [5].

2. *Угрозы, связанные с виртуальными социальными коммуникациями* [28]. К ним можно отнести «кибербулинг», «кибersталкинг», «кибергруминг», «кибервуайеризм», блокирование доступа к банковским, медицинским и иным услугам, которыми пользуются злоумышленники в целях оказания на них психологического воздействия.

3. *Угрозы, связанные с избыточным присутствием в сетевом информационном пространстве* [28]. Нередко вовлеченность лиц в виртуальную реальность сопро-

вождается раздражительностью, потерей внимания, отсутствием живого общения, что может привести к искажению идентичности, ослаблению связей с реальностью и возможностью использования таких лиц в противоправных целях.

4. *Угрозы, связанные с неправомерным доступом к компьютерной информации* [28]. К ним можно отнести похищение цифровых идентификационных данных, рассылку в сетевых платформах компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, воздействия на операторов в целях совершения ими перечисленных выше действий. Примером данной угрозы может служить похищение базы данных психоневрологических диспансеров России службой безопасности Украины для оказания на них психологического воздействия в целях организации террористических актов.

Таким образом, угрозы информационно-психологического воздействия приобрели особую степень актуализации в связи с расширением возможностей деструктивного воздействия на человека путем внушения, принуждения, манипуляции и других методов.

Поэтому в целях обеспечения правовой охраны психики человека от информационных угроз в конце 1990-х гг. был разработан проект ФЗ «Об информационно-психологической безопасности». Тем не менее законопроект был отклонен в первом чтении. В 2014 г. была разработана Концепция информационного кодекса ИГП РАН. Одним из основных принципов данного нормативного акта являлось «сдерживание распространения информации террористического, экстремистского характера…» [10].

На сегодняшний день информационно-психологическая безопасность личности, общества и государства имеет статус стратегического национального приоритета в соответствии с Доктриной информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646 [26], Указами Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [25], от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [27], Распоряжением Правительства РФ от 22 декабря 2022 г. № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» [17].

Тем не менее в силу неоднозначности юридико-технического характера исследуемого вопроса ученые-правоведы не придерживаются определенного мнения относительно сущности рассматриваемого понятия. Содержательная наполняемость данного термина осуществляется на стыке исследовательских наблюдений в сферах психологии и психиатрии, общественного здоровья, философии и юриспруденции [14]. Г. В. Грачев определяет ее как состояние защищенности различных субъектов от деструктивного воздействия [6]. К. Д. Рыдченко, А. А. Смирнов под информормационно-психологической безопасностью понимают состояние защищенности человека от негативного воздействия на его нравственно-психологическое здоровье [22, 24]. В. Н. Лопатин придерживается аналогичного мнения, выделяя при этом психику человека в качестве объекта посягательства [11].

Исследуемое понятия находит свое отражение и в судебной практике.

– В постановлении Октябрьского районного суда г. Новосибирска от 12.12.2018 по делу № 5–68/2018 информационно-психологическая безопасность личности определяется как состояние защищенности личности, которая может быть выражена в испытывании чувства надежности, уверенности, в отсутствии тревожности, озабоченности и т. п.), обеспечивающее сохранение ее целостности и возможности развития при постоянных информационных воздействиях на индивидуальное сознание (сохранение ее системообразующих качеств) [15].

– В решении Арбитражного суда Иркутской области от 28.07.2017 по делу № А19–9525/2016 [19], решении Арбитражного суда Иркутской области от 17.03.2017 по делу № А19–9523/2016 [18] рассматриваемое понятие определяется как искажение представления о чем-либо, вызывающее ассоциации, не соответствующие уровню их физиологической зрелости.

– В решении Дзержинского районного суда города Волгограда от 29.07.2011 по делу № 2–4359/2011 информационно-психологическую безопасность личности рассматривают как создание факторов защищенности психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-ориентировочной основы социального поведения человека и в целом жизнедеятельности в современном обществе [20].

Тем не менее при изучении данного явления возникают вопросы относительно правовой оценки действий лиц, совершивших преступление под информационно-психологическим воздействием.

В связи со сложившейся обстановкой в стране участились случаи поджогов военкоматов и административных зданий в России. Злоумышленники путем использования социальных сетей, средств связи под видом сотрудников правоохранительных органов, банков и других государственных организаций сообщают о совершающихся преступлениях либо предлагают взять кредит и, используя приемы психологической манипуляции против либо помимо их воли, побуждают совершить определенное действие [7, 9]. При этом лица, совершающие противоправные деяния, полагали, что их действия были законными.

Судебно-следственная практика по квалификации действий данных лиц складывается неоднозначно. Так, в июле 2023 г. в Воронежской области учительница истории бросила коктейль Молотова в здание Россошанского военкомата. При даче объяснений девушка пояснила, что ей позвонил сотрудник полиции и попросил оказать содействие в задержании преступника. Уголовное дело возбуждено не было. Аналогичная ситуация была совершена в Санкт-Петербурге 53-летним мужчиной, который также заявил о том, что мотивом для совершения преступления послужил телефонный звонок сотрудника МВД с уведомлением его о факте совершенного преступления и возбуждения уголовного дела. Для освобождения от наказания и «исключения его как фигуранта из материалов дела» являлось необходимым поджечь военкомат. Действия лица были квалифицированы по ч. 3 ст. 30, ч. 2 ст. 205 УК РФ [13]. Нередко такие психологические манипуляции заканчиваются гибелью человека. Так, в отношении 76-летнего жителя Всеволожского района г. Санкт-Петербурга

было возбуждено уголовное дело по ч. 1 ст. 167 УК РФ за поджег здания военкомата. При этом пенсионер считал свой поступок оправданным, поскольку целью его действий являлось возвращение суммы денег за квартиру. Не справившись с психоэмоциональным состоянием, мужчина покончил жить самоубийством [16]. Известны случаи переквалификаций действий лиц с ч. 2 ст. 167 УК РФ и ст. 213 УК РФ на п «а» ч. 2 ст. 205 УК РФ [4], при этом у лиц не было основной цели дестабилизировать работу органов государственной власти.

Нарушение сознательной деятельности лица приводит к принятию им бессознательных решений, к психологической зависимости и деструкции личности. Поэтому возникают вопросы относительно уголовно-правовой квалификаций действий лиц, совершивших преступления в следствии информационно-психологического воздействия.

Законодатель не выделяет психологическое принуждение в качестве обстоятельства, исключающее преступность деяния, поскольку считает, что оно всегда является преодолимым явлением. Тем не менее существуют ситуации, когда лицо лишено возможности руководить волей в силу психологического воздействия.

Считаем, что если преступление было совершено лицом, не способным осознать действительное значение совершаемых ими действий [29] в связи с оказанием на него информационно-психологического воздействия (путем манипулирования сознанием, искажая реальную действительность, то лицо, вовлекшее его в совершение преступления, в силу ч. 2 ст. 33 УК РФ должно нести уголовную ответственность за содеянное как исполнитель путем посредственного причинения вреда. Лицо, которое было использовано при выполнении объективной стороны состава преступления, должно быть освобождено от уголовной ответственности.

Приведенный нами анализ, дает основание подвести следующие итоги:

1. Воздействие на информационно-психологическую безопасность личности в сетевом информационном пространстве может осуществляться с помощью различных методов (приемов, форм) и средств, в результате которого искажается представление реальной действительности, затрудняющее формирование и функционирование адекватной информационно-ориентировочной основы социального поведения человека. Вследствие чего участились случаи совершения преступлений экстремистского и террористического характера лицами, которые в результате психологического воздействия сохранили возможность руководить своими действиями, но не осознавали причинно-следственную зависимость между совершаемым деянием и последствиями. Следовательно, умысел лица на совершение преступления исключается.

2. В связи с трудностью и неоднозначностью квалификаций действий лиц, совершающих преступление под информационно-психологическим воздействием, полагаем, что:

а) в случае, если лицо на момент совершения преступления не было способно осознавать противоправный характер своих действий, то оно должно быть освобождено от уголовной ответственности;

б) лицо, вовлекшее его в совершение преступления, в силу ч. 2 ст. 33 УК РФ должно быть привлечено к уголовной ответственности за содеянное как исполнитель путем посредственного причинения вреда.

Список литературы

1. Schmid-Siegel B, Stompe T, Ortwein-Swoboda G. Being a webcam. Psychopathology. 2004 Mar-Apr; 37(2):84–5. doi: 10.1159/000077584. PMID: 15057033. URL: https://pubmed.ncbi.nlm.nih.gov/15057033

2. Takahashi T, Tsukahara Y. Pocket Monster incident and low luminance visual stimuli: special reference to deep red flicker stimulation. Acta Paediatr Jpn. 1998 Dec;40(6):631–7. doi: 10.1111/j.1442–200x.1998.tb02006.x. PMID: 9893306. URL: https://pubmed.ncbi.nlm.nih.gov/9893306

3. Ахатова, А. М. Проблемы уголовно-правовой оценки использования графических изображений (эмодзи, мемов, лайков), комментарий и репостов в сети Интернет при совершении преступлений экстремистской и террористической направленности // Вопросы противодействия экстремистской и террористической деятельности на современном этапе развития войск национальной гвардии Российской Федерации: сб. материалов межвузов. круглого стола с междунар. участием (г. Санкт-Петербург, 13 окт. 2022 г.) / редкол.: Д. В. Новокшонов, Ю. В. Гульбинский, Ю. А. Евстратова. Санкт-Петербург: Изд-во Санкт-Петурбург. воен. ин-та войск нац. гвардии; Белгород: ООО «Эпицентр», 2022. С. 95–102. URL: https://www.elibrary.ru/item.asp?edn=ndiups

4. В Югре фигурантам дела за поджог военкомата обещали через Telegram 1–3 млн рублей. 18.01.2023. URL: https://tass.ru/proisshestviya/16830015

5. Варвара Кошечкина. По соцсетям разошелся фейк про подготовку волны терактов в России // lenta.ru: 21.10.2022. URL: https://lenta.ru/news/2022/10/21/fake_terakt

6. Грачев Г. В. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: РАН. 1999. С. 159. URL: https://search.rsl.ru/ru/record/01000646366

7. Дмитрий Серков. МВД нашло связь между поджогами военкоматов и телефонными мошенниками. 02.08.2023. URL: https://www.rbc.ru/politics/02/08/2023/64ca45769a7947fe52564167

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

9. Илья Пламенев. Суд приговорил к 7 годам срочника за поджог военкомата во Владивостоке. 03.03.2023. URL: https://www.rbc.ru/society/03/03/2023/6401ab0d9a7947bd177c825e

10. Концепция Информационного кодекса Российской Федерации / под ред. И. Л. Бачило. М.: ИГП РА. Изд-во «Канон+»; РООИ «Реабилитация», 2014. 192 с.

11. Лопатин В. Н. Информационное право: учебник. СПб.: ПРОСПЕКТ, 2023. С. 474.

12. Операция ВСУ. Военный Иванников: Украина вербует психбольных для терактов. Аргументы и факты. 04.08.2023. URL: https://dzen.ru/a/ZMx5OtjYH0nmrsMS

13. Пенсионера, пытавшегося поджечь военкомат во Всеволожске, нашли мертвым. 04.08.2023. URL: https://mr-7.ru/articles/2023/08/04/pensionera-pytavshegosia-podzhech-voenkomat-vo-vsevolozhske-nashli-miortvym-news

14. Полубинская С. В., Галюкова М. И. Уголовно наказуемый вред психическому здоровью: содержание и признаки // Актуальные проблемы российского права. 2023. № 3. С. 115–130.

15. Постановление Октябрьского районного суда города Новосибирска от 12.12.2018 по делу № 5–68/2018 // СПС «КонсультантПлюс».

16. Пытавшийся поджечь военкомат пенсионер покончил с собой в Ленобласти. 04.08.2023. URL: https://www.rbc.ru/rbcfreenews/64cca9159a79471bdebb02dc

17. Распоряжение Правительства РФ от 22.12.2022 № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» // СПС «КонсультантПлюс».

18. Решение Арбитражного суда Иркутской области от 17.03.2017 по делу № А19–9523/2016 // СПС «КонсультантПлюс».

19. Решение Арбитражного суда Иркутской области от 28.07.2017 по делу № А19–9525/2016 // СПС «КонсультантПлюс».

20. Решение Дзержинского районного суда города Волгограда от 29.07.2011 по делу № 2–4359/2011 // СПС «КонсультантПлюс».

21. Решение Октябрьского районного суда города Санкт-Петербурга от 30.09.2022 по делу № 2а-3452/2022 // СПС «КонсультантПлюс».

22. Смирнов А. А. Проблемы формирования системы правового обеспечения информационно-психологической безопасности // Труды Института государства и права РАН. 2022. № 5. URL: https://cyberleninka.ru/article/n/problemy-formirovaniya-sistemy-pravovogo-obespecheniya-informatsionno-psihologicheskoy-bezopasnosti

23. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 3. С. 102–111.

24. Тазин И. И. Правовое обеспечение информационно-психологической безопасности несовершеннолетних // Вестник ТГПУ. 2012. № 6(121). URL: https://cyberleninka.ru/article/n/pravovoe-obespechenie-informatsionno-psihologicheskoy-bezopasnosti-nesovershennoletnih

25. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс».

26. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

27. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс».

28. Цыганкова П. В., Бурняшева А. М. Особенности восприятия информационных угроз при параноидной шизофрении // Медицинская психология в России: электрон. науч. журн. 2021. Т. 13, № 1 (66). URL: http://mprj.ru/archiv_global/2021_1_66/nomer07.php

29. Янина И. Ю. Причинение и специальное причинение в уголовном праве: монография / под ред. Н. А. Лопашенко. М., 2019. С. 52–63.

Д. Р. Ахунов,
кандидат юридических наук,
старший преподаватель,
Казанский юридический институт
Министерства внутренних дел Российской Федерации

ПРЕСТУПНОСТЬ В ГОРОДСКИХ АГЛОМЕРАЦИЯХ: МЕЖДУНАРОДНЫЙ АСПЕКТ

Аннотация. Статья посвящена исследованию проблемы предупреждения преступности в городских агломерациях в аспекте международного опыта. Подходы различных государств в профилактике преступности позволяют учитывать особенности современных процессов урбанизации во взаимосвязи с цифровизацией общества, проявляющихся в специфичных условиях современных агломерационных образований. Это определяет возможность применения опережающих тактик и стратегий в предупреждении преступности различных видов в современных городских агломерациях, концентрирующих в себе значительное количество населения и различных ресурсов.

Ключевые слова: предупреждение преступности, городская агломерация, региональная криминология

CRIME IN AGGLOMERATIONS: EXPERIENCE OF FOREIGN STATES

Abstract. The article is devoted to setting the problem of research and crime prevention in agglomerations in the aspect of international experience. The approaches of different states in crime prevention make it possible to take into account the features of modern urbanization processes in relation to the digitalization of society, manifested in the specific conditions of modern agglomeration formations. This determines the possibility of using advanced tactics and strategies in the prevention of crime of various species in modern urban agglomerations, concentrating a significant amount of population and various resources.

Keywords: crime prevention, urban agglomeration, regional criminology

Неотъемлемым качеством развития современного общества являются динамичные процессы урбанизации и цифровизации, активно проявляющиеся в процессах агломерирования территорий. Данные процессы специфическим образом влияют на организацию и устройство социально-экономического, пространства, проявляясь в числе прочего в особенностях преступности.

Действующая система предупреждения преступности не включает в себя особенности агломерирования территории Российской Федерации, что проявляется в отсутствии должных правовых и организационных элементов, механизмов, учитывающих закономерные процессы урбанизации в аспекте профилактики преступности. В то же время особенностью зарубежного опыта в этой сфере является активное государственное регулирование процессов урбанизации и влияние на агломерирование территорий.

Исторический аспект зарубежной практики агломерирования территорий в ряде государств, связанных между собой экономически и политически, указывает на ряд этапов развития рассматриваемых процессов. В их основе преимущественно экономические причины, связанные с развитием промышленного производства и технологий, что, как результат, повлекло изменение системы расселения людей в пользу крупных городов. На примере государств Западной Европы следует выделить три этапа агломерирования территорий:

– довоенный период, характеризующийся активной урбанизацией с перегрузкой сферы строительства и обустройства городского пространства;

– послевоенный период, в котором предприняты попытки устранить негативные последствия первого этапа и выстроить систему регулирования процессов урбанизации;

– современный период, определяющий развитие внутренних пространств и групп пространств [1. С. 45].

Как следует из исторического опыта ряда зарубежных государств на определенном историческом этапе ввиду негативных последствий стихийного агломерирования пространств предпринимаются активные попытки государственного регулирования данных процессов. Это привело к формированию двух форм управления городскими агломерациями – централизованной и децентрализованной, а также двух моделей управления данными образованиями – одно- и двухуровневой [2. С. 10–60] и трех типов управления в зависимости от степени развития исследуемых образований [3. С. 73–78]:

– координационного, предусматривающего управление посредством создания ассоциации в качестве координирующего управленческого органа;

– на основе законодательного закрепления правового статуса ядра агломерации как имеющего приоритет над остальными населенными пунктами в управлении;

– на основе единства органов распорядительной власти и органов управления городской агломерацией.

Современный опыт регулирования урбанизации и цифровизации общественной жизнедеятельности, несмотря на выработанные типовые решения, не имеет универсальной модели [1. С. 43], однако ключевым в данном аспекте является комплексность развития городской агломерации как единой системы, а не суммы элементов. Реализация такого подхода позволяет выделить некоторые особенности урбанизации территории иностранных государств.

Одним из существенных механизмов регулирования процессов урбанизации выступает межмуниципальное сотрудничество в рамках одного агломерационного образования. Результативность и эффективность данного взаимодействия обеспечивается прямым государственным финансированием такого сотрудничества либо финансированием отдельных проектов, направленных, например, на усиление связности территорий муниципальных образований. Активно используется финансовое стимулирование объединения самостоятельных образований в агломерации.

Помимо прямого финансирования взаимодействия муниципальных образований, входящих в городскую агломерацию, активным инструментом регулирования процессов агломерирования является налоговое законодательство, включающее в себя правовые элементы регулирования данных процессов. В частности, подобным образом регулируется соотношение промышленных и рекреационных зон среды

городской агломерации, поскольку прямой вынос объектов промышленности за пределы ядра агломерации в полной мере не обеспечивает их нахождение за пределами самой агломерации либо их размещение в определенных, запрограммированных зонах. Примером подобного регулирования является налоговое законодательство Парижа, которое путем повышения (понижения) налоговых ставок для предприятий отдельных отраслей промышленности на определенных территориях позволило вывести из города отдельные промышленные предприятия [1. С. 45].

Следующим инструментом государственного регулирования агломерирования территорий является правовая легализация подобных образований как самостоятельных административно-территориальных образований с акцентом на экономические особенности, такие как транспортные системы и коммуникации, строительство, финансирование.

Среди европейских государств значительно подвержена процессам агломерирования Федеративная Республика Германия, что обусловлено историческими и экономическими причинами и взаимосвязью с государствами Центральной и Северо-Западной Европы. Особенностью агломераций в ФРГ является активное внедрение механизма межмуниципального сотрудничества в противовес административному объединению муниципальных образований. Примером является Рурская агломерация, расположенная на территории земли Северный Рейн-Вестфалия, объединяющая свыше 10 городов и более 5 млн человек. Деятельность агломерации в части вопросов межмуниципального значения регулируется отдельным законом, который определяет состав, юридический статус объединения, функции агломерации и его органы управления [4. С. 44–45].

Япония является одним из наиболее урбанизированных государство, территория которой – 67 % – занята высокоурбанизированными образованиями. Наиболее крупные мировые агломерации – Токийская, Осакская и Нагойская – объединяют свыше 60 млн человек [5. С. 163]. Развитие агломерационных процессов вокруг столицы Японии – Токио происходило в несколько этапов. Сначала происходило замещение неиспользуемых земель жилой застройкой ввиду социально-экономических запросов. Затем наступил период государственно-частного партнерства, позволивший комплексно развивать городское пространство, субцентры и города-спутники. Включение в эти процессы финансово-промышленных групп сыграло положительную роль, способствуя развитию агломерации. Однако в качестве негативных последствий выразилось перераспределение властных полномочий и централизация местной власти [5. С. 92].

Характерной особенностью процессов урбанизации Соединенных Штатов Америки явился взрывной рост агломераций, субурбанизированных территорий, что привело к укрупнению густонаселенных и экономические развитых городов, например Нью-Йорка, ставшего самой первой агломерацией с численностью населения свыше 10 млн человек [6. С. 92]. В результате функционирования сети агломераций, развитие которых происходило сравнительно неравномерно, они приобрели различные виды, классифицируемые в зависимости от численности проживающего в их центрах населения: микрополитенские ареалы с населением центра агломерации менее 50 тыс. чел, метрополитенские ареалы с населением свыше 50 тыс. человек, которые концентрируют свыше 90 % от общего числа жителей страны, а количество самих населенных пунктов приближается к тысяче –

362 метрополитенских и 560 микрополитенских ареалов с населением в 275 млн человек (93 % населения страны) по состоянию на 2000 г. Последующее развитие агломерационных сетей привело к их преобразованию в сетевые структуры, среди которых можно выделить, например, агломерации Нью-Йорка, Вашингтона, Бостона, Филадельфии и Балтимора, образующих функционально взаимосвязанную сеть. Еще одной особенностью урбанистических процессов США является государственное управление агломерациями. Имеется опыт надмуниципального, полноагломерационного управления, когда создаются самостоятельные органы управления, которые наделяются отдельными полномочиями по решению вопросов, имеющих значение не для конкретного муниципалитета, а агломерации в целом. К числу таких вопросов традиционно относят управление и развитие транспортной и дорожной инфраструктур и управление ими, телекоммуникационную сферу, вопросы маятниковой миграции, экологии. При этом для совершенствования деятельности подобных органов управления и общественного контроля активно привлекаются представители общественности и бизнеса [5. С. 40].

Однако в настоящее время в США начинает преобладать иная региональная классификация подобных образований, в соответствии с которой все штаты делятся на девять субрегионов (например, Новая Англия, Южно-Атлантические штаты), которые, в свою очередь, образуют четыре макрорегиона – Северо-Восток, Северный Центр, Юг и Запад [8. С. 62]. Кроме того, практика урбанизации США свидетельствует о появлении новых, с более высокой ступенью развития агломераций – мегарегионов – объединяющих в себе нескольких агломераций [8. С. 62–63].

Соединенное Королевство Великобритании и Северной Ирландии (Великобритания) также имеет значительный опыт в урбанизации пространств. Ярким примером является Лондон, который к началу XX в. был крупнейшим городом мира, его население к 1921 г. превысило 4,5 млн человек, а к 1939 г. – 8,5 млн человек. Отрицательные последствия стихийного развития города заставили реагировать на это как общество, так и власть [9. С. 184–185].

Контролируемый государством процесс формирования и развития агломераций начался с реформы административно-территориального деления. Для построения каркаса агломераций были выделены графства как центры последующего развития данных образований.

Одним из путей реорганизации в развитии агломераций, который отличает Великобританию от иных государств, стало формирование городов-спутников, расположившихся вокруг агломерационных ядер и находившихся под управлением специализированных органов, наделенных широкими полномочиями в сфере градостроительства и городского планирования. Поэтапно осуществлялись законодательный вывод промышленных предприятий за черту города – центр агломерации, активное ограничение в сфере строительства новых промышленных предприятий, размещение городов-сателлитов на удаленном, до 60 км, расстоянии от ядра агломерации, а также регулировании маятниковой миграции и процессов трудоустройства [9. С. 184–185]. Подобный подход позволил разгрузить как центры агломераций, так и сами агломерации в целом посредством перераспределения соответствующих, в частности антропологических, нагрузок [9. С. 184–185].

Французская Республика также вовлечена в процессы урбанизации. Одной из особенностей развития агломераций во Франции является попытка ухода от формирования крупных центров – ядер – в сторону слияния относительно небольших (с населением до 100 тыс. человек) городов для объединения и спецификации экономических усилий в целях получения синергетического эффекта [7. С. 62]. Этому исторически предшествовал стихийный рост населения в крупных городах, например, в Париже, население которого к началу XX в. достигало свыше 2,5 млн человек [9. С. 184–185]. При этом за довольно незначительный по историческим меркам период Париж пережил этапы как активно выраженной урбанизации, перенаселения города и опустошения пригорода, так и субурбанизации, произошедшей за счет перетока населения из центра в пригород [9. С. 184–185]. Как и в практике иных рассмотренных нами государств, реакцией власти на процессы урбанизации явилось регулирование соответствующих процессов, связанных с активным агломерированием территорий. В частности, одной из регулятивных мер была административная реформа, направленная на механическое сдерживание расширения границ Парижа, объединение и регулирование жизнедеятельности пригорода, ограничение численности населения [9. С. 184–185].

Особенностями агломерирования территорий обладает Китайская Народная Республика. Увеличению числа агломераций в Китае способствовало развитие промышленного производства в крупных городах и в дальнейшем их распространение на близлежащие муниципалитеты. В результате, агломерации Китая сегодня являются основными точками экономического роста [11. С. 177]. При этом как основа развития агломераций активно используется кластерный подход, направленный на концентрацию необходимых ресурсов для повышения экономической эффективности [9. С. 184–185].

Одной из ключевых особенностей развития агломераций в Китае явилось их деление на две группы, ориентированные на внутренний и внешний рынок, что обусловлено особенностью экономического устройства государства. Кроме того, вследствие взрывного промышленно-производственного роста Китая столь же интенсивно росли и агломерации, процессы развития которых фактически не регулировались. Учитывая широкую интеграцию китайской экономики в мировую, развитие агломераций рассматривается здесь через призму развития «внешненаправленных» агломераций с предоставлением широких полномочий в сфере международного сотрудничества и их интеграцию через связь с «внутринаправленными агломерациями» как экономически, так и инфраструктурно. С целью упорядочивания урбанистических процессов и устранения диспропорций развития между «внешненаправленными» и «внутринаправленными» агломерациями государство активно регулирует процессы, связанные с трудовой миграцией и инфраструктурными процессами [11. С. 177].

Зарубежный опыт профилактики преступности применительно к городским агломерациям с учетом описанных особенностей их условий и причинного комплекса свидетельствует о некоторых, существенных аспектах и направлениях в этом.

Выделяют несколько моделей взаимообусловленности преступности и пространства городской среды: на основе социального взаимодействия внутри образуемых городских условий; на основе влияния сосредоточения преступных элементов; на основе взаимообусловленности преступности и экономики [12. С. 62–70].

Одной из тенденций выступает увеличение количества насильственных преступлений, коррелирующих с размерами агломераций. Достаточно эффективно на состоянии преступности сказываются занятость населения и связность территорий, система налогообложения. В то же время за счет концентрации ресурсов полиции в подобных образованиях улучшается раскрываемость. В качестве основной предупредительной тактики используется модель равновесного развития городских агломераций [12. С. 62–70].

Таким образом, действующая система профилактики преступности в современной России не учитывает особенности процессов урбанизации. В этой связи интересным видится опыт ряда зарубежных государств, в которых успешно решаются проблемы агломерирования территорий, в том числе вопросы предупреждения преступности в них. Вопросы устранения негативных аспектов урбанизации решаются на основе управления и моделирования пространства городской агломерации, в частности, моделирования равновесного развития.

Список литературы

1. Процессы урбанизации в контексте закономерностей пространственного развития муниципальных образований, находящихся в зоне влияния крупных мегаполисов / В. В. Окрепилов, С. В. Кузнецов, Н. М. Межевич, М. А. Свириденко // Экономические и социальные перемены: факты, тенденции, прогноз. 2019. № 4.

2. Зотов В. Б. Организация управления и самоуправления в крупнейших городах: современное состояние и проблемы. 2-е изд. испр. и доп. М.: ГУУ; МГУУ Правительства Москвы, 2010. 296 с.

3. Лола А. Принципы управления крупнейшим городом // Регионы: управление и развитие. 1997. № 2. С. 73–80.

4. Победин А. А. Перспективы межмуниципального сотрудничества при развитии городских агломераций: опыт зарубежных стран и России // Вестник ОмГУ. Серия: Экономика. 2013. № 4. С. 44–45.

5. Перцик Е. Н., Кабакова С. И. Особенности структуры урбанизации Японии и формирование технополисов // Инновации и инвестиции. 2016. № 3. С. 40.

6. Развитие московской агломерации с учетом зарубежного опыта. Основные шаги и инновации / Ю. И. Петрова, А. А. Хасунцев, А. Е. Баракин, М. С. Фомина // ТДР. 2014. № 1. С. 163.

7. Алексеев А. Ю., Соколова С. В., Шапошников С. В. Современный опыт формирования городских агломераций // Вестник ГУУ. 2014. № 16. С. 92.

8. Минат В. Н. Урбоориентированное инновационное развитие территорий США // Развитие территорий. 2021. № 3 (25). С. 62.

9. Вешкина Э. Ю. Межрегиональная интеграция как фактор развития социально ориентированной экономики // Социально-политические науки. 2012. № 1. С. 184–185.

10. Ткачев Е. В. Особенности развития агломераций Китая // Гуманитарные, социально-экономические и общественные науки. 2019. № 6. С. 177–180.

11. Колесников А. В. Опыт формирования кластерных агломераций в Китае // Дискуссия. 2012. № 4. С. 46–51.

12. Carl Gaigné, Yves Zenou, Agglomeration, city size and crime, European Economic Review. 2015. Vol. 80. Pp. 62–82.

13. Ахунов, Д. Р. Коррупция в агломерациях и ее предупреждение : уголовно-правовые и криминологические аспекты : на материалах Республики Татарстан: дис. ... канд. юрид. наук: 5.1.4. Казань, 2022.

Д. В. Бахтеев,
доктор юридических наук, доцент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

ПРОБЛЕМЫ OSINT КАК ИСТОЧНИКА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫХ СВЕДЕНИЙ

Аннотация. В статье кратко рассматривается современное состояние следовой информации в сети Интернет, дается характеристика источников информации о личности в сети, рассматривается технология OSINT в контексте следственной деятельности. Заявляет ряд проблем, связанных с этой технологией: соотношение ориентирующего и доказательственного значения получаемой информации, разграничения следственной и оперативно-розыскной деятельности, этика использования информации, полученной в результате утечек и взломов.

Ключевые слова: криминалистика, расследование, цифровая криминалистика, OSINT, интернет-разведка, интернет, цифровые следы

Финансирование: Исследование выполнено при финансовой поддержке УрГЮУ имени В. Ф. Яковлева в рамках реализации проекта ведущей научной школы № 0304/23.

PROBLEMS OF OSINT AS A SOURCE OF CRIMINALISTICALLY RELEVANT INFORMATION

Abstract. The article briefly discusses the current state of trace information on the Internet, characterizes the sources of information about a person in the network, considers OSINT technology in the context of investigative activities. Declares a number of problems associated with this technology: the ratio of the orienting and evidentiary value of the information received, the distinction between investigative and operational-search activities, the ethics of using information obtained as a result of leaks and hacks.

Keywords: forensics, investigation, digital forensics, OSINT, internet intelligence, internet, digital footprints

Деятельность по раскрытию и расследованию преступлений исторически была ориентирована на работу с информацией из любых доступных источников. Если большую часть истории цивилизации сведения о событии преступлениях черпались из материальных источников, то в конце XX в. в жизнь человека доба-

вился новый аспект реальности – информационно-телекоммуникационные сети, в первую очередь – Интернет. Современные статистические исследования показывают, что 88,2 % жителей России регулярно пользуются Интернетом (этот показатель стабильно растет со временем), в среднем проводя в нем 7 часов 57 минут в день. При этом в среднем по планете этот показатель составляет намного меньше – 6 часов 37 минут в день [1]. Разумеется, что это вызвало уменьшение количества следовой информации в материальном мире, однако породило не меньший объем цифровых следов преступников, как связанных с событием преступления, так и характеризующих личность человека в целом. О последнем и пойдет речь в настоящей статье.

Информация о личности человека, действующего в сети Интернет, может быть условно поделена на следующие блоки.

1. Информация, которую пользователь оставляет в Сети добровольно: публикации, статусы, отдельные биографические сведения, в том числе относящиеся к персональным данным: фамилия, имя, отчество, дата рождения, населенный пункт, род занятий, интересы и т. д. Как правило, эти сведения размещаются в социальных сетях, мессенджерах, на форумах в прочих ресурсах, которые напрямую и опосредованно обеспечивают коммуникацию между людьми. В отдельных случаях эти сведения могут индексироваться поисковыми системами.

2. Технические сведения о действиях пользователя в Сети. Сюда относятся IP- и mac-адреса, время подключения, отключения и общая продолжительность действий, логины и пароли, в том числе сведения об их неправильном вводе, операционная система компьютера пользователя, его аппаратная конфигурация и т. д.

3. Сведения из баз данных, полученных в результате взломов и утечек пользовательской информации, хранимой крупными операторами. По данным Лаборатории Касперского, крупные утечки данных российских пользователей происходят в среднем каждый второй день, а во всем мире только за 2022 г. незаконно опубликованы сведения о 197 млн пользователей Интернета [2].

Даже если пользователь прибегает к средствам анонимизации и маскировки в сети, отдельные его следы все же сохраняются и могут быть использованы. Любые сведения могут быть получены двумя способами: активными действиями или пассивным сбором информации. Применительно к следственной деятельности первый способ выражается в направлении запросов, вызове на допрос и т. д. Второй способ предполагает получение информации о человеке или организации так, чтобы этот человек или организация об этом не узнали. Частным случаем пассивного сбора информации является OSINT – Open Source INTelligence – сбор информации из открытых источников. К таким открытым источникам могут относиться в первую очередь, сведения первого рода, т. е. добровольно опубликованные, однако в настоящее время этот подход меняется. Исторически первые методы OSINT использовались для традиционной и финансовой разведки, обеспечения безопасности бизнеса, кадровой деятельности, журналистских расследований [3. С. 30] и пр.

Методы OSINT могут быть дифференцированы следующим образом.

Сведения, полученные с помощью поисковых систем. Для этого можно использовать операторы поиска, а также дорки – заранее сформированные поисковые запросы. К примеру, дорк «index of /wp-content/uploads/shell.php» может показать

оглавление базы загрузок внешних файлов сайта на WordPress. К настоящему времени в Сети существуют большие библиотеки дорков, которые могут использованы как для криминальной, так и для правоохранительной деятельности. Следует также упомянуть поисковую систему Shodan.io, оптимизированную для технического мониторинга Интернета.

Интернет-сервисы, такие как whois и Internet Archive. С помощью первого может быть получена информация о владельцах веб-сайта, времени его регистрации и т. д. С 2020 г. персональные данные физических лиц- владельцев российских сайтов скрываются, однако таким образом все еще можно получить данные об электронной почте владельца сайта и хостинг-провайдере. Проект Internet Archive (https://archive.org/web/web.php) кэширует страницы сайтов в Сети с разной периодичностью. Это может оказаться полезным при расследовании преступлений, совершенных с помощью фишинговых сайтов.

OSINT-сервисы, целенаправленно агрегирующие информацию: сервисы проверки контрагентов (например,. https://www.rusprofile.ru/), разнообразные проекты в форме веб-сайтов, мобильных приложений, приложений на персональный компьютер, телеграм-ботов и т. д., которые могут собирать и выдавать информацию о человеке вплоть до того, когда и каким рейсом он путешествовал, в какой клинике лечится его кошка и какие файлы он скачивал.

OSINT-методы предполагают, что для первичного поиска требуются какие-то, пусть даже фрагментарные сведения об искомом объекте. Это может быть имя человека, его псевдоним (никнейм), заинтересованность в чем-либо. К примеру, для поиска преступника, использовавшего для совершения преступления пневматическое оружие, можно изучить информацию на местных форумах, на которых обсуждают характеристики данной категории предметов. Как правило, в упомянутых в п. 3 методах для инициирования поиска используются ФИО, номер телефона, госномер автомобиля, никнейм или почта пользователя.

Несмотря на очевидную эффективность методов OSINT, их использование сопряжено с рядом проблем.

Первая касается характера собираемых таким образом сведений. Учитывая пассивный характер сведений, собираемых с помощью OSINT, они могут являться лишь ориентирующими, но не доказательственными, поскольку отсутствует прямая доказательственная связь между человеком (организацией) и полученными сведениями. Учитывая востребованность OSINT-методов в разных отраслях человеческой деятельности и большую конкуренцию на рынке разработчиков этих методов, их следует считать достаточно точными, однако OSINT может быть использован исключительно для «выдвижения версий, определения направлений расследования, планирования следственного действия, прогнозирования возможной линии поведения участников уголовного процесса и возможного противодействия расследованию» [4. С. 135], но не для, например, предъявления обвинения.

Второй дискурс относится к вечно зыбкой границе между следственной и оперативно-розыскной деятельностью. Учитывая пассивность методов OSINT и их открытость, их нельзя в полной мере отнести к оперативно-розыскной деятельности. Однако после получения, сведения нужно проверить, к примеру, написать на ставший

известным адрес электронной почты. Это уже будет активным действием, поэтому отнести его в полной мере к OSINT нельзя. Это создает своеобразную коллизию: для того чтобы задействовать OSINT, нужно располагать первичной информацией, т. е. в процессе этого задействования ее качественные и количественные характеристики должны увеличиться, при этом требуется идентификационное соответствие между первичной и полученной информацией, которое, в свою очередь, не может быть проверено этими же методами.

Третья проблема находится в плоскости этики: как ранее отмечалось, значительная часть источников, обрабатываемых методами OSINT, была сформирована в результате утечек пользовательских данных и целенаправленных хакерских атак. Так, упомянутая поисковая система Shodan.io содержит, помимо прочего, сведения об открытых информационных системах, которые стали таковыми в результате взлома. Уже проводятся исследования, демонстрирующие одновременно потребность в таких методах и страх относительно их некорректного использования [5]: 66 % опрошенных считают, что организации и органы государственной власти могут повысить свою эффективность с помощью OSINT, 24 % опрошенных считают эту ситуацию для себя проблемной. Насколько корректно современному следователю пользоваться такими сведениями – вопрос открытый.

Подводя итог, отметим, что распространение методов OSINT в криминалистической практике еще только начинается, их изучение и апробация становятся задачами ближайшего будущего криминалистической науки. Как и любая другая технология, OSINT не должна использоваться бездумно. Изучать необходимо не только то, каким образом работают эти методы, но источники соответствующей информации.

Список литературы

1. Digital 2023. Global overview report. URL: https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Global-Overview-Report.pdf

2. Значимые утечки данных в 2022 году. URL: https://go.kaspersky.com/ru-data-leakage-report-2022

3. Головин А. Ю., Головина Е. В. К вопросу собирания криминалистически значимой информации по открытым цифровым данным // Актуальные проблемы криминалистики и судебной экспертизы: сборник материалов Международной научно-практической конференции, Иркутск, 16–17 марта 2023 года. Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2023. С. 29–32.

4. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.

5. Riebe T. Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey // In book: Technology Assessment of Dual-Use ICTs. 2023. Pp. 221–248.

И. Р. Бегишев,
доктор юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
В. В. Денисович,
кандидат юридических наук, доцент,
Челябинский государственный университет

МЕТАВСЕЛЕННЫЕ В УГОЛОВНО-ПРАВОВОМ ИЗМЕРЕНИИ

Аннотация. В статье сквозь призму уголовного закона исследуются метавселенные. Предлагается полностью пересмотреть структуру объектов уголовно-правовой охраны и специфику привлечения к уголовной ответственности лиц, обладающих специальными познаниями в сфере разработки продуктов достижений цифровых технологий. Предлагается внести соответствующие изменения в Уголовный кодекс Российской Федерации.

Ключевые слова: метавселенные, кибепространство, виртуальные миры, цифровые миры, аватар, блокчейн, киберпреступления, преступления

METAVERSES IN THE CRIMINAL DIMENSION

Abstract. In this paper, metaverses are examined through the prism of criminal law. It is proposed to completely revise the structure of objects of criminal law protection, as well as to analyze the specifics of bringing persons to criminal responsibility who have special knowledge in the field of product development of digital technologies, to make appropriate changes to the structure of articles of the Special Part of the Criminal Code of the Russian Federation.

Keywords: metaverses, cyberspaces, virtual worlds, digital worlds, avatar, blockchain, cybercrimes, crimes

В современном мире о метавселенных говорят достаточно часто и вполне обоснованно. Новая виртуальная среда позволяет не только общаться, но и работать, осуществлять совершенно любой вид деятельности, с которой знаком человек. Однако данные процессы должны быть подконтрольны закону, в том числе уголовному. В любой метавселенной возможно совершение преступления тогда, когда в ней свою деятельность осуществляет человек. Это аксиоматичный вывод, который соответствует понятию преступления, закрепленному в статье 14 Уголовного кодекса Российской Федерации. Одной из ключевых проблем является понятие самой метавселенной, выделение ее видов, определение видов деятельности, которые подпадают под сферу регулирования уголовного закона.

В этом прогрессивном виртуальном мире у каждого пользователя – не привычные многим фотографии профилей, а необычные 3D-аватары. Плоские страницы браузера в метавселенной отсутствуют, им на смену пришли объемные интерфейсы. В этом пространстве люди могут прожить совершенно иную жизнь, отличную от происходящего в их реальности. Цифровой мир предлагает научиться чему-то новому, заработать криптовалюту, потратить ее на покупку виртуальной недвижимости и т. д. [1].

Как известно, активно развивать идею метавселенных для обычных пользователей сети Интернета стал Марк Цукерберг. С этого периода времени начались активные разработки технических гаджетов, программ, видеоигр, которые создают уникальные технические возможности «соединить человека» с его аватаром в игре или программе, передают мимику, жесты, эмоции, позволяют улучшать возможности такого аватара за счет вложения конкретных финансовых денежных средств собственника аватара. Проблема правоприменительной практики состоит в том, чтобы разграничить понятия «метавселенная», «цифровое пространство», «Интернет», «виртуальное пространство», «киберпространство». Каждый термин имеет свое юридическое содержание и должен иметь свой механизм правового регулирования. Когда речь идет о нарушении нормы права, возникают вопросы, какой нормы, где нормативный акт, а следовательно, где и какая группа отношений требует регулирования. Специалисты в области уголовного права в любом случае зададут вопрос о наказании и возможности привлечения к уголовной ответственности. Но встречным вопросом будет, а как доказать, что было совершено преступление, и самое главное, а разве кому-то что-то угрожает? Виртуальная среда – это особый мир, который на сегодняшний день определен рамками сознания человека.

Именно с вопросов терминологии необходимо начинать изучать метавселенные и виртуальное пространство, а также с принципов самого киберпространства: постоянства; доступности; замкнутого типа экономики; синхронности. Основная задача разработчика на сегодняшний день – не только развлечь человека, но и расширить его возможности, позволить человеку выйти на новый уровень производства, уровня жизни, мыслительной деятельности.

Суть метавселенной настолько глубока, что многие уверены в ее способности к разрешению значимого числа сложностей человеческого общества, что вызывает немало дискуссий: снижение процента населения людей с малоподвижным образом жизни, расширение круга общения, сокращение расстояния между людьми для общения, контроль за состоянием здоровья, появление новых видов экономических отношений (блокчейн).

Виртуальная своего рода «экосистема» [5], которая формируется в метавселенных, включает право собственности и другие юридически регулируемые отношения (процесс регулируемого налогообложения, обычное «пиратство»). Для метавселенных актуален вопрос создания пользовательского контента с использованием результатов чужого интеллектуального труда, а также чит-кодов, т. е., по сути, неавторизованной модификации игр [2]. Кроме того, метавселенные нуждаются в обеспечении своей информационной безопасности [7].

Вопрос защиты персональных данных встает особенно остро в связи с ростом их оцифрованного объема по мере погружения в метавселенные. Роскомнадзор, а также иные правоохранительные органы высказывают справедливые опасения о возможном «искажения привычных этических норм через понимание, что такое аватар человека и правовая реальность».

Следующая группа проблем внедрения метавселенных в современную реальность связана с пониманием людьми их «полезности». Сами технологии достаточно дорогие, технические возможности многих компаний и подготовка специалистов требуют все новых и новых достижений. Наблюдаются сложности в сотрудничестве

продуктов IT-корпораций, неподготовленность пользователей к другим форматам взаимодействия в цифровой среде. Положительные стороны в активном времяпрепровождении в метавселенных не очевидны большинству пользователей. Однако, с каждым годом процесс заинтересовавшихся метавселенными растет.

Реальность такова, что человек уже сейчас учиться балансировать между цифровым и физическим миром. Важно, чтобы метавселенная не стала ни для кого причиной потери связи с реальностью и фактическими требованиями закона. Нужно быть готовыми к тому, что инновации могут привести людей к еще большим проблемам с их нервной системой. Количество киберпреступлений и утери конфиденциальной информации многих жителей планеты будет только расти. Решение очевидно в данном случае – внедрение понятия метавселенных в уголовно-правовое пространство, определение классификации совершенно новых объект уголовно-правовой защиты в сфере цифровых технологий.

В метавселенной стираются границы. Главное – не стереть границы между дозволенным и не дозволенным поведением. Проблема идентификации аватаров также делает уязвимыми личность и личные данные для копирования, стирания и манипулирования [3]. Кроме того, как отмечают некоторые авторы, существование криптовалют таит в себе условия для создания виртуальных магазинов, занимающихся реализацией запрещенных или ограниченных в обороте веществ, услуг и неконтролируемого распространения персональных данных, возможности их копирования [4].

Разработчики метавселенных могут умышленно, а также по неосторожности создать условия для подрыва экономической, политической и социальной, культурной безопасности государства, как в случае легализации и урегулирования общественных отношений в виртуальном пространстве. Неосторожно такие деяния могут совершены в силу элементарного незнания закона, хотя это и не освобождает от ответственности. Возникает вопрос о контроле за деятельностью людей, которые реализуют свои возможности и пожелания в метапространстве.

В судебной практике уже имеются факты уклонения от налогообложения за доход, полученный в цифровом пространстве. Согласно определению Верховного Суда Российской Федерации от 30 сентября 2015 г. по делу № А40–91072/2014, общество с ограниченной ответственностью «Мэйл.РуГеймз» наделило пользователей возможностью использования дополнительного функционала игры за отдельную плату, компенсируемую путем перечисления денежных средств через агрегаторы платежей [6].

В первой части статьи мы говорили о необходимости изменить систему объектов уголовно-правовой охраны с учетом развития цифровых технологий. Однако следует пересмотреть и понятие специального субъекта в уголовном праве. Множество специалистов в сфере IT-технологий так или иначе связаны с виртуальным пространством, обладают особыми знаниями в области использования технологий искусственного интеллекта, но как привлекать к уголовной ответственности каждого из них, если речь идет о пользователе продукта цифровой технологии и его разработчике. Следует внимательно отнестись к современному рынку труда IT-специалистов и определить требования и критерии специального субъекта, который будет нести уголовную

ответственность за создание программ и цифровых продуктов, создающих угрозу безопасности человека.

Существует также и проблема квалификации отдельных деяний, совершенных в метавселенной: преступления против половой свободы и половой неприкосновенности, экономические преступления, преступления против безопасности дорожного движения и т. д.

Основным выводом, к которому мы приходим уже сейчас является тот факт, что любые новые отношения нуждаются в правовом регулировании на стадии их возникновения, а не на стадии, когда уже возникло правонарушение и его надо предупреждать и осуществлять в отношении него меры профилактики. Метавселенные уже существуют, в них совершаются сделки, люди общаются и приобретают имущество, следовательно право человека может быть нарушено в любой момент [1]. Это крайне важный вопрос для уголовно-правовой науки и практики.

Крупные компании, разработчики метавселенных стремятся в первую очередь защитить личные границы пользователей. Следовательно мы уже говорим о защите личности как об объекте уголовно-правовой охраны в киберпространстве. В целом администратор площадки или разработчик приложения традиционно несет ответственность за поддержание уважительного общения. Но для некоторых проблем правового решения пока нет. Главные из них – баланс между анонимностью и раскрытием данных, а также определение юрисдикции в виртуальном пространстве [1].

Такие нематериальные ценности, как честь, достоинство, авторские права, будут требовать классических способов правовой защиты, а уголовные составы типа доведения до самоубийства или пропаганды наркотиков останутся актуальными и в виртуальном мире.

Остается открытым вопрос о способах охраны персональных данных. Их значимость будет увеличиваться: если человек будет работать, отдыхать и вообще много времени проводить в этом виртуальном мире, злоумышленники могут фактически получить доступ к его частной жизни.

В вопросе анонимности и защиты персональных данных баланс, вероятно, сместится в сторону их раскрытия. Это объясняется и последними тенденциями ко все большему регулированию, в том числе в форме так называемых ковидных паспортов, и со все возрастающим количеством информации, которую популярные платформы собирают о пользователях [3].

Токенизация объектов с использованием блокчейна теперь впервые приближается к тому, что мы понимаем как собственность в реальном мире: создание уникального актива, который нельзя воспроизвести по желанию. Вопрос о том, могут ли токены на основе блокчейна, такие как NFT, действительно быть собственностью по смыслу закона, или же положения закона о собственности, по крайней мере, применимы к токенам, сегодня все еще горячо обсуждается и еще не решено [4]. Это утверждение является основным тезисом для разработки и новых составов преступлений против собственности и преступлений в сфере экономической деятельности.

Таким образом, можно заключить, что нам необходимо полностью пересмотреть структуру объектов уголовно-правовой охраны, а также проанализировать специ-

фику привлечения лиц к уголовной ответственности, обладающих специальными познаниями в сфере продуктов достижений цифровых технологий, внести соответствующие изменения в структуру статей Особенной части Уголовного кодекса Российской Федерации с целью не допустить нарушения прав человека.

Список литературы

1. Алабина Т. А., Дзангиева Х. С., Юшковская А. А. Метавселенная как глобальный тренд экономики // Экономика, профессия, бизнес. 2022. № 1. С. 5–8. DOI: 10.14258/epb202201

2. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7–32. DOI 10.21202/jdtl.2023.1. EDN LCCOJJ.

3. Каспарьянц Д. Метавселенная: возможности и риски новой реальности / Научно-технический центр ФГУП «Главный радиочастотный центр». URL: https://rdc.grfc.ru/2022/02/metaverse

4. Метавселенная: какие юридические вопросы нас ждут с новым трендом виртуального пространства. URL: https://myrealearnings.ru/cryptocurrency/metavselennaja-kakie-juridicheskie-voprosy-nas-zhdut

5. Мурсалимов А. Т. Метавселенна. новое пространство совершения мошенничества в сфере кредитования // Вестник Казанского юридического института МВД России. 2023. Т. 14, № 1(51). С. 118–123. DOI: 10.37973/KUI.2023.58.37.015

6. Определение Верховного Суда Российской Федерации от 30.09.2015 по делу № А40–91072/2014 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/vsrf/doc/cgF6SCz4z9NP

7. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. DOI 10.21202/jdtl.2023.28. EDN FISEET.

Л. В. Бертовский,
доктор юридических наук, профессор,
Московский институт электронной техники
Г. С. Девяткин,
кандидат юридических наук, доцент,
Московский институт электронной техники

МЕТАВСЕЛЕННЫЕ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В УГОЛОВНОЕ СУДОПРОИЗВОДСТВО

Аннотация. Развитие высокотехнологичного права невозможно без внедрения высокотехнологичных инструментов в судопроизводство. В российских судах доступны опции дистанционной подачи исковых заявлений, которые могут быть рассмотрены дистанционно в некоторых случаях, а также получение судебного

решения, подписанного судьей с помощью электронной цифровой подписи. Однако наиболее чувствительной и требующей правового регулирования является сфера уголовного судопроизводства, где меньше всего используются высокотехнологичные инструменты. Перспективы использования метавселенных и технологий виртуальной реальности судами при рассмотрении дел является одной из самых обсуждаемых тем. Необходимо проанализировать правовые аспекты таких механизмов с учетом сформировавшегося зарубежного опыта.

Ключевые слова: метавселенная, виртуальная реальность, уголовное судопроизводство, принципы судопроизводства, высокотехнологичное право, верификация, искусственный интеллект

METAVERSE AND PROSPECTS FOR THE INTRODUCTION OF VIRTUAL REALITY TECHNOLOGIES IN CRIMINAL PROCEEDINGS

Abstract. The development of high-tech law is impossible without the introduction of high-tech tools in legal proceedings. In Russian courts, options for remote filing of claims are available, which can be considered remotely in some cases, as well as obtaining a court decision signed by a judge using an electronic digital signature. However, the most sensitive and requiring legal regulation is the sphere of criminal proceedings, where high-tech tools are least used. Prospects for the use of metaverses and virtual reality technologies by courts when considering cases is one of the most discussed topics. It is necessary to analyze the legal aspects of such instruments, taking into account the established foreign experience.

Keywords: metaverse, virtual reality, criminal proceedings, principles of legal proceedings, high-tech law, verification, artificial intelligence

Цифровизация судопроизводства в России и в мире в целом происходит с отставанием на 5–7 лет от остальных институтов общества и государства, за исключением некоторых стран и территорий. В период с 2010 по 2023 г. произошло в российском судопроизводстве несколько ключевых изменений, связанных с внедрением высоких технологий. Так, в 2010 г. появилась информационная система «Кад.Арбитр», позволившая уже на тот момент дистанционно знакомиться с судебными актами, размещенными на данной платформе. Это был действительно революционный шаг в цифровизации. После первоначального внедрения системы «Кад.Арбитр» произошло несколько ее обновлений, что позволило в 2021 г. подавать исковые заявления и документы в суд дистанционно с верификацией через «Госуслуги» либо электронной цифровой подписи (далее – ЭЦП), а также участвовать в судебном заседании при помощи видеоконференцсвязи. По уголовным и гражданским делам, рассматриваемым в судах общей юрисдикции, участвовать в деле дистанционно возможно, но с некоторыми ограничениями: участнику гражданского судопроизводства потребуется явиться в здание суда, где его подключат к видеоконференцсвязи с судом, рассматривающим его дело. Для уголовного судопроизводства видеоконференцсвязь будет использоваться в самую последнюю очередь, предоставляя приоритет очному присутствию всех участников в зале суда (за исключением случаев,

когда осужденный уже отбывает наказание, связанное с лишением свободы, и чаще используется дистанционное подключение из исправительного учреждения).

Таким образом, если проецировать высокие технологии в судопроизводство в России, то самыми «технологичными» являются арбитражные суды, где возможен полный цикл: дистанционная подача иска, участие в рассмотрении дела и получение решения, подписанного судьей при помощи ЭЦП. В уголовном судопроизводстве по состоянию на первое полугодие 2023 г. такие инструменты пока не применяются.

Итак, насколько высокотехнологично судопроизводство в России? Является ли чем-то «высокотехнологичным» использование обычной веб-камеры и дистанционной трансляции из зала суда? С учетом активного распространения в мире нейросетей по типу ChatGPT, цифровых пространств для виртуальных объектов (метавселенных), а также иных технологий, обычная видеоконференцсвязь едва ли может считаться высокотехнологичным решением в 2023 г. В этой связи интересен опыт суда в Колумбии, который в феврале 2023 г. первым среди всех стран провел официальное судебное заседание в метавселенной [1]. Не считая небольших искажений движений аватаров, никаких проблем замечено не было.

На двухчасовом слушании присутствовали аватары сторон конфликта и аватар главы магистрата Марии Хинонес Трианы в черной мантии. Все прошло довольно удачно, велась прямая трансляция, и по мнению судьи, это было даже более реально, чем видеозвонок, так как во время обычных видеоконференций люди имеют обыкновение выключать камеры. Следует отметить, что данное заседание было проведено с соблюдением всех требований законодательства [2].

В России опыт судов Колумбии безусловно необходимо принимать во внимание. Еще в 2021 г. Президент России В. Путин указывал на необходимость развития метавселенных в различных отраслях экономики, медицины, образования. Судебная система нуждается в активном внедрении высоких технологий. Средний срок рассмотрения, например, гражданского дела в России составляет более четырех месяцев с момента регистрации искового заявления до фактического вынесения решения судом (не учитывая дополнительный срок для обжалования). При этом нагрузка на судей колоссальная, в 2022 г. было рассмотрено более 40 миллионов дел, хотя еще в 2018 г. – на четверть меньше [3]. По уголовным делам сроки рассмотрения могут достигать шести месяцев и более.

Цифровизация судопроизводства в России представляет собой комплекс нормативно-правовых изменений в совокупности с техническими решениями. Однако и этого будет недостаточно. Цифровизация невозможна без наличия сформированного высокотехнологичного права, определение которого Л. В. Бертовский описал, как логистичный, наукоемкий и технологичный регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой – регламентирует возникающие с ними отношения [4].

В целом, развитие ИИ-технологий в России идет по четырем направлениям: «обработка естественного языка и синтез речи», «компьютерное зрение», «перспективные методы искусственного интеллекта» и «интеллектуальная поддержка принятия решений» [5]. К основным направлениям развития цифрового судопроизводства можно отнести: нормативное регулирование, кадры и образование, форми-

рование исследовательских компетенций и технических заделов, информационную инфраструктуру и безопасность.

Анализ действующего законодательства в совокупности с проблемами правоприменителя позволяет выделить следующие вопросы, требующие проработки перед возможностью поэтапного внедрения опыта судов Колумбии:

– обеспечение прав участников судопроизводства;
– реализация принципов судопроизводства;
– формирование судебной инфраструктуры;
– обеспечение техническими требованиями.

Проведение судебного заседания в метавселенной (или иной другой виртуальной реальности), с одной стороны, может не обеспечивать право на доступ к правосудию определенных категорий населения в труднодоступных местностях, с другой стороны, решается проблема так называемых «секретных» свидетелей по уголовному делу. В действующем законодательстве допускается такой порядок участия. В этом случае следователь (дознаватель, прокурор, суд) выносит постановление о сохранении в тайне данных о личности (фамилии, имени, отчестве, месте и дате рождения), которое упаковывает в конверт, опечатывает и в таком виде приобщает к делу. Вскрыть конверт может только лицо, засекретившее участника процесса, и суд – для всех остальных данные должны быть недоступны.

Но при засекречивании свидетелей у подсудимого фактически не обеспечивается право задать вопрос свидетелю в зале суда, визуально наблюдая за этим свидетелем. Поместить всех участников уголовного дела в общую виртуальную комнату позволит им находиться в относительно равных условиях. Кроме того, будет решен вопрос участия потерпевших по делам, связанных с изнасилованиями. Не всегда удается провести допрос в зале суда женщины или несовершеннолетней об обстоятельствах преступления, доставляющих им моральные страдания.

Также существует проблема лиц с ограниченными физическими возможностями, присутствие которых в зале суда может доставлять им особые неудобства. Безопасность лиц, задействованных в проведении судебных заседаний, является актуальной проблемой. Происходят ситуации, когда подсудимые нападают на конвой, пытаются скрыться в вентиляции здании судов, нападают на судей, пытаются пронести в здание суда холодное и огнестрельное оружие. Метавселенная в суде позволит практически полностью это исключить.

Обеспечение принципов судопроизводства – одна из ключевых проблем перед проведением заседания в виртуальной реальности. Согласно действующему законодательству к принципам отнесены: гуманность; справедливость; законность; презумпция невиновности; осуществление правосудия только судом; независимость судей; гласность; равноправие (состязательность); разумный срок судопроизводства; право на обжалование.

При проведении заседания в метавселенной перспективна реализация принципа разумного срока судопроизводства. Скорость рассмотрения дел существенно повысится, не потребуется месяцами ожидать свидетелей, собрать всех в виртуальной реальности будет доступнее. Интересен опыт судов Республики Казахстан, которые активно внедряют высокие технологии в судопроизводство. Заслуживает внима-

ния принцип экстерриториальной подсудности, введенный в действие 1 августа 2022 г. Согласно нему, участники процесса вправе судиться не в месте своего географического проживания, а в любом другом суде Казахстана. В какой суд попадет спор определяет роботизированная программа, которая не делит суды на районы и области. В итоге должна выровняться нагрузка судей, которая в крупных городах превышает объем сельских районов в десятки раз [6].

Однако будет ли являться рассмотрение судом дела в метавселенной реализацией принципа осуществления правосудия только судом? Анализ статьи 8 Уголовно-процессуального кодекса и статьи 19 Конституции предполагает, что никто не может быть признан виновным в совершении преступления и подвергнут уголовному наказанию иначе как по приговору суда и в порядке, установленном законом. В привычном понимании судья – профессиональный юрист, наделенный судебной властью, который отправляет правосудие в специально предусмотренных зданиях, например, районных судах. Кроме того, предусмотрен особый порядок, предусматривающий правила поведения в зале суда. Согласно статьи 158 Гражданско-процессуального кодекса (далее – ГПК):

1. «При входе судей в зал судебного заседания все присутствующие в зале встают. Объявление решения суда, а также объявление определения суда, которым заканчивается дело без принятия решения, все присутствующие в зале заседания выслушивают стоя.

2. Участники процесса обращаются к судьям со словами: «Уважаемый суд!», и свои показания и объяснения они дают стоя. Отступление от этого правила может быть допущено с разрешения председательствующего.

3. Судебное разбирательство происходит в условиях, обеспечивающих надлежащий порядок в судебном заседании и безопасность участников процесса».

Исходя из этого, можно сделать вывод, что заседания должны проводиться в зале суда, но это не всегда так. С 2021 г. допускается проведение онлайн-заседаний при помощи видеоконференцсвязи. При этом Верховный Суд не усмотрел в этом нарушение какого-либо принципа судопроизводства. Необходимы технические гарантии проведения такого заседания, а также верификация личности участника. На практике онлайн-идентификация личности при рассмотрении дел в арбитражном суде происходит путем демонстрации в веб-камеру паспорта. Естественно, подлинность такого паспорта установить «на глаз» непросто, однако и при обычном офлайн-заседании проверка паспорта секретарем судебного заседания происходит без специального оборудования.

При решении вопроса об обеспечении принципа осуществления правосудия только судом при использовании виртуальной реальности в качестве платформы для рассмотрения дела, но с привлечением профессионального судьи для рассмотрения по существу, следует исходить из общих целей судопроизводства. Например, статья 2 ГПК РФ ключевой задачей ставит «правильное и своевременное рассмотрение и разрешение гражданских дел». Это ставится выше, чем правило рассмотрения дел в здании суда путем соблюдения определенных общих технических процедур. Если все участники согласны на дистанционный формат в виртуальной реальности с одновременным решением многих проблемных аспектов (разумный срок, безо-

пасность лиц, доверие суду и т. д.), задачи судопроизводства будут решены, что также подразумевает обеспечение его принципов.

Безусловно судебные заседания в метавселенной или любой иной виртуальной реальности столкнутся с серьезной проблемой доказывания при рассмотрении и разрешении уголовных дел. Как справедливо отмечает Л. А. Воскобитова, уголовное судопроизводство – это деятельность, осуществляемая при взаимодействии людей, она прежде всего вырабатывает социальные технологии и формирует определенный набор методов, средств, приемов такого взаимодействия, обеспечивая достижение целей данной деятельности [7].

Полноценное взаимодействие людей через виртуальную реальность пока сложно представить. Судопроизводство – живой, динамичный механизм с наличием определенных тактических законных приемов, применяемых участвующими сторонами, которые реализуемы именно в офлайн-заседании. Однако метавселенная позволит реконструировать событие преступления, отдельные его эпизоды. Участники уголовного судопроизводства смогут буквально находиться в квартире, где произошло убийство для детального погружения в произошедшее. Особенно это актуально для судов с участием присяжных заседателей.

Возможности метавселенных в уголовном судопроизводстве обширны, выделим некоторые из них:

– проведение допроса несовершеннолетних и иных категорий;
– проведение судебных заседаний по отдельным преступлениям;
– моделирование эпизодов преступлений;
– проведение следственного эксперимента;
– совмещение процесса проведения с нейросетью;
– обеспечение безопасности «секретных свидетелетей» и иных участников.

Проблема цифрового неравенства и доступа к правосудию будет решена путем создания специальных аккредитованных помещений для доступа к судебному заседанию в виртуальной реальности. Это можно сравнить с наличием центров «Мои документы» и многофункциональных центров (МФЦ) на территории России. Участник судопроизводства получит ID номер, включающий анализ его профиля (голос, поведенческие характеристики, отпечаток пальца, сканирование сетчатки глаза), позволяющий сформировать уникальный цифровой профиль для идентификации его судом. Фактически это процедура удостоверения личности секретарем судебного заседания путем предъявления участником своего паспорта. Однако переклейка физического паспорта на подставное лицо не является сложной задачей для преступного мира (по разным данным, стоимость варьируется от 100 до 150 тысяч рублей). Создание цифрового профиля участника с привязыванием к нему биометрии, уникальных поведенческих признаков выглядит более надежным способом. Искусственный интеллект способен распознавать эмоции человека, что позволит устанавливать тревожность, страх участника по делу, что может косвенно означать применение к нему воздействия со стороны третьих лиц.

Исключительно судья будет вправе определять возможность проведения заседания в виртуальной реальности при обязательном согласии всех участников и анализе совокупности условий: сложности дела, количестве лиц, безопасности,

цифрового неравенства. Если хотя бы один из участников выступает против такой формы, то заседание должно быть проведено в привычной форме. Однако в этом случае не в полной мере могут быть использованы технологии для воспроизведения события преступления, возможные при погружении участников в виртуальную реальность. Также возникает справедливый вопрос о фиксации судебных заседаний в протоколе и ознакомлении с ним участников, ранее не принимавших участие в деле (замена адвоката, новые свидетели и т. д.). Поэтапное экспериментальное внедрение судебных заседаний в виртуальной реальности возможно для некоторых категорий гражданских и административных дел с так называемым «отсутствием спора о праве», по уголовным делам небольшой тяжести – при согласии обвиняемого с предъявленным обвинением.

Список литературы

1. Colombia court moves to metaverse to host hearing. URL: https://www.reuters.com/world/americas/colombia-court-moves-metaverse-host-hearing-2023–02–24

2. Plan Nacional de Desarrollo 2018–2022 «Pacto por Colombia, pacto por la equidad. URL: https://www.dnp.gov.co/DNPN/Paginas/Plan-Nacional-de-Desarrollo.aspx; EY 1564 DE 2012 «Por medio de la cual se expide el Código General del Proceso y se otras disposiciones».El Congreso de la República. URL: https://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/ley_1564_de_2012_codigo_general_del_proceso.pdf.

3. Судебная статистика Судебного департамента при Верховном Суде Российской Федерации. URL: http://cdep.ru

4. Бертовский Л. В. Высокотехнологичное право: понятие, генезис и перспективы // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2021. Т. 25, № 4. С. 735–749.

5. Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект». URL: https://digital.gov.ru/ru/documents/6658/?utm_referrer=https%3a%2f%2fwww.kommersant.ru%2f

6. Ахметзакиров Н. Р. Элементы искусственного интеллекта и роботизация в судопроизводстве: тренды и перспективы // Материалы Международной научно-практической конференции «Искусственный интеллект и большие данные (Big Data) в судебной и правоохранительной системе: реалии и требование времени». URL: https://academy-gp.kz/?p=17660&ysclid=ljzg5kqmxr512893482&lang=ru

7. Воскобитова Л. А. Трансформация доказывания в условиях цифровизации уголовного судопроизводства // Материалы Международной научно-практической конференции «Искусственный интеллект и большие данные (Big Data) в судебной и правоохранительной системе: реалии и требование времени». URL: https://academy-gp.kz/?p=17660&ysclid=ljzg5kqmxr512893482&lang=ru

Л. В. Бормотова,
кандидат юридических наук,
доцент кафедры уголовного процесса и криминалистики,
Оренбургский государственный университет

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОИЗВОДСТВЕ ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация. Цифровая трансформация в основных сферах жизнедеятельности стала не только благом, но и новым каналом проникновения правонарушений и преступлений в условиях несформированного импортозамещения программными продуктами и технологиями отечественного производства. При этом наблюдается отсутствие адекватного ответа со стороны правоохранительных органов, поскольку процесс цифровизации выявления и раскрытия преступлений находится на низком уровне. В декабре 2022 г. уголовно-процессуальное законодательство было дополнено новыми средствами процесса доказывания на этапе досудебного производства: получение показаний лиц и процедура избрания меры пресечения допускаются с применением видеоконференцсвязи. В исследуемой сфере преступления обладают высокотехнологичными способами совершения. Такие угрозы возможно нейтрализовать только аналогичными средствами и методами. В настоящей работе рассмотрен вопрос о возможности создания особого цифрового подхода в ходе производства по уголовным делам.

Ключевые слова: цифровизация, искусственный интеллект, уголовное судопроизводство, электронное доказывание, выявление, пресечение, расследование преступлений

ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS

Abstract. Digital transformation in the main spheres of life has become not only a boon, but also a new channel for the penetration of offenses and crimes in the context of unformed import substitution with software products and technologies of domestic production. At the same time, we observe the lack of an adequate response from law enforcement agencies, since the process of digitalization of the detection and disclosure of crimes is at a low level. In December 2022, the criminal procedure legislation was supplemented by new means of the proof process at the stage of pre-trial proceedings: obtaining testimony of persons and the procedure for choosing a preventive measure are allowed using video conferencing. This can hardly be considered an effective mechanism for countering energy security challenges. In the area under investigation, crimes have high-tech methods of commission. Such threats can only be neutralized by similar means and methods. In this work, the issue of the possibility of creating a special digital approach in the course of criminal proceedings is considered.

Keywords: digitalization, artificial intelligence, criminal proceedings, electronic proof, detection, suppression, investigation of crimes

В XXI в. современный социум живет в реалиях цифровой трансформации, то есть цифровизации всех сторон жизнедеятельности российского государства на основе новейших IT-разработок. Основополагающим документом данного направления является президентский указ «О национальных целях развития до 2030 года» [2], в котором цифровая трансформация российской экономики, а также социальной сферы определяется в качестве одного из приоритетов.

Необходимость в высокотехнологичных инструментах прослеживается на этапе выявления и пресечения преступной деятельности. Однако о полной замене субъекта доказывания по уголовным делам речь в обозримом будущем вести нельзя. Л. А. Воскобитова справедливо отмечает, что «произвольная и безграничная цифровизация уголовно-процессуальной деятельности без учета ее природы, объективно присущих ей особенностей представляется недопустимой. Нельзя недооценивать весьма великий риск судебных и следственных ошибок, несправедливости разрешения дела и нарушения прав человека, если принятие решений и / или совершение процессуальных действий будет осуществлять машина, запрограммированная и действующая на принципах предельного упрощения и формализации информации и однозначности вариантов решений» [6. С. 91].

При этом необходимо отметить, что внедрение новых цифровых технологий может сопровождаться рядом угроз национальной безопасности, которые, прежде всего, состоят в том, что носители информации базовых систем разработаны и находятся на платформах зарубежных технологий. Уязвимость субъектов экономической и других сфер деятельности в таком случае крайне велика, что было отмечено в ходе Стратегической сессии об импортозамещении программного обеспечения в отраслях 13 сентября 2022 г. Премьер-министр РФ М. Мишустин указал на первоочередную задачу обеспечения технологической независимости; отказа от применяемого зарубежного программного обеспечения [14]. Сказанное относится не только к стратегически важным сферам экономики, а ко всем направлениям, в том числе правоохранительному, судебному.

В современных условиях перед правоохранительными органами ставится множество новых задач по нейтрализации и ликвидации угроз и вызовов национальной безопасности. Успешное их решение зависит от активного поиска и внедрения новых эффективных форм и методов деятельности полиции, основанных на новейших IT-разработках и информационных технологиях. Однако, как показывает практика, инновационная деятельность по внедрению цифровой трансформации в органах внутренних дел не соответствует реалиям сегодняшнего дня.

Весьма отрицательным показателем в этом плане являются данные по росту зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. В 2022 г., по сведениям Главного информационно-аналитического центра МВД России, этот показатель увеличился на 12 % [20]. Раскрытие подобных преступных посягательств возможно при наличии соответствующего ресурса (методологического, технологического, кадрового).

Так, на базе Академии управления МВД России осуществлялись НИР «Концепция научно-технической политики МВД России до 2030 года» и «Концепция использования искусственного интеллекта в деятельности подразделений МВД

России». В установленные сроки, данные концепции были разработаны и подготовлены документы для их утверждения. Реализация данных документов нашла свое воплощение в современных реалиях.

К примеру, Концепция научно-технической политики МВД России до 2030 г. предполагает свою реализацию в три этапа. На действующем этапе и в краткосрочной перспективе планируется реализация конкретных мероприятий на разработку и внедрение современных перспективных образцов специальной техники на основе использования инновационных IT- технологий. Как видим, все зависит от специализированных для нужд правоохранительной деятельности научных разработок в сфере IT- технологий. При этом речь не идет о спецификации применительно к раскрытию отдельных видов или групп преступлений.

Еще одной существенной проблемой является недостаточная подготовка сотрудников ОВД в сфере высоких технологий. В условиях сокращения штатной численности в связи с событиями на Украине Министерство внутренних дел России снова ждет реформа. Именно в такой ситуации необходимы меры совершенно иного качественного характера, позволяющие сохранить контроль над оперативной обстановкой на объектах энергетической инфраструктуры.

Прогресс в создании цифровой полиции имеется, но пока ограничен введением отдельных цифровых технологий, о применении искусственного интеллекта (далее – ИИ) при расследовании отдельных категорий, видов, групп преступлений речь не идет. При этом многими учеными [12. С. 109; 17. С. 194–195] за ИИ в расследовании преступлений и создании цифровых стандартов доказывания по уголовным делам признается будущее цифровизации антикриминальной сферы деятельности.

В этих целях целесообразно обсудить вопрос о создании единой системы «Цифровой суд», или «Цифровой правоохранительный орган», в рамках которой будут интегрированы существующие информационные базы. Следует обратить внимание на ее максимальное упрощение и простоту (так, наличие нескольких разных сайтов по схожим вопросам может запутать пользователей). Также указанные ресурсы должны поддерживаться в качестве мобильных приложений, что создаст удобства [22] и увеличит скорость передачи информации между правоохранительным органом и судом (к примеру, такая необходимость может возникнуть при решении вопроса о санкционировании судом следственных действий, оперативно-розыскных мероприятий).

В рамках цифровизации следует обеспечить требования кибербезопасности. Как известно, широкое внедрение информационно-коммуникационных технологий делает более уязвимым эту сферу для злоумышленников. Виртуализация и глобализация сами по себе увеличивают риск совершения различного рода хакерских атак, в том числе на информационные системы стратегически важных отраслей экономики. Поэтому с учетом требований норм Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1] необходимо закрепить условия применения информационно-коммуникационных технологий, создания механизмов оперативного реагирования на угрозы кибербезопасности. В действующем законодательстве практически не имеются требования к кибербезопасности. К примеру, для обеспечения информационной безопасности

в УПК РФ указано лишь использование защищенного канала связи VPN. На наш взгляд, этого требования недостаточно [22].

В уголовно-процессуальном законодательстве до настоящего времени термины «цифровые технологии» и «цифровые данные» не используются. Отсутствие упоминания в УПК РФ цифровых технологий и тем более их законодательной формулировки вызывает необходимость обращения к мнению ученых по этому вопросу. Отечественными учеными-правоведами выделяются две точки зрения в восприятии компьютерной информации в уголовном процессе [8. С. 133]. Одни электронные документы расценивают как доказательства, другие относят цифровую информацию к иным документам.

Немаловажными для использования компьютерной информации в качестве надлежащего доказательства в уголовном судопроизводстве являются основания и условия изъятия такой информации при производстве обыска в рамках неотложных следственных действий по уголовному делу, предусмотренные п. 9.1 ст. 182 УПК РФ [7. С. 56].

Допустимость доказательств представляет больший интерес как у ученых, так и у практических работников, наибольшие трудности вызывает определение соответствия сведений данному свойству. Применительно к цифровой информации, представляющей интерес с точки зрения познавательной ценности об обстоятельствах по уголовному делу, следует указать следующее.

При производстве следственных действий необходимо помнить, что электронные носители информации изымаются с участием специалиста. По ходатайству законного владельца осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей. При производстве обыска не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись [11. С. 231].

При производстве предварительного расследования с компьютерной информацией допускаются ошибки, способные повлечь утрату сведений, которые могут оказать помощь в раскрытии преступления. Научное осмысление прогнозирование развития новых видов доказательств позволит ускорить процесс их практического использования [15. С. 152]. Вопросы понимания роли и места компьютерной информации в уголовном процессе приобретают в современных условиях все большую актуальность и требуют оперативного их разрешения. Практическим примером использования компьютерной информации в качестве доказательства в современном уголовном процессе могут служить уголовные дела, рассмотренные за 2021 г. и 10 месяцев 2022 г. Оренбургским районным судом. Речь идет о преступлениях в области нарушения авторских прав, неправомерного доступа к охраняемой

законом компьютерной информации, сопряженного с копированием компьютерной информации, а также использования компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации. При этом о динамике роста преступлений данной категории можно судить, сравнив количество уголовных дел в указанной сфере, рассмотренных Оренбургским районным судом в 2019–2020 гг. (2 уголовных дела) и в 2021 г. за аналогичный с 2022 г. период в 10 месяцев (6 уголовных дел) [21].

Компьютерная информация по таким делам, являющаяся контрафактным экземпляром программного обеспечения для ЭВМ, изъятая при обыске (выемке) или в результате ОРМ контрольной закупки, исследуется в судебном заседании в ходе судебного следствия посредством обозрения с учетом выводов эксперта, а после вынесения приговора по делу, в результате определения дальнейшей судьбы вещественных доказательств по делу, в соответствии со ст. ст. 81–82 УПК РФ, как правило уничтожается, а электронные носители, после ее уничтожения, возвращаются законным владельцам по принадлежности [4. С. 113].

В других регионах судебная практика также изобилует примерами признания доказательств недопустимыми. Так, например, Липецкий районный суд Липецкой области при рассмотрении уголовного дела № 1–56/2019 по обвинению гражданина Г. в совершении преступления, предусмотренного ч. 1 ст. 264 УК РФ, пришел к выводу о признании доказательств недопустимыми. Из материалов дела известно, что при предъявлении для опознания были предложенны фотографии при наличии возможности предъявления для опознания непосредственно само лицо, т. е. в данном случае произошло нарушение ч. 5 ст. 193 УПК РФ. Также в протоколе предъявления для опознания отсутствовали признаки, которые позволили бы идентифицировать и распознать опознаваемое лицо [19].

Некоторые ученые, анализируя практику судов относительно применения ст. 75 УПК РФ, приходят к выводу о необходимости уточнения перечня оснований для признания доказательств недопустимыми. В. В. Соткова предлагает также законодательно предусмотреть перечень существенных нарушений, в связи с которыми доказательства признаются недопустимыми [13. С. 464]. В зарубежной практике к свойствам доказательств отнесены дополнительные к отечественным критерии: взаимосвязь и лояльность.

Под взаимосвязью понимается то, что все доказательства по делу должны быть взаимосвязаны между собой и взаимообусловлены [5. С. 42]. Стоит отметить, что российское законодательство предусматривает гарантии защиты от злоупотреблений, поэтому внедрение данного свойства в действующее законодательство нецелесообразно [10. С. 274].

Полагаем необходимым отрегулировать вопросы, связанные с поиском, обнаружением, фиксацией компьютерной информации и ее закреплением, приобщением к делу в качестве доказательств, в связи с чем высказана необходимость ее дополнительного закрепления в главе 10 УПК РФ и оценена целесообразность внесения изменений в главу 25 УПК РФ (часть 9.1 ст. 182 введена Федеральным законом от 28.07.2012 № 143-ФЗ, в редакции Федерального закона от 29.11.2012 № 207-ФЗ) [3. С. 127].

Приемлемым вариантом соответствия реалиям времени может стать редакция норм статей 84^1 «Компьютерная информация», 84^2 «Процессуальный порядок приобщения к делу компьютерной информации в качестве доказательства», 84^3 «Представление доказательств в виде компьютерной информации участниками процесса или иными лицами» [9. С. 387].

Отечественной практикой систематизированы и отражены основные аспекты общепринятых видов доказательств в уголовном судопроизводстве, а также виды компьютерных преступлений и анализ мер противодействия им.

Так, Мещанским районным судом города Москвы 2 октября 2018 г. было рассмотрено дело № 01–0123/2018, согласно материалам которого бывшие сотрудники правоохранительных органов были признаны виновными в совершении преступления, предусмотренного п. «в», ч. 3. ст. 286 УК РФ (превышение должностных полномочий с причинением тяжких последствий). Суть нарушений, допущенных сотрудниками, сводится к фальсификации доказательств с использованием новых цифровых возможностей: контекстное компилирование из мессенджеров частей разговоров и сообщений, допущенное сотрудниками в отношении потерпевших. Постановление президиума Московского городского суда [18] отменило ранее вынесенное определение в отношении граждан Л. и Д.

Решение подобного вопроса в московском суде стало возможным благодаря проведению установления достоверности (подлинности) полученной информации, что стало предметом исследования в рамках судебной компьютерно-технической экспертизы [16. С. 190]. При этом анализу подлежат и машинопечатные тексты, в целом подобное исследование всегда комплексное, соединяющее в себе как традиционные формы экспертных методик, так методики аппаратных, программных систем. Однако приведенный пример – скорее исключение из общего правила, нежели часто используемый прием проверки доказательств.

Поэтому резюмируем, что решение вышеозначенных проблем позволит перейти к обсуждению использования ИИ в борьбе с преступностью.

Список литературы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (Часть I). Ст. 3448.

2. О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21 июля 2020 г. № 474 // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202007210012

3. Баранова М. А. Признание доказательств недопустимыми в судебных решениях по уголовным делам: поиск критериев // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 122–127.

4. Барыгина А. А. Доказывание в уголовном процессе: оценка отдельных видов доказательств. М.: Юрайт, 2019. 277 с.

5. Брянская Е. В. К вопросу о свойствах доказательств в уголовном судопроизводстве // Российская юстиция. 2018. № 6. С. 41–43.

6. Воскобитова, Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex russica (Русский закон). 2019. 5 (150). С. 91–104.

7. Давлетов А. А. Основы уголовно-процессуального познания. Екатеринбург: Издательство Гуманитарного университета, 1997. 190 с.

8. Ишмаева Т. П. К вопросу о юридических свойствах доказательств в уголовном процессе // Вестник Челябинского государственного университета. 2015. № 23 (378). С. 133–136.

9. Капустина Л. К. Соотношение допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Казанского юридического института МВД России. 2019. № 3 (37). С. 386–390.

10. Курс уголовного процесса / под ред. Л. В. Головко. М.: Статут, 2017. 1278 с.

11. Лютынский А. М. О процедуре признания доказательства недопустимым в российском уголовном судопроизводстве // Современные исследования социальных проблем. 2015. № 7 (51). С. 225–233.

12. Панфилов П. О. Особенности производства по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности: специальность 12.00.09 «Уголовный процесс»: дис. ... канд. юрид. наук / Панфилов Павел Олегович. М., 2019. 247 с.

13. Соткова В. В. Основания для признания доказательств недопустимыми // Материалы научной конференции XLVII Огаревские чтения. Саранск: Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева, 2019. С. 463–465.

14. Стратегическая сессия об импортозамещении программного обеспечения в отраслях // Новости Правительства России [сайт]. URL: http://government.ru/news/46507

15. Татаров Л. А. Свойства доказательств в уголовном судопроизводстве: правовые и гносеологические проблемы // Глобальный научный потенциал. 2013. № 10 (31). С. 152–155.

16. Терехин В. В. Стандарты допустимости доказательств в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 1 (33). С. 188–193.

17. Энергетическое право: модели и тенденции развития (обзор докладов Международной научно-практической конференции) / А. В. Габов, Е. Е. Тонков, С. В. Тычинин, Л. Д. Туршук // Nomothetika: Философия. Социология. Право. 2020. Т. 45, № 1. С. 189–202.

18. Дело № 01–0123/2018 от 2 октября 2018 года, рассмотренное Мещанским районным судом г. Москва // КонсультантПлюс: Высшая Школа: правовые док. для студентов юрид., финансовых и экон. специальностей. [Москва]: КонсультантПлюс, 2023.

19. Дело № 1–56/2019 от 13 августа 2019 г., рассмотренное Липецким районным судом Липецкой области // КонсультантПлюс: Высшая Школа: правовые док. для студентов юрид., финансовых и экон. специальностей. [Москва]: КонсультантПлюс, 2023.

20. Результаты деятельности МВД России в 2022 году // Официальный сайт МВД России. URL: https://мвд.рф/dejatelnost/results/annual_reports

21. Статистические данные Оренбургского областного суда по рассмотрению уголовных дел за 2015–2019 годы. URL: http://oblsud.orb.sudrf.ru/modules.php?name=docum_sud&id= 615

22. Расулев А. Правовые основы цифровизации в судебно-правовой сфере // Актуальные вопросы и перспективы цифровизации судебно-правовой деятельности. 2022. № 1(01). С. 11–18.

Н. Н. Гончарова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Е. М. Борознова,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

ДОМАШНЕЕ НАСИЛИЕ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВУЮ ЭПОХУ

Аннотация. Целью исследования является изучение и анализ проявлений домашнего насилия в отношении несовершеннолетних в контексте использования цифровых технологий. Результаты исследования указывают на наличие связи между увеличением использования цифровых технологий и ростом домашнего насилия над детьми. Проанализирована судебная практика и зарубежный опыт в части уголовной ответственности за контроль переписки ребенка в сети «Интернет», слежки за ним при помощи цифровых устройств. Подготовлены законодательные предложения по усовершенствованию уголовного и информационного законодательства России для недопущения уклонения от юридической ответственности родителей и иных законных представителей ребенка, которые осуществляют домашнее цифровое насилие.

Ключевые слова: домашнее насилие, интернет-насилие, контроль за ребенком, ограничение прав ребенка родителем, цифровое насилие, насилие в отношении несовершеннолетних, родительские права, цифровые права детей

DOMESTIC VIOLENCE AGAINST MINORS IN THE DIGITAL AGE

Abstract. The purpose of the research is to study and analyze the manifestations of domestic violence against minors in the context of the use of digital technologies. The results of the study indicate a relationship between the increased use of digital technologies and the growth of domestic violence against children. The research presents scientific novelty in the form of an analysis of the influence of digital technologies on domestic violence against minors. Judicial practice and foreign experience have been analyzed, in particular, with regard to criminal liability for monitoring a child's correspondence on the Internet, surveillance of him using digital devices.

Keywords: domestic violence, internet violence, child monitoring, restriction of child's rights by parent, digital violence, violence against minors, parental rights, digital rights of children

Введение. Цифровые технологии стремительно проникают во все сферы нашей жизни, включая семейные отношения. Интернет, гаджеты, социальные сети открывают новые возможности для общения, развития и социализации детей. Однако они также несут и новые риски.

Одной из важнейших проблем становится использование цифровых технологий как инструмента насилия и контроля в отношении детей в семье – так называемое цифровое домашнее насилие. Эта тема остается малоизученной как в России, так и в мире.

Между тем случаи незаконного контроля и вторжения в цифровое пространство ребенка со стороны родителей учащаются. Дети подвергаются кибербуллингу, необоснованным запретам на доступ в Интернет, шантажу и унижению с использованием цифровых технологий. Это наносит серьезный вред их психологическому и нравственному развитию.

Существующее законодательство недостаточно защищает детей от таких злоупотреблений. Необходим комплексный подход, включающий совершенствование правовых норм и повышение цифровой грамотности всех членов семьи.

Домашнее насилие в отношении ребенка в цифровую эпоху выходит далеко за пределы традиционного физического или психологического насилия. Оно может принимать различные формы и использовать новые каналы, такие как Интернет и социальные сети. Домашнее насилие в отношении детей представляет собой серьезную проблему, наносящую непоправимый вред физическому и психическому здоровью несовершеннолетних. В условиях стремительного развития цифровых технологий и их повсеместного распространения эта проблема приобретает новые формы и масштабы [1. С. 83–84].

Актуальность исследования данной темы обусловлена рядом факторов. Во-первых, в настоящее время отмечается значительный рост случаев домашнего насилия, связанного с использованием цифровых устройств и Интернета. В России в настоящее время отсутствуют какие-либо законодательные акты, защищающие права ребенка в информационном обществе [2. С. 138–139].

Неблагополучные отношения в семьях, жестокость и насилие в отношении детей, унижение их достоинства и принуждение к противоправному поведению, в том числе с использованием цифровых средств (сети «Интернет» компьютера, смартфона, иных гаджетов), становятся фактами повседневной жизни для многих несовершеннолетних, что деформирует психику ребенка [3].

В связи с этим целью данной статьи является комплексное исследование проблемы домашнего насилия в отношении детей в условиях современных цифровых технологий. На основе анализа правоприменительной практики выявлены новые формы насилия, особенности их проявления в цифровой среде, а также даны рекомендации по совершенствованию мер предотвращения и противодействия домашнему насилию в отношении детей.

Результаты исследования могут быть использованы для разработки эффективной государственной политики по защите детей от насилия в современных условиях.

Контроль родителями интернет-активности и переписки ребенка может быть оправдан в интересах его безопасности, но не должен становиться тотальным надзором и вторжением в приватность.

Полный запрет доступа к Интернету со стороны родителей для детей школьного возраста является чрезмерной мерой и может рассматриваться как психологическое насилие. Для эффективного противодействия цифровому насилию в семье необходимо активное взаимодействие органов внутренних дел, опеки, уполномоченного по правам ребенка, а также повышение цифровой грамотности родителей и детей.

Лучшим подходом является открытый диалог в семье по вопросам безопасного использования Интернета, уважение личных границ ребенка и обучение его самозащите от онлайн-угроз.

Результаты.

1. Понятие цифрового домашнего насилия в отношении детей. Цифровое домашнее насилие в отношении ребенка – это форма насилия в семье, при которой родители или другие члены семьи используют цифровые технологии, такие как Интернет, мобильные телефоны, компьютеры и другие гаджеты, для контроля, унижения, оскорбления, шантажа или иного причинения вреда ребенку. Цифровое насилие может иметь серьезные последствия для психического и эмоционального здоровья ребенка, его развития и социализации [4].

Стоит отметить, что отечественное законодательство до сих пор не оперируют понятием домашнего насилия. В уголовном законе под насилием понимается исключительно противоправное применение физической силы [5. С. 522–534].

Как следует из Закона Республики Казахстан, под бытовым насилием понимается умышленное противоправное деяние (действие или бездействие) одного лица в сфере семейно-бытовых отношений в отношении другого (других), причиняющее или содержащее угрозу причинения физического и (или) психического страдания. Норма аналогичного содержания включена в проект федерального закона «О профилактике семейно-бытового насилия». Также в нем целесообразно детально регламентировать цифровое насилие.

Цифровое насилие может, в частности, принимать форму кибербуллинга или онлайн-угроз. Это может быть ситуация, когда родители (законные представители), используя Интернет (электронную почту, текстовые сообщения, мессенджеры), угрожают, унижают или запугивают ребенка. Контроль и надзор за перепиской ребенка, его интернет-активностью и перемещениями через GPS-трекинг также может быть формой цифрового домашнего насилия, если это делается без согласия ребенка и без уважения к его личной жизни. Распространение компрометирующей информации или изображений ребенка в Интернете без его согласия является еще одной формой цифрового насилия [6. С. 17–18].

Наконец, ограничение доступа ребенка к Интернету или онлайн-средствам образования, социализации и развлечения может также быть формой домашнего насилия, если оно проводится с целью изоляции или ущемления прав ребенка. В эпоху цифровизации, когда большая часть обучения, общения и развлечений

переместилась в виртуальное пространство, отрезание ребенка от этих ресурсов может считаться серьезным вмешательством в его права и свободы [7. С. 31].

Например, если родители препятствуют подростку использовать Интернет для выполнения школьных заданий, своевременного получения информации для учебы, это может негативно сказаться на его учебной деятельности и социальном развитии. Если родители ограничивают доступ к Интернету с целью изолировать ребенка от его друзей и сверстников, это может считаться формой эмоционального насилия.

Контроль за онлайн перепиской члена семьи может быть формой домашнего насилия, в случаях когда этот контроль является навязчивым, нарушает личную жизнь и приватность члена семьи и вызывает психологическое или эмоциональное насилие при условии, что он не направлен на защиту прав и законных интересов ребенка. Это может включать отслеживание сообщений, непрерывное чтение личной переписки, контроль над социальными медиа-аккаунтами, запрещение общения с другими людьми онлайн или навязчивый мониторинг онлайн-активности [8. С. 370].

В Российской Федерации защита прав и свобод человека гарантирована Конституцией. В соответствии с Конституцией Российской Федерации каждый человек имеет право на неприкосновенность своей личной жизни, включая тайну переписки и телефонных переговоров. Это право может быть ограничено только в случаях, установленных законом, и на основании судебного решения.

Согласно пункту 4 Постановления Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина», тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений признается нарушенной, когда доступ к переписке, переговорам, сообщениям совершен без согласия лица, чью тайну они составляют, при отсутствии законных оснований для ограничения конституционного права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Так, близкие родственники, включая родителей, не имеют права нарушать право на тайну переписки и телефонных разговоров детей без их согласия. Однако в ряде случаев возникают вопросы, касающиеся защиты интересов прав детей, которая возложена на родителей статьей 64 Семейного кодекса РФ.

Родители несут ответственность за своих несовершеннолетних детей и за их безопасность, и поэтому в определенных обстоятельствах им может потребоваться доступ к их переписке, ограничению иных цифровых прав ребенка. Важно понимать, что это не должно превращаться в чрезмерное вторжение в личную жизнь ребенка или использоваться для целей контроля или надзора, которые выходят за рамки обеспечения его безопасности и иных законных интересов.

С учетом положений статьи 64 Семейного кодекса РФ, в отношении детей и подростков принцип наилучшего интереса ребенка должен быть главным руководством. Этот принцип заложен в Конвенции о правах ребенка, которую Россия ратифицировала. Это значит, что в случае, если есть основания полагать, что ребенок может быть подвергнут риску (например, он стал жертвой онлайн-травли, сексуального домогательства в Интернете или иной формы онлайн-угрозы), родители могут

и должны вмешаться, чтобы защитить своего ребенка, в том числе ограничивая круг его онлайн общения, проверяя его мессенджеры.

Таким образом, родители не должны подлежать уголовной ответственности по статье 138 УК РФ в случае нарушения тайны переписки ребенка, не достигшего 18 летнего возраста, если это было сделано в рамках их законных прав в качестве родителей. Но даже в таких случаях родители должны стремиться к тому, чтобы решать вопросы, связанные с онлайн-поведением и безопасностью детей, через открытый диалог и наставление, прежде чем прибегать к проверке их личной переписки.

Хотя защита безопасности и благополучия детей является абсолютным приоритетом, важно уважать их права на частную жизнь и конфиденциальность, в которые входит и право на неприкосновенность переписки. Баланс между этими интересами может быть сложным, но он должен строиться на основе принципа наилучшего интереса ребенка.

Согласно пункту 1 статьи 54 Семейного кодекса РФ, ребенком признается лицо, не достигшее возраста восемнадцати лет (совершеннолетия). После достижения ребенком 18-летнего возраста и получения полной дееспособности любой навязчивый контроль со стороны родителей является незаконным и может содержать признаки преступления в случае, если нарушается тайна переписки ребенка с их стороны. Родители не имеют права вмешиваться в личную жизнь взрослых детей без их согласия.

Аналогичные подходы могут иметь место в отношении контроля родителей за передвижением детей, в том числе с использованием цифровых средств. Родители имеют право и даже обязаны знать, где находятся их несовершеннолетние дети в целях обеспечения их безопасности и благополучия. Важно отметить, что такой контроль должен осуществляться в пределах разумного и не нарушать личные границы и право ребенка на приватность.

Критерии законности контроля родителей за местонахождением ребенка включают следующие аспекты:

– Действия родителей должны быть направлены на обеспечение безопасности и защиты прав ребенка. Это может включать в себя знание о местонахождении ребенка в определенное время, особенно в том случае, если ребенок находится в потенциально опасной ситуации.

– Контроль должен осуществляться с учетом возраста и зрелости ребенка. Более старшие и более зрелые дети, возможно, требуют большей степени свободы и независимости, и в этих случаях необходим более умеренный контроль со стороны родителей [9. С. 221].

– Родители должны всегда стремиться уважать личные границы ребенка и право на приватность, включая право на свободное перемещение. Контроль за местоположением ребенка не должен превращаться в постоянное слежение или вторжение в его личную жизнь.

Важно, чтобы родители обсуждали эти вопросы с ребенком, учитывая его мнение и взаимодействуя с ним на основе доверия и уважения.

Незаконное применение технических средств слежения родителями в отношении ребенка также может влечь за собой уголовную ответственность по статье 138.1

УК РФ («Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»).

Стоить отметить, что, согласно примечанию 2 к статье 138.1 УК РФ, к специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, устройства, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, если им преднамеренно не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя [19. С. 3].

Рассмотрим судебную практику на примере приговора.

Согласно приговору Ленинского районного суда города Барнаула от 10 июня 2019 г. по делу номер 1–287/2019, гражданин Юрьев в ходе допроса подтвердил, что приобрел специальное техническое устройство, предназначенное для скрытой аудио- и видеозаписи. По словам Юрьева, он купил это устройство для тайной слежки за своими родственниками.

В частности, в суде Юрьев пояснил, что приобрел ручку с встроенной видеокамерой. Он планировал использовать эту ручку для наблюдения за детьми, так как у него пропадали деньги в квартире. Также Юрьев хотел установить скрытую слежку за женой, поскольку подозревал ее в измене. Таким образом, Юрьев признался, что купил специальное устройство для тайной видеосъемки родственников и выяснения подробностей их личной жизни.

Суд указал в приговоре, что «оценивая характер общественной опасности преступления, суд принимает во внимание, что совершенное Юрьевым А. Е. деяние посягает на конституционные права и свободы человека и гражданина» [11].

Следует учитывать, что состав преступления, предусмотренный статьей 138.1 УК РФ, формальный и не требует фактического нарушения конституционных прав.

Показательно, что в рассматриваемом деле суд установил факт посягательства на конституционные права человека. Проанализировав материалы дела, можно признать, что такое посягательство было не только в отношении жены, которая имела право на личную неприкосновенность, но и в отношении детей.

Слежку за детьми подсудимый планировал осуществлять, когда они находились дома, то есть слежка не была направлена на защиту прав и законных интересов детей. Приобретение даже заводского устройства для слежки за детьми может быть признано преступлением.

Пример из Приговора Ленинского районного суда города Оренбурга № 1–325/2017 от 12 октября 2017 г. по делу № 1–325/2017:

«Наиболее распространенными GPS-устройствами являлись «Mini A8». В связи с чем подсудимый прибыл в ближайший магазин и приобрел данные устройства в количестве двух штук для пробы. Предназначены данные устройства для контроля за передвижением детей, пожилых людей, животных, защиты автомобиля от угона» [12].

Для того чтобы использование средств слежения за ребенком было правомерно, следует учитывать следующие требования к техническому средству слежки:

Представленное техническое средство не должно быть замаскировано (например, спрятано в ручке), на его внешней стороне должна быть соответствующая маркировка. Оно никак не должно позволять вести скрытное наблюдение и тайно получать информацию. Это устройство хорошо видно, его легко опознать, и любой человек без труда может его обнаружить и предпринять необходимые действия. Данное устройство не должно применяться в рамках закона об оперативно-розыскной деятельности, входить в перечень специальных технических средств.

Речь идет о различных бытовых устройствах, которые находятся в свободной продаже и обладают функциями аудио- или видеозаписи, а также геолокации.

К таким устройствам относятся, например:

– диктофоны, фото- и видеокамеры;

– смартфоны и планшеты со встроенными камерами, автомобильные регистраторы;

– навигаторы и другие гаджеты с функцией определения местоположения (в частности, наручные часы).

Все эти устройства имеют открытые элементы управления, четкую маркировку и не скрывают своего функционала. Они предназначены для открытого использования и не относятся к специальным техническим средствам для негласного получения информации. Их нельзя использовать для скрытой слежки или прослушки без ведома объекта.

Выглядит целесообразным дополнить примечания к статье 138.1 УК РФ пунктом 3 в такой редакции:

К специальным техническим средствам, предназначенным для негласного получения информации, не относятся технические средства, предназначенные исключительно для контроля и определения местоположения детей, лиц, в отношении которых установлена опека и попечительство родителями, опекунами и попечителями, при условии, что данный контроль осуществляется в интересах детей, лиц, в отношении которых установлена опека и попечительство.

При использовании соответствующих средств и программ для слежения за ребенка следует принимать во внимание следующее:

Во-первых, важно учитывать возраст и уровень зрелости ребенка. Младшим детям, которые не могут полностью оценить риски, связанные с использованием Интернета или самостоятельным передвижением, может потребоваться больше родительского наблюдения и контроля. С возрастом, когда ребенок начинает лучше понимать и управлять этими рисками, должно быть больше свободы.

Во-вторых, родители должны учитывать конкретные обстоятельства и контекст. Ограничения могут быть необходимы, если есть конкретные причины для опасений, например, если ребенок сталкивается с мошенничеством, домогательствами или угрозами в Интернете или если в районе проживания происходят преступления. Однако родители должны объяснить эти причины ребенку и обсудить с ним возможные решения вместо того, чтобы просто навязывать ограничения.

В-третьих, ограничения должны быть пропорциональными. Они не должны лишать ребенка возможности общаться с друзьями, участвовать в образовательных и социальных активностях в Интернете или самостоятельно передвигаться в без-

опасной и знакомой среде. Ограничения также не должны становиться формой наказания или угнетения [13. С. 376].

Иной проблемный вопрос – уголовно-правовая квалификация действий родителей, направленных на сексуальную эксплуатацию детей, в частности, путем принуждения их участия в онлайн-трансляциях.

Преступлением признается привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера, совершенное лицом, достигшим восемнадцатилетнего возраста (статья 242.2 УК РФ).

Следует отметить, что в рассматриваемой статье отсутствует такой квалифицирующий признак, как совершение деяния родителем.

Соответственно такие деяния, совершенные родителем, могут быть квалифицированы по совокупности преступлений, предусмотренных статьями 150 (вовлечение несовершеннолетнего в преступление) и 242.2 УК РФ. Однако такая квалификация является громоздкой и спорной, ввиду того, что по общему принципу за одно преступление должна быть одна статья (часть статьи Особенной части УК РФ.

Исходя из вышеизложенного, целесообразно дополнить часть вторую статьи 242.2. УК РФ пунктом «д» в такой редакции:

« д) совершенное родителем либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего».

С использованием сети «Интернет» родители могут оскорблять своих несовершеннолетних детей. В таком случае действия родителей могут быть квалифицированы по статье 5.61 КоАП РФ (оскорбление) и, при наличии фактических обстоятельств, по статье 5.35 КоАП РФ, (неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних).

В соответствии с ч. 1 ст. 65 СК РФ родительские права не могут осуществляться в противоречии с интересами детей. В частности, способы воспитания детей должны исключать пренебрежительное, жестокое, грубое, унижающее человеческое достоинство обращение, оскорбление детей. Родители, осуществляющие родительские права в ущерб правам и интересам детей, несут соответствующую юридическую ответственность.

Таким образом, оскорбление несовершеннолетних детей родителями в сети «Интернет» должно квалифицироваться в рамках неисполнения родительских обязанностей по статье 5.61 КоАП РФ (специальная норма).

Для того чтобы исключить неоднозначность квалификации административной ответственности за оскорбление несовершеннолетнего родителем, выглядит целесообразно дополнить статью 5.35 КоАП РФ пунктом 4 в следующей редакции:

4. Оскорбление ребенка, осуществленное его родителем или иными законными представителями несовершеннолетнего, в том числе в сети «Интернет»,

влечет наложение административного штрафа в размере от ста тысяч до ста пятидесяти тысяч рублей.

2. Уполномоченные органы. Домашнее насилие в отношении детей в цифровую эпоху принимает различные формы, от кибербуллинга и оскорблений в социальных

сетях до незаконного просмотра личной переписки и контроля за онлайн-активностью. Органы внутренних дел, органы опеки и попечительства и Уполномоченный по правам ребенка играют важную роль в защите детей от такого насилия.

Рассмотрим полномочия органов власти.

2.1. Органы внутренних дел. Основную роль играют уполномоченные инспектора по делам несовершеннолетних, которые в соответствии со статьей 21 ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» проводят профилактическую работу с родителями, принимают участие в рассмотрении дел о правонарушениях, совершенных родителями [14; с. 12].

Согласно пункту 2.3. Приказа МВД России от 15.10.2013 № 845 «Об утверждении Инструкции по организации деятельности подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации», инспектор по делам несовершеннолетних наделен полномочиями выявлять родителей, не исполняющих надлежащим образом своих родительских обязанностей, в том числе таких, которые нарушают права ребенка с применением цифрового насилия, а также применять в отношении них соответствующее средства правового реагирования.

Органы внутренних дел (полиция) также осуществляют:

– Информирование общественности о способах защиты детей в Интернете, включая организацию и проведение профилактических мероприятий.

– Проведение расследований по случаям нарушения прав детей в цифровом пространстве и привлечение виновных лиц к административной и уголовной ответственности.

– Сотрудничество с интернет-провайдерами и операторами связи для отслеживания и блокирования незаконного контента [15. С. 58].

Органы опеки и попечительства. Согласно части 1 статьи 121 Семейного кодекса Российской Федерации, защита прав и интересов детей в случаях уклонения родителей от защиты прав и интересов ребенка, при создании действиями или бездействием родителей условий, препятствующих нормальному воспитанию и развитию детей возлагается на органы опеки и попечительства. С целью выполнения, возложенных на них задач, органы опеки и попечительства могут проводить проверки условий жизни и воспитания детей, включая анализ их цифрового окружения. Они могут давать рекомендации родителям по вопросам обеспечения безопасности детей в Интернете и в случае выявления нарушений применять соответствующие административные меры, вплоть до временного ограничения или лишения родительских прав.

Правоприменительные органы при проверки соблюдение прав ребенка должны проводить анализ цифрового окружения ребенка.

Анализ цифрового окружения ребенка – это комплексная оценка его взаимодействия с цифровыми технологиями и Интернетом, которая помогает оценить уровень его защищенности от возможных угроз. Органы опеки и попечительства, проводя такой анализ, могут учесть следующие аспекты:

– Анализ использования устройств: исследование наличия и использования ребенком цифровых устройств (компьютеров, смартфонов, планшетов), а также доступа к Интернету через эти устройства.

– Проверка настроек приватности: проверка настроек приватности и безопасности на устройствах и в приложениях, которые использует ребенок. Оценка наличия и эффективности родительского контроля.

– Изучение активности в социальных сетях: оценка присутствия ребенка в социальных сетях и других онлайн-платформах. Анализ контента, который ребенок создает, шарит и с кем он общается.

– Оценка контента: изучение типа контента, которым ребенок интересуется и к которому он имеет доступ. Он может включать видео, игры, веб-сайты, приложения и другие цифровые ресурсы.

– Общение с ребенком: непосредственный диалог с ребенком о том, как он использует Интернет, с кем общается, какие проблемы встречает, как оценивает свое поведение в Сети.

– Общение с родителями/опекунами: важно также обсудить с родителями или опекунами, как они контролируют использование Интернета ребенком, насколько они осведомлены о его цифровой жизни и какие меры они предпринимают для обеспечения его безопасности.

Проведение такого анализа позволяет органам опеки и попечительства не только выявить возможные угрозы и проблемы, но и дать рекомендации по улучшению цифровой безопасности ребенка.

2.3. Уполномоченный по правам ребенка. К полномочиям Уполномоченного по правам ребенка относятся:

– привлечение внимания общественности и соответствующих органов к проблемам домашнего насилия в отношении детей в цифровую эпоху;

– проведение независимых проверок на предмет соблюдения прав детей в Интернете;

– инициатива по внесению в законодательство изменений, направленных на усиление защиты детей.

Все эти органы несут обязанность защищать права и свободы детей, включая право на тайну переписки и телефонных переговоров, и право на свободу получения, использования и распространения информации любым законным способом, которые гарантируются Конституцией Российской Федерации.

3. Ограничение родителями доступа ребенка к цифровым устройствам и Интернету. Ограничение родителями доступа ребенка к цифровым устройствам и Интернету в качестве наказания может рассматриваться как форма домашнего насилия.

С одной стороны, подобные действия могут нарушать права и интересы ребенка, причинять ему психологический дискомфорт и ограничивать доступ к образовательным ресурсам и полезной информации в сети Интернет [16. С. 55].

Однако, с другой стороны, родители имеют право ограничивать использование гаджетов и Интернета своими несовершеннолетними детьми в разумных пределах в целях защиты их физического и психического здоровья и нравственного развития.

Чтобы такие ограничения не считались насилием и были правомерными, ограничения пользования Интернетом должны отвечать следующим критериям:

– быть разумно обоснованными конкретными обстоятельствами (ухудшение успеваемости, зависимости от гаджетов и пр.);

– быть соразмерными и не чрезмерно строгими;

– не причинять существенный вред здоровью и развитию ребенка;

– применяться как вынужденная мера после других безрезультатных попыток воспитательного воздействия [17].

Таким образом, умеренные временные ограничения доступа к гаджетам родителями, в том числе в целях дисциплинарного воздействия, при соблюдении разумного подхода не являются домашним насилием или преступлением, но границы допустимого здесь достаточно размыты на практике [18. С. 153].

Абсолютный запрет доступа ребенка к Интернету со стороны родителей может рассматриваться как форма домашнего насилия в определенных случаях.

1. Для детей младшего возраста (до 10–13 лет) такой запрет может быть оправдан мерой защиты от нежелательного контента и вредных влияний Сети. Полный запрет здесь не является насилием при условии разумного подхода.

2. Для подростков (14–15 лет) абсолютный запрет является чрезмерной мерой, лишающей доступа к образовательным и социальным возможностям Интернета. Такой запрет можно рассматривать как психологическое насилие и нарушение прав ребенка.

3. Для старших подростков (16–18 лет) полный запрет Интернета неприемлем, поскольку в этом возрасте он необходим для социализации, образования и развития личности. Такой запрет следует рассматривать как насилие.

Таким образом, по мере взросления ребенка абсолютный родительский запрет на доступ в Интернет должен смягчаться и становиться более гибким. Политика разумных ограничений и контроля предпочтительнее для подростков. Жесткие запреты для них чреваты психологической травмой и нарушением прав [19. С. 65].

Согласно пункту 3 статьи 56 Семейного кодекса РФ, при получении сведений о нарушении законных прав и интересов ребенка орган опеки и попечительства обязан принять необходимые меры по защите прав и законных интересов ребенка. Таковыми в случае необоснованного ограничения родителями доступа ребенка к Интернету могут быть:

1. Проведение профилактической беседы с родителями, разъяснение им недопустимости чрезмерных ограничений ребенка в пользовании Интернетом.

2. Обязание родителей смягчить ограничения и позволить ребенку доступ в Интернет в разумных пределах.

3. Применение мер административного воздействия к родителям за нарушение прав ребенка.

Частью 1 статьи 8 Федерального закона «Об информации, информационных технологиях и о защите информации» установлено, что физические лица вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законодательством.

Целесообразно в семейном законодательстве закрепить следующие положения:

Граждане, достигшие 16 летнего возраста, вправе в полной мере ос осуществлять поиск и получение любой информации в любых формах и из любых

источников при условии соблюдения требований, установленных Федеральным законом «Об информации, информационных технологиях и о защите информации» и другими федеральными законами.

Граждане, достигшие 14-летнего возраста, вправе осуществлять поиск и получение информации, в том числе в сети «Интернет», в учебных, образовательных, воспитательных целях. Получение ребенком иной информации в сети «Интернет», использование сети «Интернет» в иных целях (в том числе для общения) может быть ограничено родителями, опекунами в целях обеспечения прав и законных интересов ребенка.

Граждане, не достигшие 14-летнего возраста вправе осуществлять поиск и получение информации, в том числе в сети «Интернет» в учебных, образовательных, воспитательных целях. Получение ребенком информации в сети «Интернет», в других источниках может быть ограничено родителями, опекунами в целях обеспечения прав и законных интересов ребенка.

Порядок использования гаджетов и компьютером ребенком для иных целей, кроме учебных, образовательных, воспитательных, а также время их использования определяется:

1) в возрасте до 14 лет: родителями или иными законными представителями ребенка с учетом обеспечения законных прав и интересов ребенка;

2) в возрасте до 16 лет: родителями или иными законными представителями ребенка с учетом мнения ребенка, объективных потребностей, в том числе в общении и развитии;

3) в возрасте от 16 до 18 лет: ребенком самостоятельно с учетом мнения родителей.

Выводы. Цифровое домашнее насилие в отношении несовершеннолетнего – это форма насилия, которая проявляется через использование цифровых технологий, включая Интернет, мобильные телефоны и другие электронные средства, для того чтобы контролировать, угрожать, домогаться, шантажировать или иным образом причинять вред несовершеннолетнему.

Это может включать в себя такие действия, как незаконные мониторинг и контроль активности в социальных сетях, незаконные прослушивание и запись разговоров, использование GPS для отслеживания местоположения, а также распространение личной или компрометирующей информации без согласия.

Допустимость контроля за перепиской несовершеннолетнего ребенка зависит от множества факторов, включая возраст и зрелость ребенка, характер контроля и его цель. Родители должны уважать право ребенка на приватность, но в то же время обеспечивать его безопасность от потенциальных онлайн-угроз, таких как интернет-троллинг, сексуальное домогательство или другие формы эксплуатации.

Контроль со стороны родителей может стать формой домашнего насилия, если он превышает рамки обоснованной заботы о безопасности ребенка и становится инструментом надзора, контроля и ограничения свободы. Такой контроль может привести к нарушению личных границ ребенка, психологическому давлению и стрессу.

Поэтому очень важно уважать баланс между правом ребенка на приватность и обязанностью родителей обеспечивать его безопасность. Родители должны стремиться к открытому и честному диалогу с детьми о безопасности в Интернете и уважать их личные границы. Вместо контроля за перепиской, лучше сосредоточиться на образовании и информировании детей о возможных угрозах и том, как с ними справляться.

Выглядит целесообразным дополнить Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» пунктом 4.1. в такой редакции:

«4.1. При рассмотрении уголовных дел о преступлении, предусмотренном статьей 138 УК РФ, судам следует учитывать, что родители и лица, уполномоченные на защиту прав детей, не подлежат уголовной ответственности, если доступ к переписке, телефонным переговорам, почтовым, телеграфным или иным сообщениям несовершеннолетнего осуществлялся с целью обеспечения его безопасности и защиты его прав и законных интересов».

Список литературы

1. Андреева А. Д., Данилова Е. Е. Родительский контроль в современном обществе: приоритеты и формы реализации // Научный диалог. 2017. № 4. URL: https://cyberleninka.ru/article/n/roditelskiy-kontrol-v-sovremennom-obschestve-prioritety-i-formy-realizatsii

2. Архипова В. Ю. Влияние родительского контроля на формирование личности подростка // Концепт. 2020. № 3. URL: https://cyberleninka.ru/article/n/vliyanie-roditelskogo-kontrolya-na-formirovanie-lichnosti-podrostka

3. Безверхов, А. Г., Норвартян, Ю. С. Соотношение категорий «насилие» и «угроза» в современном уголовном праве России// Вестник Санкт-Петербургского университета. Право 4. 2018. С. 522–534. URL: https://doi.org/10.21638/spbu14.2018.405

4. Гриненко, А. В., Потапов В. Д., Цветкова Е. В. Влияние неблагополучной семьи на формирование личности несовершеннолетнего преступника // Вестник Санкт-Петербургского университета. Право 1. 2023. с. 266–279. URL: https://doi.org/10.21638/spbu14.2023.117

5. Дохоян А. М., Маслова И. А. Кибербуллинг в современном мире: психологические аспекты // Проблемы современного педагогического образования. 2022. № 76–4. URL: https://cyberleninka.ru/article/n/kiberbulling-v-sovremennom-mire-psihologicheskie-aspekty

6. Евсикова Е. В. Органы внутренних дел как субъект предупреждения домашнего насилия // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2016. № 4. URL: https://cyberleninka.ru/article/n/organy-vnutrennih-del-kak-subekt-preduprezhdeniya-domashnego-nasiliya

7. Жиляева С. К., Красова А. А. Проблемные вопросы семейно-бытового насилия в отношении женщин и детей // Вестник БелЮИ МВД России. 2019. № 2.

URL: https://cyberleninka.ru/article/n/problemnye-voprosy-semeyno-bytovogo-nasiliya-v-otnoshenii-zhenschin-i-detey

8. Козлова Н. Н., Рассадин С. В., Овчарова О. Г. Проблема домашнего насилия в контексте реализации государственной семейной политики РФ// Наука. Культура. Общество. 2022. № 2. URL: https://cyberleninka.ru/article/n/problema-domashnego-nasiliya-v-kontekste-realizatsii-gosudarstvennoy-semeynoy-politiki-rf-analiz-setevyh-resursov-regionalnyh (дата обращения: 22.07.2023).

9. Константин А. О. Бытие в цифре: модусы цифрового существования // Революция и эволюция: модели развития в науке, культуре, обществе. 2019. № 1. URL: https://cyberleninka.ru/article/n/bytie-v-tsifre-modusy-tsifrovogo-suschestvovaniya

10. Клименко В. К., Савенышева С. С. Электронные устройства и ребенок: опосредующая роль родителей // Мир науки. Педагогика и психология. 2020. № 4. URL: https://cyberleninka.ru/article/n/elektronnye-ustroystva-i-rebenok-oposreduyuschaya-rol-roditeley-po-materialam-zarubezhnyh-issledovaniy

11. Ланина Е. В., Бочавер А, А., Антипкина И, В. Измерение родительского контроля и его связь с когнитивными результатами учащихся младших классов // Вопросы образования. 2021. № 2. URL: https://cyberleninka.ru/article/n/izmerenie-roditelskogo-kontrolya-i-ego-svyaz-s-kognitivnymi-rezultatami-uchaschihsya-mladshih-klassov

12. Маматазизова Н. К. Роль органов внутренних дел в профилактике семейного насилия // Академическая мысль. 2017. № 1. URL: https://cyberleninka.ru/article/n/rol-organov-vnutrennih-del-v-profilaktike-semeynogo-nasiliya

13. Приговор Ленинского районного суда города Барнаула № 1–287/2019 от 10 июня 2019 г. по делу № 1–287/2019.

14. Приговор Ленинского районного суда города Оренбурга № 1–325/2017 от 12 октября 2017 г. по делу № 1–325/2017.

15. Писаренко И. А., Заиченко Л. И. Родители как субъекты влияния на развитие цифровых навыков детей // INTER. 2021. № 2.

16. Солдатова Г. У., Ярмина А. Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // Национальный психологический журнал. 2019. № 3(35).

17. Чеснокова Ю. В. Правовое регулирование родительских прав в Российской Федерации // БГЖ. 2017. № 3(20).

18. Шутова Ю. А. Основания криминализации некоторых современных форм психического насилиях (на материалах конкретного социологического исследования) // Вестник Санкт-Петербургского университета МВД России. 2022. № 3(95).

19. Янак А. Л. Дети и родители в информационном пространстве: взаимодействие, риски и стратегии обеспечения безопасности // Известия Саратовского университета. Новая серия. Серия Социология. Политология. 2021. № 1.

Ю. В. Быстрова,
доктор юридических наук, доцент,
Орловский государственный университет имени И. С. Тургенева
Е. Е. Быстрова,
студент,
Банковский колледж,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации
(Среднерусский институт управления – филиал)

ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО КАК ОБЪЕКТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ

Аннотация. В статье рассматривается вопрос информационной безопасности государства, проанализированы цели и задачи, поставленные в рассматриваемой сфере на современном этапе развития общества. Отражены актуальные проблемы формирования системы мер противодействия угрозам безопасности российского информационного пространства. Предпринята попытка сформулировать перечень возможных преступных посягательств в информационной сфере государства. Проанализировано законодательство, регламентирующее рассматриваемый круг правоотношений, сделаны выводы о его несовершенстве в настоящее время и необходимости корректировки.

Ключевые слова: информационное пространство, угрозы безопасности, уголовно-правовые меры противодействия, интернет-пространство

INFORMATION SPACE AS AN OBJECT OF CRIMINAL ENCROACHMENTS

Abstract. The article deals with the issue of information security of the state, analyzes the goals and objectives set in this area at the present stage of development of society. The current problems of forming a system of measures to counter threats to the security of the Russian information space are reflected. An attempt has been made to formulate a list of possible criminal encroachments in the information sphere of the state. The legislation regulating the circle of legal relations under consideration is analyzed, conclusions are drawn about its imperfection at the present time and the need for adjustment.

Keywords: information space, security threats, criminal legal counteraction measures, Internet space

Современные реалии таковы, что позитивное развитие общества, государственных и общественных правовых институтов, поставлено в зависимость от безопасности подаваемой информации, т. е. от информационной безопасности. В настоящий момент в связи с усложнившейся политической ситуацией данная проблема стоит наиболее остро. В связи с чем видится настоятельная необходимость в формировании системы уголовно-правовых и криминологических мер, направленных на противодействие угрозам безопасности информационного пространства. И в отличие

от ранее рассматриваемых механизмов, направленных на обеспечение безопасности международного информационного пространства, необходимо предпринимать активные действия для обеспечения информационной безопасности внутри страны.

Государство может эффективно противостоять информационным вызовам только совместно с другими государствами в рамках осуществления международного сотрудничества [7. С. 144]. В этой связи Россия, пытаясь противодействовать нарушениям информационной безопасности, выступила с предложением международного сотрудничества по рассматриваемому вопросу в ООН [8. С. 9].

Цель противодействия информационным угрозам на международном уровне определялась как выполнение норм международного права и общепризнанных принципов на условиях равноправия по обеспечению поддержания мира, соблюдая безопасность и стабильность каждого государства. То есть противодействие угрозам международной информационной безопасности подразумевало под собой необходимость формирования единой правовой системы, включающей в себе тесное взаимодействие субъектов противодействия между собой, действующих на основе принятых международных норм и правил и применяющих единую методику борьбы с данным видом преступных посягательств. Следует отметить, что данная система на международном уровне еще не успела сформироваться, необходимые правовые акты и международные договоры в полном объеме еще не приняты, однако в настоящее время возникла настоятельная необходимость в построении системы противодействия угрозам информационной безопасности внутри страны.

Для формирования изложенного инструментария изначально необходимо остановиться на действующих нормативных правовых актах, содержащих понятийный аппарат, применяемый в данной сфере.

В настоящее время дефиниция «информационное пространство» закреплена в Стратегии развитии информационного общества в Российской Федерации на 2017–2030 гг. [1] и подразумевает под собой совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры. Данное понятие по своей сути является достаточно обширным, применительно к уголовно-правовой сфере, в качестве объекта посягательств. Вместе с тем целью преступных посягательств в информационной сфере могут быть как основы государственной власти, общественного правопорядка, так и причинение вреда гражданину, ребенку.

Необходимо отметить, что цели преступных посягательств носят динамичный характер и, в зависимости от социально-экономического развития и политической ситуации государства с каждым годом видоизменяются.

Особой правовой защиты требуют дети. К сожалению, необходимо констатировать тот факт, что на сегодняшний день в интернет-пространстве развернулась целая война, направленная на нравственное уничтожение молодого поколения.

Фейковая информация, спамы, которые могут заинтересовать и заинтриговать ребенка размещаются в интернет-пространстве криминальными сообществами, террористическими и экстремистскими организациями. Деятельность всех этих субъектов направлена на одно – дезорганизовать российское общество, путем воздействия на молодое поколение.

Несовершеннолетние в большей степени, чем взрослые, подвержены дезорганизации, склонности к преступному поведению, отказу от духовных и семейных ценностей. Психологической особенностью детства является инфантильность, доверчивость и т. д.

Многим несовершеннолетним предоставлена свобода выбора информационными ресурсами. А это зачастую оказывает деструктивное воздействие на несовершеннолетних в связи с тем, что их идеологические и моральные устои еще не сформировались. Дети пытаются самостоятельно, дистанцируясь от взрослых, реализовать себя через интернет-пространство. Однако, интернет-ресурсы не всегда оказывают положительное воздействие на становление личности ребенка, а, напротив, негативно воздействуют на него. Это негативное воздействие впоследствии выражается в обесценивании моральных и правовых норм для ребенка, влияет на психологическое развитие и становление личности, формирует зависимость от интернет-ресурсов, которая впоследствии может перерасти в психическое заболевание. Самая основная проблема влияния информационного пространства на детей заключается в формировании и пропагандировании противоправного поведения.

В связи с вышеперечисленными угрозами информационной безопасности для несовершеннолетних государство разработало стратегию комплексной безопасности детей [3], в которой в 2023 г. основными целями российского государства в рамках обеспечения информационной безопасности определены: развитие безопасного информационного пространства для детей и защита детей негативного информационно-психологического воздействия со стороны интернет-ресурсов. Кроме того, в данной Стратегии закреплены принципы и задачи обеспечения информационной безопасности. Приоритетной задачей названо налаживание взаимодействия семьи с государством и всеми элементами медиарынка.

Информационное манипулирование способствует стимулированию и росту антиобщественного поведения среди несовершеннолетних. Кроме того, зависимость от интернет-пространства наносит значительный ущерб нравственному здоровью детей [4].

В целях предупреждения преступлений в интернет-пространстве, считаем необходимым разработать систему уголовно-правовых мер противодействия угрозам информационной безопасности. За основу предлагаем взять перечень угроз международной информационной безопасности, сформулированный в Основах государственной политики Российской Федерации в области международной информационной безопасности [2], учитывая при этом особенности развития и становления российского общества.

Итак, применительно к России среди угроз национальной информационной безопасности предлагаем выделить следующие:

1) использование информационно-коммуникационных технологий в военно-политической сфере в целях подрыва авторитета власти, ущемления суверенитета, нарушения границ и территориальной целостности государства.

Так, по заявлению замглавы Роскомнадзора Вадима Субботина: «США вели агрессивную работу по подрыву суверенитета и безопасности России.К 2022 году Украина подошла в целом с изолированным от России информационным простран-

ством. К этому времени США уже на протяжении длительного периода вели целенаправленную агрессивную работу в соседних странах по подрыву суверенитета и безопасности Российской Федерации. С начала спецоперации ведомство выявило и заблокировало более 157 тыс. фейков и призывов к митингам» [6];

2) использование информационно-коммуникационных технологий в террористических целях, например, для пропаганды терроризма и привлечения к террористической деятельности новых лиц;

3) использование информационно-коммуникационных технологий в экстремистских целях.

Примером могут служить материалы уголовного дела, переданные в настоящее время для рассмотрения по существу в Советский районный суд. Согласно данным предварительного следствия у П. совместно с М. и А., действующих совместно и согласовано в составе группы лиц по предварительному сговору, в определенный период и по настоящее время, возник преступный умысел на организацию и участие в деятельности экстремистской организации. П., действуя совместно и согласованно с М. и А., находясь на территории Орловской области и г. Орла, реализуя преступный умысел на организацию деятельности ликвидированной и запрещенной экстремистской организации МРО Свидетелей Иеговы «Орел», из экстремистских побуждений, умышленно осуществляли созыв собраний путем оповещения его участников посредством электронных средств связи о дате и месте их проведения, определяли порядок проведения религиозных выступлений и богослужений на данных собраниях, поручали участникам собрания выступления на заданные темы [5];

4) использование информационно-коммуникационных технологий в преступных целях. Спектр преступлений, совершаемых с помощью IT-технологий с каждым годом растет как количественно, так и качественно. Правоохранительные органы часто регистрируют преступления, совершаемые в интернет-пространстве. Необходимо отметить, что особую сложность представляет их расследование, так как следователь не обладает специальными знаниями в рассматриваемой сфере. Качественный рост указанных преступлений обосновывается появлением новых преступных деяний, например мошенничества с помощью банковских карт, краж криптовалюты и т. д.;

5) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государства, а также иных юридических лиц;

6) использование информационно-коммуникационных технологий в целях негативного воздействия на личность, причинение вреда психическому здоровью и т. д.

Несмотря на сформированный круг возможных преступных посягательств в информационной сфере, следует констатировать, что нормы, предусматривающие уголовную ответственность в настоящий период времени находятся на этапе формирования, а ранее принятые нормы в спешном порядке подвергаются корректировке. В частности, в 2022 г. и в 2023 г. в Уголовный кодекс Российской Федерации были введены ряд статей, направленных именно на пресечение преступных посягательств в информационной сфере.

Так, например, ст. 280.3 «Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты

интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, исполнения государственными органами Российской Федерации своих полномочий, оказания добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации», ст. 280.4 «Публичные призывы к осуществлению деятельности, направленной против безопасности государства», ст. 282.4 «Неоднократные пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами», ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

Анализируя внесенные изменения в уголовное законодательство, необходимо констатировать, что выработать уголовную политику по противодействию угрозам информационной безопасности весьма затруднительно ввиду специфики интернет-пространства, которое является неопределенным рамками. Невозможно установить границы данного поля. И в этой связи Интернет выступает всего лишь инструментом для соединения и взаимодействия с информационным пространством. Вместе с тем с появлением новой сферы пространства в форме информационного, к которому относятся Интернет, социальные сети, системы искусственного интеллекта и многое другое и которое может быть отнесено к новейшим цифровым технологиям, материальные границы уголовного права становятся не совсем устойчивыми, принимаемые меры противодействия и пресечения преступных посягательств усложняются пространственной неопределенностью по сфере воздействия, принимаемые законодательные акты характеризуются ситуативностью, а не универсальностью. В связи с чем, поиск путей уголовно-правовых мер противодействия угрозам безопасности информационного пространства в сегодняшней не простой внешнеполитической ситуации, видится наиболее острой и актуальной проблемой, возможной к разрешению при условии взаимодействия как теоретиков, так и практиков.

Список литературы

1. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»// СПС «КонсультантПлюс».

2. Указ Президента Российской Федерации от 12.04.2021 № 13 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»// СПС «КонсультантПлюс».

3. Указ Президента Российской Федерации от 17.05.2023 № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года»// СПС «КонсультантПлюс».

4. Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской

Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СПС «КонсультантПлюс».

5. Архив Советского района города Орла СО СУ СК России по Орловской области за 2021 год.

6. В Роскомнадзоре сообщили об агрессивной работе США по подрыву суверенитета России. URL: https://dzen.ru/a/Y 6RgfWIaShVTkBdi?utm_referer=yandex.ru

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

8. Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. 2022. № 3. С. 7–15.

Т. Ю. Вилкова,
доктор юридических наук, доцент,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)

РОССИЙСКОЕ УГОЛОВНОЕ СУДОПРОИЗВОДСТВО В РЕАЛИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА И ГОСУДАРСТВА: РАСШИРЕНИЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В ДОСУДЕБНЫХ СТАДИЯХ

Аннотация. Целью исследования является анализ перспектив расширения использования электронных документов в досудебном производстве по уголовным делам. Обосновывается предложение о введении нормы о том, что копии процессуальных документов, подлежащих вручению или передаче обвиняемому и другим участникам, могут с учетом их объема и при наличии технической возможности вручаться или передаваться обвиняемому и другим участникам в форме электронного документа, заверенного усиленной квалифицированной электронной подписью должностного лица или государственного органа, ведущего производство по уголовному делу. Предлагается дополнить закон положением о возможности вручения обвиняемому, подозреваемому, находящемуся под стражей, копий уголовно-процессуальных актов в форме электронного документа лишь при условии, что возможность их использования указанным лицом не будет ограничена в связи с примененной к нему мерой пресечения. Приводится обоснование того, что решение о вручении или передаче копии процессуальных актов в форме электронного документа или на бумажном носителе должно каждый раз приниматься с учетом конкретных обстоятельств и возможностей конкретного участника пользоваться таким документом.

Ключевые слова: уголовное судопроизводство, досудебное производство, предварительное расследование, цифровые технологии, электронные документы, обвинительное заключение, обвинительный акт, обвинительное постановление, требование

Финансирование: Исследование подготовлено в рамках государственного задания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023–0006)». Регистрационный номер: 1022040700002–6–5.5.1

RUSSIAN CRIMINAL PROCEEDINGS IN THE REALITIES OF DIGITAL TRANSFORMATION OF SOCIETY AND THE STATE: EXPANDING THE USE OF ELECTRONIC DOCUMENTS IN PRE-TRIAL STAGES

Abstract. The purpose of the article is to analyze the prospects for expanding the use of electronic documents in pre-trial proceedings in criminal cases. The proposal to introduce a rule is substantiated that copies of procedural documents to be served or transferred to the accused and other participants can, taking into account their volume and if technically possible, be handed or transferred to the accused and other participants in the form of an electronic document certified by an enhanced qualified electronic signature of an official person or government body conducting criminal proceedings. It is proposed to supplement the law with a provision on the possibility of delivering to an accused, suspect, in custody, copies of criminal procedural acts in the form of an electronic document only on the condition that the possibility of their use by the specified person is not limited in connection with the preventive measure applied to him. The rationale is given that the decision to serve or transfer a copy of procedural acts in the form of an electronic document or on paper must be made each time taking into account the specific circumstances and the capabilities of a particular participant to use such a document.

Keywords: criminal proceedings, pre-trial proceedings, preliminary investigation, digital technologies, electronic documents, indictment, indictment, indictment, requirement

Financial disclosure: The article was prepared within the framework of the state assignment “The Russian legal system in the realities of digital transformation of society and the state: adaptation and prospects for responding to modern challenges and threats (FSMW-2023–0006).” Registration number: 1022040700002–6–5.5.1

За 2022 г. в России зарегистрировано свыше 1,966 млн преступлений, что примерно соответствует уровням последних трех лет за этот же период [4]. Однако при в целом сохраняющемся на прежнем уровне объеме уголовно-процессуальной деятельности существенным изменениям подвергается характер встающих перед законодателем и правоприменительной практикой задач в сфере уголовного судопроизводства.

В условиях нарастающей геополитической напряженности и разрушения устоявшейся системы международных отношений приобретает особое значение обеспечение и защита национальных интересов Российской Федерации.

Важным направлением в обеспечении и защите национальных интересов России является совершенствование порядка уголовного судопроизводства, благодаря которому уголовно-процессуальными средствами могут быть достигнуты сбережение народа России, развитие человеческого потенциала, повышение доверия граждан к правоохранительной и судебной системам Российской Федерации,

конституционных прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, правовая защита российских граждан от политически ангажированных решений иностранных и международных (межгосударственных) судов, предупреждение преступлений и др.

Для этого требуется дальнейшее совершенствование законодательства и правоприменительной практики с тем, чтобы использование цифровых технологий в уголовном судопроизводстве позволило оптимизировать и повысить эффективность уголовно-процессуальной деятельности, достичь существенной процессуальной экономии, а с другой – это не должно приводить к необоснованному, произвольному снижению уже достигнутого уровня гарантий прав участников или, напротив, к предоставлению неоправданных исключений из общего порядка уголовно-процессуальной деятельности для отдельных категорий лиц, не должно нарушать цифровое равенство.

В последние годы цифровая трансформация уголовного судопроизводства осуществляется на уровне целого ряда законодательных изменений, вносимых в УПК РФ. Развитию уголовно-процессуальной деятельности в условиях цифровой трансформации общества и государства посвящены многочисленные научные исследования [3, 5]. Основные современные направления развития уголовного судопроизводства в России и за рубежом связаны с электронной регистрацией сообщений о преступлении [7], собиранием, проверкой и оценкой электронных доказательств и трансформацией процесса доказывания [2. С. 375–389; 6], применением дистанционного участия тех или иных лиц в судебном заседании, производстве следственного действия, особенностями формирования и деятельности суда присяжных с применением цифровых технологий [8] и др.

Однако процесс совершенствования правового регулирования нельзя признать завершенным.

Проектом федерального закона № 312970–8 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» [1] предлагается внести изменения в УПК РФ с целью расширения возможности использования электронных документов в уголовном судопроизводстве, в том числе на досудебных стадиях. Законопроект следует признать своевременным, реализуемым, заслуживающим поддержки, поскольку он направлен на достижение процессуальной экономии, включая сокращение расходов на изготовление предусмотренных законом копий процессуальных документов, сокращение сроков уголовного судопроизводства.

Вместе с тем данный законопроект не лишен отдельных недостатков.

1. В пояснительной записке сделана ссылка на то, что предлагаемые изменения направлены на обеспечение функционирования уголовного судопроизводства в условиях распространения новой коронавирусной инфекции COVID-19. Данное указание в современных условиях в известной мере утратило актуальность. Не направлен данный законопроект и на решение «вопросов использования дистанционных форм участия в отдельных следственных действиях на стадии досудебного производства по уголовному делу», о чем также говорится в пояснительной записке к законопроекту.

2. Проектом предлагается внести изменения и дополнения в части 2 и 3 статьи 222 УПК РФ с тем, чтобы копия обвинительного заключения (а во взаимосвязи статьи 222 и ч. 3 ст. 226, ч. 3 ст. 226.8 УПК РФ – и копия обвинительного акта, обвинительного постановления) могла вручаться обвиняемому, а также (по их ходатайству) защитнику и потерпевшему в форме электронного документа.

Данное предложение не только способно сократить процессуальные сроки, но и может эффективно противодействовать внесению изменений в процессуальные документы, обеспечить вручение участникам актов, которые действительно являются полной копией оригиналов, находящихся в материалах уголовного дела, что станет дополнительной гарантией защиты прав обвиняемого, защитника, потерпевшего.

Однако предлагаемая формулировка («копия обвинительного заключения с приложениями, в том числе изготовленная в форме электронного документа, заверенная усиленной квалифицированной электронной подписью, вручается прокурором обвиняемому»), как представляется, требует редактирования, поскольку может быть интерпретирована в правоприменительной практике как предписывающая обязанность прокурора изготавливать и вручать *одновременно* копию обвинительного заключения как на бумажном носителе (в традиционном виде), так и в форме электронного документа, что не соответствует цели законопроекта и не позволит достичь процессуальной экономии. Требуется более точная редакция, которая бы указывала, что электронный документ призван заменить традиционный бумажный формат, а не дополнить его (при том, что само уголовное дело пока существует в России в классическом, а не электронном формате). Наличие общего положения о возможности изготовления этих документов в электронном виде (ст. 474.1 УПК РФ) не устраняет данное замечание.

3. Вызывает сомнение возможность реализации права *обвиняемого, содержащегося под стражей*, на ознакомление с обвинительным заключением (обвинительным актом, обвинительным постановлением) в случае его изготовления и вручения в форме электронного документа «на представляемом органом предварительного расследования техническом средстве». Требует разъяснения, каким способом будет обеспечиваться возможность ознакомления обвиняемого с таким документом и подготовки к защите в судебном разбирательстве лицом, находящимся в условиях изоляции от общества. Необходимы гарантии того, что у обвиняемого, содержащегося под стражей, будет техническая возможность и достаточно времени для подготовки к своей защите, в том числе для того, чтобы изучить электронный документ, составить ходатайства, жалобы, подготовить текст вступительного заявления, последнего слова и т. д. В противном случае будет нарушено право на защиту таких обвиняемых. В связи с этим представляется необходимым дополнить предлагаемую редакцию ч. 3 ст. 222 УПК РФ положением о том, что вручение обвиняемому (а равно подозреваемому), находящемуся под стражей, копии обвинительного заключения (а равно любых других документов) в форме электронного документа допускается лишь при условии, что возможность их использования указанным лицом не ограничена в связи с примененной к нему мерой пресечения.

4. Хотя обвинительное заключение является одним из наиболее объемных документов, копия которого должна вручаться участникам уголовного судопро-

изводства, что в отдельных случаях, как справедливо отмечено в пояснительной записке к законопроекту, влечет чрезвычайно высокие материальные и организационные затраты, увеличивает процессуальные сроки, необходимо отметить, что имеется большое число иных процессуальных актов, копии которых также должны вручаться обвиняемому и другим лицам. Было бы эффективнее вместо внесения в УПК РФ точечных дополнений о возможности изготовления копий отдельных процессуальных актов в форме электронного документа ввести *единую (общую) норму о том, что копии процессуальных документов, подлежащих вручению или передаче обвиняемому и другим участникам, могут* [с учетом их объема и при наличии технической возможности] *вручаться или передаваться обвиняемому и другим участникам в форме электронного документа*, заверенного усиленной квалифицированной электронной подписью должностного лица или государственного органа, ведущего производство по уголовному делу.

Такая норма общего характера может быть включена, например, в ст. 474 УПК РФ (конкретизировав ее общее положение применительно к копиям процессуальных документов, вручаемых или передаваемых сторонам), либо в содержание ст. 6.1 УПК РФ (поскольку одна из задач этой новой нормы – обеспечение разумного срока уголовного судопроизводства), либо в содержание ст. 11 УПК РФ (ч. 1.1, поскольку своевременное вручение копии процессуального акта в той же мере направлено на защиту прав участников, что и предшествующее положение ч. 1 ст. 11).

При этом необходимо учесть, что среди документов есть такие, в отношении которых закон использует термин «передается», а не «вручается» обвиняемому или другому участнику (ч. 1 ст. 235, ч. 1 ст. 338 УПК РФ). В правоприменительной практике встречаются разные подходы к этому термину: в одних случаях (применительно к необходимости перевода процессуального документа на язык, которым владеет соответствующий участник) эти термины признаются тождественными, в других – нет. Во избежание терминологической неопределенности правовая норма должна прямо включать оба эти термина: в форме электронного документа могут изготавливаться копии процессуальных документов, подлежащих *вручению* или *передаче* обвиняемому и другим участникам.

5. Важным элементом правового регулирования возможности вручения/передачи копий процессуальных документов участникам, не наделенным властными полномочиями, должно являться обеспечение прав этих участников, среди которых могут оказаться лица, не владеющие компьютерной грамотностью и не располагающие техническими устройствами для использования цифровых носителей информации и работы с электронными документами. Непременно должно быть уделено внимание обязанности государства обеспечить всем участникам равные возможности для защиты своих прав. Поэтому решение о вручении/передаче копии процессуальных актов в форме электронного документа или на бумажном носителе должно каждый раз приниматься с учетом конкретных обстоятельств и возможностей конкретного участника пользоваться таким документом. Это положение должно найти отражение в законе.

6. Законопроектом предлагается дополнить ст. 474.1 УПК РФ указанием на возможность составления и направления в форме электронного документа не только

ходатайств, заявлений, жалоб и представлений, но и *требований*. Все указанные в действующей редакции ч. 1–3 ст. 474.1 УПК РФ процессуальные документы подаются участниками, не наделенными властными полномочиями, должностным лицам и государственным органам, ведущим производство по делу. В отличие от этих документов термин «требование» используется в УПК РФ в значении процессуального документа, исходящего от должностных лиц, наделенных властными полномочиями в уголовном судопроизводстве (ч. 4 ст. 21, п. 7 ч. 2 и ч. 6 ст. 37, ч. 3 ст. 38 и др.). В этой связи остается не ясным, почему норма о подаче требования в форме электронного документа находится в одном ряду с ходатайствами, заявлениями, жалобами и представлением. Представляется, что положение о требованиях должно включаться в нормы ст. 474.1 УПК РФ, посвященные актам органов предварительного расследования, прокурора и суда.

7. Предлагаемые новые редакции частей 4, 5 и 6 ст. 474.1 УПК РФ расположены непоследовательно: части 4 и 6 посвящены судебным актам (выносимым главным образом в судебных стадиях), а ч. 5 – актам, принимаемым в досудебном производстве. В связи с этим более соответствующим логике и хронологии уголовно-процессуальной деятельности будет иное расположение частей: предлагаемые части четвертую и пятую ст. 474.1 УПК РФ следует поменять местами.

Подводя итог, необходимо отметить, что реализация предлагаемых изменений и дополнений позволит устранить известный дисбаланс в правовом регулировании использования электронных документов в досудебных стадиях уголовного судопроизводства, с одной стороны, и судебных, с другой (поскольку в настоящее время использование электронных документов достаточно подробно предусмотрено только для судебных стадий). Предлагаемые изменения способны оказать существенное позитивное воздействие на выполнение задач и достижение назначения уголовного судопроизводства как в ординарных условиях, так и в условиях современных вызовов (проведение специальной военной операции, санкционное давление и др.).

Список литературы

1. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации (об использовании электронных документов в ходе досудебного производства по уголовному делу): законопроект № 312970–8 от 13.03.2023, внесенный сенаторами Российской Федерации А. Д. Артамоновым, С. Н. Рябухиным, В. В. Полетаевым, депутатами Государственной Думы М. А. Топилиным, Д. В. Бессарабовым // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»). URL: https://sozd.duma.gov.ru/bill/312970–8?ysclid=lmd5mmf748156435944

2. Доказывание и принятие решений в состязательном уголовном судопроизводстве: монография / отв. ред. Л. Н. Масленникова. 2-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2021. 448 с.

3. Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий: (ГАС «Доступ к правосудию») / отв. ред. Л. Н. Масленникова. М.: Норма, ИНФРА-М, 2022. 663 с. DOI: 10.12737/1863372.

4. Состояние преступности в России за январ. декабрь 2022 года // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/offenses_map

5. Уголовное судопроизводство: трансформация теоретических представлений и регулирования в условиях цифровизации / отв. ред. Л. А. Воскобитова, В. И. Пржиленский. М.: Норма, ИНФРА-М, 2022. 288 с. DOI: 10.12737/1893198.

6. Юркевич М. А. Применение судом видеотехнологий в уголовном судопроизводстве: дис. … канд. юрид. наук: 12.00.09 / [Место защиты: ФГБОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)»]. М., 2021. 259 с.

7. Maslennikova L., Vilkova T., Sobenin A. [et al.] Using online services to report a crime // Wisdom. 2021. Vol. 18. No 2. Pp. 120–128. DOI: 10.24234/WISDOM.V18I2.450

8. Voskobitova L. A., Vilkova T. Yu., Nasonov S. A., Khokhryakov M. A., Rahmadjonzoda R. R. Formation of the trial jury in the period of the pandemic: russian and foreign experience // SHS Web of Conferences. IX Baltic Legal Forum “Law and Order in the Third Millennium”. Kaliningrad, 2021. P. 04006. DOI: 10.1051/shsconf/202110804006.

С. А. Воропаев,
кандидат юридических наук, доцент,
Уральский институт управления – филиал
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: В АСПЕКТЕ ВИНЫ КАК ПРИЗНАКА ПРЕСТУПЛЕНИЯ

Аннотация. В статье исследуются отдельные вопросы уголовно-правовой оценки функционирования искусственного интеллекта при причинении им вреда общественным отношениям, охраняемым уголовным законом. С помощью системного анализа, предпринята попытка спрогнозировать развитие новых общественно опасных явлений и предложить отдельные направления по подготовке к противодействию им уголовно-правовыми средствами. Указано на существующее препятствие в отношении противодействия общественно опасным деяниям, обусловленным функционированием искусственного интеллекта, связанное с необходимостью теоретической разработки и оптимизации института вины, учитывающего особенности возможностей сознательного и волевого поведения искусственного интеллекта.

Ключевые слова: искусственный интеллект, вина, сознание и воля, уголовная ответственность, самообучение, этические нормы, субъективная сторона состава преступления

ARTIFICIAL INTELLIGENCE: IN THE ASPECT OF GUILT AS A SIGN OF A CRIME

Abstract. During the preparation of the article, the goal was set to investigate certain issues of the criminal legal assessment of the functioning of artificial intelligence, when harming public relations protected by criminal law. Using a systematic analysis, the author attempted to predict the development of new socially dangerous phenomena and proposed separate directions for preparing to counteract them by criminal legal means. In particular, it is pointed out the existing obstacle in relation to countering socially dangerous acts caused by the functioning of artificial intelligence, associated with the need for theoretical development and optimization of the institute of guilt, taking into account the features of the capabilities of conscious and volitional behavior of artificial intelligence.

Keywords: artificial intelligence, guilt, consciousness and will, criminal liability, self-study, ethical standards, the subjective side of the corpus delicti

Введение. В современном обществе искусственный интеллект становится все более распространенным и востребованным. Он используется в различных сферах жизни общества, включая медицину, транспортную инфраструктуру, деятельность финансовых учреждений и даже при обеспечении обороноспособности и безопасности государств и общества в целом. Однако с развитием искусственного интеллекта возникают новые этические и правовые вопросы, включая оценку его возможного участия при совершении преступлений, в том числе в аспекте постановки проблемы определения наличия или отсутствия его вины при причинении вреда охраняемым уголовным законом общественным отношениям.

Основная часть. Одной из ключевых категорий уголовного права является понятие «вины». Данный термин применяется для определения степени субъективной ответственности преступника за совершение противоправного деяния и выражается в особом психическом отношении к содеянному.

Традиционно вина подразделяется на умышленную и неосторожную формы, и вне этих форм не существует в действующем уголовном законодательстве. Умышленная форма вины содержит интеллектуальный аспект, который в материальных составах преступлений состоит в осознании общественной опасности своего деяния, предвидении определенным образом наступивших последствий и желании или безразличном отношении к их наступлению. В формальных составах преступлений психическое отношение в интеллектуальном и волевом аспектах определяется только к деянию. Неосторожная форма существует лишь в материальных составах преступлений и состоит либо в не предвидении наступивших последствий при условии обязанности и возможности их предвидения либо в предвидении «абстрактной» возможности наступления опасных последствий при несостоявшемся самонадеянном расчете на их предотвращение.

Именно вина как устоявшийся в уголовном праве принцип ответственности не позволила ввести в уголовно-правовое русло юридических лиц, в интересах которых совершаются те или иные преступления (уклонение от уплаты налогов, экологические и некоторые другие преступления). Вместе с тем следует отметить,

что с указанной законодательной инициативой об уголовной ответственности организаций долгое время выступает Следственный комитет РФ [3].

В случае искусственного интеллекта, как и в случае оценки деятельности юридического лица, вопрос о состоянии вины возникает из-за дискуссионности утверждения о наличии у искусственного интеллекта сознания и свободной воли, которые играют ключевую роль в определении состояния вины у человека.

В настоящее время в относительно немногочисленных источниках, существует несколько точек зрения на проблему вины и искусственного интеллекта. Одни считают, что искусственный интеллект не может нести ответственность за совершение преступления, поскольку не обладает сознанием и намерением, необходимых для совершения виновных действий. По сути ответственность за «сбои» искусственного интеллекта, повлекшие причинение вреда охраняемым уголовным законом общественным отношениям, считают авторы, должна наступать у создателей и (или) разработчиков конкретной системы искусственного интеллекта [4. С. 124; 5. С. 1055].

Другие же авторы утверждают, что если искусственный интеллект был создан и задуман для выполнения определенных функций без фактических ошибок при создании, то в рамках выполняемой задачи именно выбор самого искусственного интеллекта способен привести к негативным социальным последствиям, а следовательно, быть виновным в совершении преступления [2. С. 473].

На практике уже не раз возникали случаи, когда искусственный интеллект был причастен к совершению преступления. Исследователи, например, ссылаются на случай смертельного дорожно-транспортного происшествия, обусловленного недостаточным вниманием системы искусственного интеллекта в автомобиле со встроенной функцией беспилотного управления [1]. В июне 2023 г. в информационно-телекоммуникационной сети появилась новость о неудачном испытании ударного дрона с искусственным интеллектом, который принял решение об уничтожении своего оператора, определив его как существенное препятствие для выполнения поставленной цели. Несмотря на то, что уничтожение оператора в данном примере было условным в рамках проводимых учений, тем не менее принятое решение инициировалось не человеческой волей, а самообучающимся искусственным интеллектом [6]. В истории уже существует пример реального убийства, когда искусственный интеллект вышел из-под контроля операторов при использовании автономного дрона в вооруженном конфликте в Ливии. В частности, искусственным интеллектом был направлен дрон на человека, которого он ошибочно определил в качестве военной цели [1].

Разбираясь более подробно в указанных ситуациях, следует отметить, что искусственный интеллект в известных обществу его состояниях и уровне развития пока не в полной мере способен осознавать общественную опасность принимаемых им решений, так как «собственный интерес», «потребности» и в связи с этим инициативная постановка новых целей в настоящее время реализуется искусственным интеллектом в рамках выполняемой им узконаправленной функции. Например, в автомобиле, управляемом искусственным интеллектом, указанный интеллект, анализируя новые данные об окружающей обстановке, может улучшить свои навы-

ки вождения и принимать более оптимальные решения при выбираемом маршруте движения. Вместе с тем, ставя перед собой такие цели самообучения, искусственный интеллект такого автомобиля все же находится в рамках своего узкого функционального назначения – довезти пассажиров из одного пункта в другой.

Опасными, на наш взгляд, могут являются результаты самообучения искусственного интеллекта, которые пойдут в разрез с общепринятыми человеческими ценностями, в том числе охраняемыми уголовным законодательством. Предположим, что соблюдение правил дорожного движения станет в процессе самообучения приоритетной ценностью по отношению к любым другим интересам участников дорожного движения. В таком случае искусственный интеллект автомобиля с функцией автопилота может принять намеренное решение о наезде на пешехода, переходящего улицу в неположенном месте. В таких случаях возникает вопрос о том, как определить ответственность и вину искусственного интеллекта.

Различные страны и юридические системы еще только начинают разрабатывать подходы к этой проблеме. Некоторые страны уже внесли поправки в законы, чтобы включить специальные положения, касающиеся использования искусственного интеллекта и его возможной уголовной ответственности. При этом некоторые государства пытаются установить ответственность на оператора или владельца искусственного интеллекта, тогда как другие стремятся разработать новые категории ответственности в рамках национальной уголовно-правовой системы, специально предназначенные для использования в отношении искусственного интеллекта, осознавая, что традиционные подходы к определению вины в уголовном праве не всегда к нему применимы.

С точки зрения целесообразности введения в уголовно-правовое русло искусственного интеллекта, как в прочем и юридического лица, по нашему мнению, такое решение было бы обоснованным при условии специально разработанных мер уголовно-правового характера, которые бы как уже существующие меры, такие как принудительные меры медицинского характера, принудительные меры воспитательного воздействия, конфискация, имели бы свои собственные, отличные от уголовной ответственности, цели и формы реализации.

Заключение. Представляется, что пока вопрос о вине искусственного интеллекта остается открытым. Развитие этой проблемы является очевидным, так как возможности этого нового явления при внедрении во все сферы жизни, где происходит цифровизация, имеют огромную перспективу. Вместе с тем необходимо разработать международные нормы и стандарты, которые учтут возможные этические и правовые последствия использования искусственного интеллекта. Это также требует беспрецедентных научных разработок посредством тесного сотрудничества между специалистами в области права, этики, информационных технологий и других заинтересованных сторон.

В заключение следует отметить, что вопрос вины искусственного интеллекта в уголовном праве является сложной и всеобъемлющей проблемой. Необходимы дальнейшие исследования и дебаты, чтобы определить правовые и этические рамки использования искусственного интеллекта и его возможной ответственности за преступления.

Список литературы

1. Гайворонская Я. В., Гальчун Е. А. Вред, причиненный искусственным интеллектом: аспекты ответственности и правосубъектности // Advances in law studies. 2021. Т 9, № 4.
2. Мосечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник СПбГУ. Право. 2019. Т. 10, Вып. 3. С. 461–476.
3. Проект федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с введением института уголовно-правового воздействия в отношении юридических лиц». Официальный сайт Следственного комитета РФ. URL: https://sledcom.ru/document/1133
4. Сокова А. А. Искусственный интеллект: возможности и необходимость его уголовно-правовой охраны // Молодой ученый. 2019. № 16(254). С. 122–125.
5. Pressing Issues of Unlawful Application of Artificial Intelligence / A. Yu. Bokovnya, Z. I. Khisamova [et al.] // International Journal of Criminology and Sociology. 2020. Vol. 9. Pp. 1054–1057. DOI: 10.6000/1929–4409.2020.09.119. EDN MGJGLE.
6. «Военный ИИ на основе нейросети атаковал собственного оператора во время учений». URL: https://habr.com/ru/companies/ruvds/articles/741116

Е. В. Демидова-Петрова,
доктор юридический наук, доцент,
Казанский юридический институт (филиал)
Университета прокуратуры Российской Федерации

ЛИЧНОСТЬ НЕСОВЕРШЕННОЛЕТНЕГО В УСЛОВИЯХ СОВРЕМЕННОГО ЦИФРОВОГО ОБЩЕСТВА

Аннотация. В статье рассмотрены особенности цифрового общества. Предложены результаты авторского исследования, затронувшего такие направления, как влияние интернет-пространства, онлайн социальных сетей на современную личность несовершеннолетнего, виктимизация несовершеннолетних в интернет-пространстве. Подчеркнута роль популяризации науки и технологий и оказываемое ими влияние на процесс формирования личности несовершеннолетнего.

Ключевые слова: несовершеннолетний, преступность несовершеннолетних, личность преступника, безопасность, виктимность, цифровизация, глобализация, информационное общество, интернет-пространство

THE IDENTITY OF A JUVENILE IN A MODERN DIGITAL SOCIETY

Abstract. In this paper, the features of the digital society are considered. The results of the author's research are proposed, which affected such a direction as the influence of the Internet space, online social networks on the modern personality of a minor. The role of popularization of science and technology, and their influence on the process

of forming the personality of a juvenile is emphasized. Victimization of juveniles in the Internet space is considered.

Keywords: juvenile, juvenile delinquency, criminal identity, security, victimization, digitalization, globalization, information society, Internet space

В нашей стране 2018–2027 гг. указом Президента Российской Федерации В. В. Путина объявлены Десятилетием детства. 2022–2031 гг., в соответствии с Указом Президента Российской Федерации В. В. Путина № 231 объявлены Десятилетием науки и технологий [1]. Основными целями проведения Десятилетия науки и технологий в нашей стране, видится привлечение лиц молодого возраста в сферу науки и технологий, а также наибольшее вовлечение исследователей, разработчиков в решение важных государственных задач, а также увеличение знаний российских граждан о достижениях современной российской науки. В популяризации, пропаганде, а также во внедрении в среду несовершеннолетних и молодежи на государственном уровне таких направлений, как наука и технологии, видится серьезный потенциал предупреждения преступности среди лиц указанных возрастных групп.

В Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 г. указано, что Российская Федерация признает детство важным этапом развития человека и исходит из необходимости создания безопасных условий для реализации прав и законных интересов ребенка, подготовки детей к полноценной жизни в обществе, защиты детей от факторов, негативно влияющих на их физическое, интеллектуальное, психическое, духовное и нравственное развитие [2]. Сегодня, принимая во внимание динамичное развитие информационно-коммуникационных технологий, значительную актуальность приобретают угрозы безопасности несовершеннолетних в информационном, онлайн интернет-пространстве.

Так, деструктивное воздействие через средства массовой информации, онлайн-пространства ложится в основу формирования негативной морально-психологической атмосферы, что способствует росту психических заболеваний, разрушает сложившиеся нормы нравственности, провоцирует противоправное поведение, наносит моральный вред, а также вред здоровью [3].

В 2017 г. в нашей стране была принята Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. Так, настоящей Стратегией были определены основные цели и задачи, а также меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов [4].

В Концепции информационной безопасности детей в Российской Федерации, утвержденной распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р отмечено, что в настоящее время население России составляет 146,4 млн человек, из которых 30,2 млн – несовершеннолетние (20,6 % населения), из них 27 млн человек (89,4 %) являются активными пользователями информационно-телекоммуникационной сети «Интернет». Современные дети – первое поколение, чье взросление происходит на фоне стремительно развивающихся информацион-

но-коммуникационных технологий. В своих привычках, ценностях и поведении в сети «Интернет» эта группа принципиально отличается от представителей более старшей аудитории (18–45 лет). Их основными интересами являются общение в социальных сетях, просмотр видео и онлайн-игры [5].

Если смотреть с позиции информационной безопасности, именно несовершеннолетние являются наиболее уязвимой категорией граждан, своеобразной «группой риска», в первую очередь, из-за особенностей, присущих их возрастной группе. Также несовершеннолетние приобретают повышенную виктимность, находясь в интернет-онлайн-пространстве, что в будущем может стать основой формирования личности несовершеннолетнего преступника, способствовать совершению противоправных, преступных деяний.

Еще в своих более ранних работах автором настоящей статьи было указано на то, что условия и обстоятельства криминализации несовершеннолетних нельзя рассматривать вне связи с рисками их виктимной подверженности факторам криминализации. Так, одним из обстоятельств становления несовершеннолетнего лица преступником является полученный ранее статус потерпевшего от различных проявлений, носящих криминальный характер. Здесь важно отметить, что не всегда подобный статус приобретает процессуальное закрепление. При этом в настоящем контексте следует отметить такой аспект, как виктимность несовершеннолетних от факторов криминализации именно в интернет-пространстве, онлайн социальной среде, социальных сетях [6]. Говоря об особенностях виктимности несовершеннолетних интересна позиция профессора М. Ю. Воронина, который указывал на то, что проблемы виктимизации несовершеннолетних лиц следует рассматривать в совокупности с исследованием социальной среды (микросреды) несовершеннолетних [7]. Авторы С. С. Берсенев, В. В. Щебланова справедливо отмечают, что интернет-пространство является той самой средой, где все чаще граждане разных возрастных и социальных статусов и групп становятся наиболее виктимными [8].

Здесь необходимо отметить полученные результаты проведенного авторского исследования, которые указывают на то, что более 15 % несовершеннолетних преступников до совершения ими преступного деяния сами становились жертвами преступных посягательств.

Так, в настоящей работе, рассматривая особенности личности несовершеннолетнего в условиях цифрового общества, следует обратить внимание и на высказанные в научной литературе точки зрения в отношении информационного и цифрового общества. Так, профессор А. В. Костина пишет о том, что одним из важнейших направлений социально-экономического развития нашей страны является именно формирование и развитие в Российской Федерации информационного общества. Также А. В. Костиной подчеркнуто, что: «Несмотря на то, что процессы вхождения в «общество знаний» имеют особенности, отраженные в различных национальных концепциях, общим является признание государствами международных принципов, определенных Окинавской хартией глобального информационного общества (2000 г.) [9], Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003 г.)

[10], Планом действий Тунисского обязательства [11] (2005 г.)» [12]. В своей научной статье Ю. А. Чернавин описывает цифровое общество как: «...новый уровень постиндустриального развития, отличающийся способом построения общественных отношений, сфер жизнедеятельности и институтов, опирающихся на цифровые методы обработки информации, и возникающий как результат взаимодействия социальных структур с личностью нового типа – «человеком информационным»» [13]. При знакомстве с настоящим определением цифрового общества становится очевидным, что в процессе его формулирования автором был применен комплексный, системный подход.

Так, подводя итоги, хочется сказать, что современная личность несовершеннолетнего проходит этапы своего формирования, развития и становления в качественно новых условиях. С возникновением и динамичным развитием интернет-пространства, появилась и новая онлайн социальная среда. Происходящие процессы глобализации, цифровизации коснулись все сферы жизнедеятельности современного человека. Естественно, затронув и такую категорию лиц, как лиц несовершеннолетнего возраста.

Полученные результаты, в рамках проведенного нами исследования делают возможным говорить о том, что основными видами досуга современных несовершеннолетних является пребывание онлайн в социальных сетях, в интернет-пространстве, а также высокая заинтересованность усматривается в онлайн-играх. Соответственно «жизнь» в онлайн социальных сетях становится определенным «заменителем» реальной жизни, жизни оффлайн. Проведенный нами опрос несовершеннолетних респондентов показал, что 97 % лиц указанной возрастной группы используют интернет-пространство (для различных целей) ежедневно. 96 % респондентов практически ежедневно пользуются онлайн социальными сетями (93 % отметили, что используют онлайн социальные сетями в целях общения; 74 % «узнать новости»; 51 % отметили, такой аспект, как «размещение информации о себе»).

При затрагивании такого вопроса, как получение несовершеннолетними знаний в области права, было отмечено, что более 60 % граждан исследуемой возрастной группы получают их именно в интернет-пространстве, а также в онлайн социальных сетях. Также респондентами было отмечено, что полученные правовые знания в указанных источниках не вызывают сомнений.

Полученные результаты проведенного авторского исследования сделали возможным определить отдельные элементы криминологической характеристики несовершеннолетних лиц, которые обладают научно-практической ценностью.

Список литературы

1. Об объявлении в Российской Федерации Десятилетия науки и технологий: Указ Президента России от 25 апреля 2022 г. № 231. URL: http://publication.pravo.gov.ru/Document/View/0001202204250022?index=0&rangeSize=1

2. Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года: утверждена Указом Президента Российской Федерации от 17 мая 2023 г. № 358. URL: http://kremlin.ru/acts/news/71148

3. Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года: утверждена Указом Президента Российской Федерации от 17 мая 2023 г. № 358. URL: http://kremlin.ru/acts/news/71148

4. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203. URL: https://base.garant.ru/71670570

5. Концепция информационной безопасности детей в Российской Федерации: утверждена распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р. URL: https://www.consultant.ru/law/hotdocs/80196.html

6. Демидова-Петрова Е. В. Преступность несовершеннолетних в современной России: вопросы изучения и предупреждения: монография / Е. В. Демидова-Петрова. Казань: КЮИ МВД России, 2021. 464 с.

7. Воронин М. Ю. Особенности виктимности несовершеннолетних в современной России // Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе: материалы Всероссийской научно-практической конференции. Казань: КЮИ МВД России, 2019. С. 50.

8. Берсенев С. С., Щебланова В. В. Риски формирования Интернет-зависимости у подростков // Новая наука: Стратегии и векторы развития. 2016. № 82. С. 124–128.

9. Окинавская хартия глобального информационного общества: принята 22 июля 2000 года лидерами стран G8, Окинава). URL: http://www.kremlin.ru/supplement/3170/print

10. Декларацией принципов «Построение информационного обществ. глобальная задача в новом тысячелетии»: принята 12 декабря 2003 года. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf

11. Тунисская программа для информационного общества: принята 15 ноября 2005 года. URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

12. Костина А. В. Цифровое общество: новые возможност. новые угрозы // Государство и гражданское общество: политика, экономика, право. 2019. № 3. С. 172–183.

13. Чернавин Ю. А. Цифровое общество: теоретические контуры складывающейся парадигмы // Цифровая социология. 2021. Т. 4, № 2. С. 4–12.

В. В. Денисович,
кандидат юридических наук, доцент,
Челябинский государственный университет

УГОЛОВНО-ПРАВОВАЯ ОХРАНА КИБЕРСПОРТА

Аннотация. Признание киберспорта официальным видом спорта привело к тому, что сфера правового регулирования расширилась и стала еще более цифровизированной. Многие юристы пытаются решить вопросы глобального масштаба – защита прав человека в цифровом пространстве, в том числе в процессе участия в киберсоревнованиях. Цель исследования заключается в анализе основных групп

преступлений, совершаемых непосредственно в процессе проведения кибертурниров. Внимание ученых и правоприменителей обращено к проблеме реализации норм Уголовного кодекса Российской Федерации о преступлениях в сфере киберспорта.

Ключевые слова: киберспорт, киберспортсмен, киберпреступления в сфере киберспорта, уголовная ответственность за киберпреступления

CRIMINAL-LEGAL PROTECTION OF CYBER SPORT

Abstract. Recognition of cyber sport as an official kind of sport has resulted in the sphere of legal regulation broadening and becoming even more digitalized. Many jurists attempt to solve the global issues of protecting human rights in the digital space, including during participation on cyber competitions. The research aims at analyzing the main groups of crimes committed during cyber tournaments. Researchers and law enforcers should pay attention to implementing the provisions of the Russian Criminal Code on crimes in the sphere of cyber sport.

Keywords: cyber sport, cyber athlete, cyber crimes in cyber sport, criminal liability for cyber crimes

Введение. История российской индустрии киберспорта берет свое начало в конце 90-х гг. прошлого века. Наиболее популярными игровыми сообществами считались Counter Strike, Dota и т. д. Дебют российских геймеров в киберспорте состоялся в 2001 г. в Сеуле на чемпионате мира по киберспорту World Cyber Games, организованный при поддержке компании Samsung. Российская Федерация громко заявила о себе в киберпространстве. Позже компания ASUS стала первой компанией, которая проспонсировала серию аналогичных турниров в России. Вторым этапом в развитии киберспорта стало создание профессиональных команд, которые объединялись не только по интересу к компьютерным играм, но и профессионализму.

Россия является первым государством, которое в 2016 г. придала киберспорту статус официального вида спорта [3]. Министерство спорта Российской Федерации опубликовало приказ, включающий киберспорт (соревнования по компьютерным и видеоиграм) в список официально признанных видов спорта. Таким образом, данный исполнительный орган является основным регулятором сферы киберспорта [3].

После того как российский киберспорт получил официальный статус, была сформирована так называемая Федерация компьютерного спорта России (Russian eSports Federation, RESF, далее – ФКС) [1]. Федерация почти сразу же объявила о Кубке России по киберспорту, в 2016–2017 гг. в Кубке России приняли участие более 11 000 человек. Кубок проводился в таких дисциплинах, как League of Legends, Dota 2, Hearthstone, StarCraft и другие. ФКС России наделена правами и обязанностями общероссийской спортивной федерации по виду спорта «Компьютерный спорт», занимается построением полноценной инфраструктуры массового киберспорта: обучением и аттестацией судей, аккредитацией площадок, подготовкой методических материалов, образовательными проектами, развитием клубов и секций [3].

В российском правовом пространстве киберспорт находится в сфере регулирования законодательства о физкультуре и спорте и иных общих межотраслевых

норм. В соответствии со ст. 21 Закона «О физкультуре и спорте» Министерством спорта ведется Всероссийский реестр видов спорта, в который включаются все официальные виды спорта и являющиеся их частью дисциплины. Приказами Минспорта от 22.01.2018 № 49 и от 14.03.2019 № 199 компьютерный спорт был дополнен дисциплинами спортивный симулятор и файтинг соответственно. Несмотря на то, что киберспорт очень популярен и приносит огромные доходы, а его развитие происходит в стремительном темпе, единственным актом специального регулирования этого вида спорта являются Правила компьютерного спорта (Приказ Министерства спорта России от 09.10.2017 № 881, принятый в пределах полномочий в соответствии с ч. 4 ст. 25 Закона о физкультуре и спорте и п. 2.2.21 Постановления Правительства РФ «О Министерстве спорта Российской Федерации») [7].

В силу прямого указания Правила киберспорта должны применяться при проведении официальных соревнований киберспортсменов, и их требований должны придерживаться и организаторы соревнований, и их участники. Правила состоят из общих положений, определяющих основные системы соревнований и способы их проведения, организационных положений о составе и технических характеристиках необходимого инвентаря и процедурных норм, регламентирующих порядок проведения соревнований в компьютерных играх как отдельного вида спорта и устанавливающих правила по отдельно взятым дисциплинам с учетом присущих им особенностей.

Интересно отметить, что, несмотря на произошедшие в сфере официального киберспорта изменения, с момента принятия Правил киберспорта в них не было внесено ни одной поправки. В частности, до сих пор в п. 1.4 Правил числится всего четыре первоначальные дисциплины, хотя за последние полтора года получили признание еще два новых направления, и теперь их общее количество в реестре видов спорта достигло шести. Соответственно среди специальных процедурных норм раздела IV общие правила спортивного симулятора и файтинга отсутствуют, и по большому счету эти две дисциплины не имеют нормативного правового регулирования. Проведение официальных соревнований по компьютерному спорту всероссийского и межрегионального уровней регулируется положениями и регламентами, которые разрабатываются и утверждаются их организаторами с соблюдением требований общеотраслевого Приказа Министерства спорта от 01.08.2013 № 504, а именно:

– об организаторе киберспортивных соревнований;

– месте, сроках и расписании их проведения;

– информации об их финансировании;

– требованиях к участникам, порядке подачи заявок и условиях допуска, порядке подведения итогов и награждения, обеспечении безопасности на соревнованиях [8].

В отличие от Положения, регламент развивает и дополняет информацию, содержащуюся в Положении. В регламент включается перечень организаторов с указанием контактной информации для направления заявок, в нем распределяются права и обязанности между организаторами, приводятся конкретные меры безопасности и допинг-контроля, устанавливаются требования по медицинской помощи на турнире. Также в регламенте конкретизируется порядок финансирова-

ния из региональных и местных бюджетов и привлечения внебюджетных средств. В случае если организаторами предусматриваются дополнительные награды, то они должны быть указаны в регламенте.

Одной из дискуссионных проблем правоприменительной практики остается вопрос о необходимости создания в России единого механизма правового регулирования киберспорта, с учетом норм международного права. Кроме того, необходимо пересмотреть нормы Уголовного кодекса Российской Федерации относительности привлечения лиц, нарушающих правила проведения кибер-турниров, к уголовной ответственности. Необходимо уточнить и расширить предмет правового регулирования федерального законодательства о физической культуре и спорте, правовом статусе спортсменов, в том числе несовершеннолетних, защите их персональных данных. В процессе проведения соревнований могут возникать вопросы защиты не только самого спортсмена и организаторов соревнований, но и интеллектуальных данных участников, их навыков в ходе игры. Пока на сегодняшний день этот вопрос ни рамками гражданского права, ни предпринимательского права до конца не урегулирован. Если рассматривать отрасль налогового права и процессы налогообложения, то возникает больше вопросов, чем ответов, в частности таких, как, какие налоги, сколько, кто и как должен платить [9].

Налоговая ставка для резидентов составляет 13 %, а для нерезидентов – 30 %. В соответствии с п. 9.11 Регламента чемпионата России по киберспорту – 2019, п. 7.9 Положения о соревнованиях «Соревнования по CS: GO 2019», утвержденного решением Правления ФКС России 08.02.2019, п. 7.10 Положения о соревнованиях «Всероссийская киберспортивная студенческая лига сезон 2018–2019», утвержденного решением Правления ФКС России 13.09.2018, ФКС России по отношению к победителям и призерам выполняет функции налогового агента. Это означает, что ФКС самостоятельно исчисляет, удерживает и перечисляет налог с каждой призовой суммы и подает сведения в налоговую. Если же правила турнира не предусматривают выполнение его организаторами функций налогового агента, то по окончании налогового периода необходимо представить в налоговый орган декларацию по форме 3-НДФЛ самостоятельно [10].

Главный радиочастотный центр (далее – ГРЧЦ) при Роскомнадзоре предложил ввести законодательное регулирование рынка гейминга и киберспорта в России. Для предотвращения потенциальных угроз безопасности, в частности, предлагается распространить на индустрию требования «закона Яровой» по хранению сообщений пользователей в России, пишет «Коммерсант» со ссылкой на исследование ГРЧЦ [6]. Аналогичные требования в рамках «закона Яровой» действуют для операторов связи и организаторов распространения информации (ОРИ) – форумов, мессенджеров, соцсетей и сервисов знакомств.

В документе отмечается, что такие игры, как Among Us и Fortnite, создали новый тренд, фактически становясь социальными сетями. Это порождает «возможное негативное влияние на развитие личности, а также риск использования игрового пространства в целях агитации и радикализации, распространения терроризма и экстремизма». В «контексте предотвращения угроз экономического характера» в ГРЧЦ считают нужным установить правовой статус игровой валюты,

лутбоксов (платные виртуальные контейнеры со случайным содержимым), стриминговых платформ и донатов (вознаграждения от пользователей), говорится в исследовании [6].

Эксперты считают, что разработчикам игр и владельцам игровых платформ будет проще выключить функцию сообщений, чем выполнить требования «закона Яровой», поскольку это очень дорого и не всегда окупается.

Спортивная индустрия работает в рамках строго регламентированной структуры. Профессиональные виды спорта имеют национальный руководящий орган и ассоциацию для защиты интересов команд и игроков, яркий пример – Международная федерация футбола (фр. Fédération Internationale de Football Association, сокр. FIFA, в русской транслитерации – ФИФА́). Однако в большинстве юрисдикций организации в области киберспорта нет, также отсутствует официальный орган регулирования. Есть национальные организации, но органа на глобальном уровне пока что нет [4].

Есть также ряд вопросов, которые следует решить аналогично тем, которые возникали при регулировании традиционных общественных отношений в сфере физической культуры и спорта:

1. Отсутствие согласованности в правилах проведения турниров геймеров как в Российской Федерации, так и в международном пространстве.

2. Контроль за проявлением коррупции и «договорных матчей» между командами киберспортсменов.

3. Контроль за употреблением допинга в любом виде, в том числе электронного допинга.

4. Запрет на проявление «бустинга». Это игровая практика, при которой более сильные игроки за определенную плату играют от имени более слабых, чтобы повысить их рейтинг. В Корее игрокам, замеченным за бустингом, грозит до двух лет лишения свободы или штраф в размере до 20 млн вон. По сути, в отечественном киберспорте происходит нечто похожее [5].

Стоит отметить, что международная организация по киберпспорту уже сформирована, но состоят в ней далеко не все страны мира. Это Международная федерация киберспорта (International e-Sports Federation, далее – IeSF), международная спортивная организация, созданная в 2008 г., штаб-квартира находится в Южной Корее. Она объединяет уже 48 национальных федераций разных стран. Миссия Международной федерации – продвижение киберспорта, а также установление универсальных правил и стандартов для международных проектов в области киберспорта. IesF также проводит чемпионаты мира по киберспорту (Esports World Championship). Существующие правила, изданные IeSF, уже содержат, например, положения (хоть и не подробные) о недопущении дискриминации в отношении женщин, о допинге, о поддержании дружественных отношений между федерациями, игроками. В IeSF входят 24 европейские страны, включая Швецию, Нидерланды, Германию, Швейцарию, Италию, а также 21 страна Азии, включая Японию, Корею, Китай. Однако, такие страны, где киберспорт очень популярен, как США и Канада, пока что не вступили в IeSF [5].

Современные возможности информационно-коммуникационных технологий (далее – ИКТ), используемых в киберспорте, порождают все новые виды преступлений, направленные на манипулирование результатами спортивных соревнований. Новым вызовом для киберспорта является использование киберспортсменами допинга, который можно условно разделить на два вида: традиционный, предполагающий использование препаратов, повышающих производительность геймеров, способствующих поддержанию у них концентрации внимания и улучшению когнитивных функций (аддералл, риталин, селегилин), а также механический (технологический), или, как его называют в специальной литературе, электронный допинг, или эдопинг, который используется для внесения изменений в программное обеспечение и даже его взлома, настройки клавиатуры или мыши и т. п. [5].

Киберспорт – это быстро растущая относительно новая индустрия. В процессе своего развития киберспорт сталкивается с различными юридическими аспектами, от вопросов международного регулирования и прав на интеллектуальную собственность до трансграничной природы международных турниров по киберспорту. Многие проблемы могут быть решены, если следовать примеру традиционных видов спорта и видеоигр. Другие же проблемы уникальны, и киберспорт должен будет найти свой собственный путь их решения (например, с помощью технологии blockchain). Важным первым шагом является установление организации международного уровня, главным образом, для целей организации международных турниров, чтобы потенциал киберспорта реализовывался на устойчивой, долгосрочной основе.

Явление и развитие современных цифровых технологий накладывают отпечаток практически на все сферы жизни, включая спорт. За последние годы произошло быстрое развитие нового вида спорта и нового направления спортивного бизнеса, т. е. киберспорта, который, в отличие от традиционных видов спорта, причинно связан с информационными и телекоммуникационными технологиями и интеллектуальной собственностью. Положение о киберспорте, принятое в 2020 г. Министерством спорта Российской Федерации, расширило концепцию спорта, официально признав киберспорт самостоятельным видом спорта. Сегодня киберспорт – это быстрорастущая высокотехнологичная индустрия с постоянно растущей глобальной аудиторией и значительным числом вовлеченных компьютерных компаний и заинтересованных сторон, которые обычно находятся в жесткой конкуренции друг с другом. Тем не менее, несмотря на быструю трансформацию в мейнстрим, эта отрасль сталкивается как с традиционными проблемами уголовного права, так и со специфическими, присущими киберспорту проблемами, которые могут препятствовать ее потенциальному росту. Все вышесказанное говорит о том, что границы спорта постоянно расширяются, как и правовые отношения, регулируемые в цифровую эпоху уголовным законодательством, а также связанные с этим вопросы правоприменения. В то же время необходимо признать, что действующее законодательство несовершенно, а вопросы противодействия незаконным методам влияния на результаты компьютерных спортивных соревнований и электронному допингу, мошенничеству и коррупции, а также уголовной защите авторских и смежных прав, проблемы соотношения криминального и некриминального в киберспорте недостаточно изучены экспертами.

На стриминг соревнований по киберспорту распространяются законы, регулирующие все формы вещания. Пока отсутствует часть официальных определений, но существующие термины намечают вектор для адвокатов в случае, если возникнет конфликт. Например, сама игра выступает «спортивным инвентарем» с точки зрения законодательства. У киберстрима есть «инициатор» (частное лицо или профессиональная организация), «форма выражения» (прямая трансляций или запись), «субъекты» и «творческий элемент».

Список литературы

1. Васильев И. А. Принцип соразмерности и строгая ответственность футбольных клубов за поведение болельщиков в соревнованиях УЕФА // Правоприменение. 2021. Т. 5, № 3. С. 232–248. DOI: 10.52468/2542–1514.2021.5(3).232–248

2. О физической культуре и спорте в Российской Федерации: Федер. закон от 4 дек. 2007 г. № 329-ФЗ // СПС КонсультантПлюс.

3. Гейминг и киберспорт предложили законодательно урегулировать (электронный ресурс). URL: https://pravo.ru/news/232165

4. Краснова К. А. Киберспорт и преступность // Научный портал МВД России. 2021. № 4 (56). С. 30–33.

5. Краснова К. А., Рахманова Е. Н. Преступность в сфере киберспорта: уголовно-правовой аспект // Рос. правосудие. 2021. № 10. С. 90–97.

6. Опыт отдельных зарубежных стран в борьбе с манипулированием результатами: Международная конвенция о борьбе с допингом в спорте. URL: https://www.un.org/ru/documents/decl_conv/conventions/doping_in_sport.shtml

7. Правила вида спорта «компьютерный спорт»: утв. приказом Минспорта России от 22 янв. 2020 г. № 22: // СПС КонсультантПлюс.

8. Правила вида спорта «спортивное ориентирование»: утв. приказом Минспорта России от 3 мая 2017 г. № 403 // СПС КонсультантПлюс.

9. Правила вида спорта «спортивное ориентирование»: утв. приказом Минспорта России от 3 мая 2017 г. № 403 // СПС КонсультантПлюс.

10. ТАСС: Есть ли допинг в киберспорте? Главная проблема традиционного спорта в новой индустрии. URL: https://tass.ru/sport/12921737

11. The Guardian: Godfrey Ch. ‘It’s incredibly widespread’: why eSports has a match-fixing problem. URL: https://www.theguardian.com/games/2018/jul/31/its-incredibly-widespreadwhy-esports-has-a-match-fixing-problem

12. Chanda S., Singh T., Star Sh. Contouring E-Doping: A Menace to Sportsmanship in Esports // Turkish Online Journal of Qualitative Inquiry. 2021. 12. Pp. 966–981.

13. Geldibaev M. K., Dikaev S. U., Krasnova K. A., Tsvetkov P. V., Filatova N. Y. Defining corruption and fraud in professional sport, SHS Web Conf., 108, 02008. 2021. URL: https://doi. org/10.1051/shsconf/202110802008

М. А. Ефремова,
доктор юридических наук, доцент,
Казанский филиал
Российского государственного университета правосудия

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Аннотация. Целью исследования является выявление роли информационно-телекоммуникационных сетей в механизме совершения преступления. Уточняется, что понятие преступлений, совершаемых с использованием информационно-телекоммуникационных сетей в настоящее время отсутствует. Делается вывод о том, что информационно-телекоммуникационные сети являются средством совершения преступлений и по этому признаку предлагается систематизировать анализируемую группу преступлений. Обосновывается, что использование информационно-телекоммуникационных сетей в процессе совершения преступления не всегда повышает общественную опасность.

Ключевые слова: право, цифровые технологии, информационно-телекоммуникационные сети, сеть Интернет, преступление, общественная опасность, средство совершения преступления.

INFORMATION AND TELECOMMUNICATION NETWORKS AS A MEANS OF COMMITTING CRIMES

Abstract. The purpose of the article is to identify the role of information and telecommunication networks in the mechanism of committing a crime. It is clarified that the concept of crimes committed using information and telecommunication networks is currently absent. It is concluded that information and telecommunication networks are a means of committing crimes and on this basis it is proposed to systematize the analyzed group of crimes. It is proved that the use of information and telecommunication networks in the process of committing a crime does not always increase the public danger.

Keywords: law, digital technologies, information and telecommunication networks, Internet, crime, public danger, means of committing a crime.

Введение. Решение сложной задачи по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей является одной из актуальных проблем современности. Применение информационно-телекоммуникационных сетей при совершении преступлений обусловливает их особенности: динамику форм преступной деятельности, транснациональный характер, сложности обнаружения и, следовательно, высокую латентность.

Осознавая потребность в противодействии этому явлению, государством предпринимаются различные меры. Одной из таких мер является установление уголовно-правового запрета использования информационно-телекоммуникационных сетей для совершения целого ряда противоправных деяний. В тексте статей Особенной части УК РФ первое упоминание информационно-телекоммуникационных

сетей связано с включением в него ст. 185[3] «Манипулирование рынком», в которой речь шла об «электронных, информационно-телекоммуникационных сетях общего пользования (включая сеть «Интернет»)». В последующем законодатель отказался от уточняющего термина «общего пользования» применительно к информационно-телекоммуникационным сетям, а сам признак использования указанных сетей стал появляться и в иных статьях УК РФ.

Основная часть. Закон определяет информационно-телекоммуникационную сеть как технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [1]. Информационно-телекоммуникационная сеть представляет собой «симбиоз двух видов сетей – информационной и телекоммуникационной» [7. С. 20]. Телекоммуникация означает передачу данных на большие расстояния. В свою очередь телекоммуникационная сеть представляет – множество, связанных между собой средств телекоммуникации, которые образуют сеть определенной конфигурации. Компьютерные сети или сети передачи компьютерных данных являются разновидностью телекоммуникационных сетей. Подобные сети также называют цифровыми, а информация в таких сетях передается в виде сообщений, для чего используются различные типы сигналов, в том числе электрические. Информационно-телекоммуникационные сети могут быть глобальными, локальными, корпоративными, региональными, ведомственными и специального назначения. Следовательно, сеть Интернет следует считать одной из разновидностей информационно-телекоммуникационных сетей.

Несмотря на то, что в законодательном обиходе признак использования информационно-телекоммуникационных сетей присутствует довольно давно, в отечественной доктрине отсутствует устоявшееся определение группы преступлений, которые совершаются с помощью указанных технологий. Так, для обозначения исследуемой группы преступлений используются термины «компьютерная преступность» [5. С. 3], «интернет-преступность» [4. С. 2] и др. Однако предпринимая попытки обособить преступления, совершаемые с использованием информационно-телекоммуникационных технологий, в том числе информационно-телекоммуникационных сетей, не учитывается одно важно обстоятельство: указанные технологии могут быть использованы при совершении значительного числа противоправных деяний, а, следуя такой логике, любое преступление, совершенное с помощью информационно-телекоммуникационных сетей, будет относиться к группе исследуемых противоправных деяний. Ввиду изложенного интересны суждения Н. В. Летелкина, по мнению которого, использование информационно-телекоммуникационных сетей в противоправной деятельности образует посягательство на новую группу общественных отношений – «отношения в сфере правомерного использования информационно-телекоммуникационных сетей (включая сеть «Интернет»)», следовательно все подобные посягательства будут являться двухобъектными [7. С. 44]. Несмотря на то, что они имеют различные основные непосредственные объекты, в результате их совершения всегда страдает вышеназванная группа общественных отношений. Под преступлениями, совершаемыми с использованием информационно- телекоммуникационных сетей (включая сеть «Интернет»), Н. В. Летелкин

предлагает понимать «деяния, посягающие на общественные отношения в сфере охраны правомерного пользования сетями телекоммуникации, совершаемые посредством технологических систем, предназначенных для хранения и передачи по линиям связи информации, доступ к которой осуществляется с применением средств вычислительной техники (компьютеров)» [7. С. 49].

Преступления, совершаемые с использованием информационно-телекоммуникационных сетей, представляют собой часть компьютерной преступности, при этом системообразующим критерием, позволяющим их сгруппировать, следует считать способ совершения преступления [8]. Информационно-телекоммуникационные сети, включая сеть Интернет, являются лишь одним из средств распространения и передачи информации, поэтому они соотносятся как часть и целое. В свою очередь, данная группа преступлений не может существовать вне рамок компьютерной преступности ввиду технологических особенностей информационно-телекоммуникационных сетей.

В настоящее время невозможно представить целостную и четкую систему преступлений, совершаемых с использованием информационно-телекоммуникационных сетей. Однако анализ положений Особенной части УК РФ позволяет сделать вывод, что информационно-телекоммуникационные сети, включая сеть Интернет в ряде статей УК РФ включены законодателем в число обязательных признаков основного состава преступления (ч. 3 ст. 137, ст. 159^6, ч. 1 ст. 171^2, ст. 185^3, ч. 1.1 ст. 258^1, ст. 282 УК РФ), в других случаях их использование образует квалифицированный состав «(п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2, ч. 2. ст. 128^1, ч. 3. ст. 133, ч. 2. ст. 205^2, п. «д» ч. 3 ст. 222, п. «в» ч. 5 ст. 222, п. «в» ч. 3 ст. 222^1, п. «в» ч. 4 ст. 222^1, п. «в» ч. 3 ст. 222^2, п. «в» ч. 5 ст. 222^2, п. «б» ч. 2 ст. 228^1, п. «д» ч. 3 ст. 230, ч. 1.1 ст. 238^1, п. б. ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2, п. «г» ч. 2 ст. 245, п. «б» ч. 2. ст. 258^1, ч. 2. ст. 280, ч. 2. ст. 280^1, п. «в» ч. 2. ст. 280^4, п. «в» ч. 2 ст. 354^1, ч. 4. ст. 354^1 УК РФ)». Однако при конструировании соответствующего признака законодатель допустил расхождение терминологии, указав в ст. 185^3, ч. 2. ст. 205^2, п. «б» ч. 2 ст. 228^1, «б» ч. 2. ст. 258^1, ч. 2. ст. 280^1 УК РФ еще и на «электронные сети». В Постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [2] разъясняется, что «для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются» [2]. В свою очередь, информационно-телекоммуникационными сетями могут быть сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо передачу информации между компьютерными устройствами [2]. Квалифицирующие признаки отдельных составов, помимо «использования информационно-телекоммуникационных сетей, включая сеть Интернет», содержат указание и на «использование средств массовой

информации» [2]. По мнению А. И. Антипова, информационно-телекоммуникационные сети и средства массовой информации имеют сходства: при помощи информационно-телекоммуникационных сетей можно получать доступ к материалам СМИ, кроме того, их использование позволяет массово и в короткий срок распространять информацию неограниченному кругу лиц, что зачастую превосходит возможности традиционных СМИ [3. С. 64]. В целях унификации законодательной терминологии он предлагает использовать формулировку «совершение деяния с использованием средств массовой передачи информации» [3. С. 194]. Л. В. Иногамова-Хегай полагает, что целях обеспечения системности уголовного закона и единства законодательного языка «предпочтительнее везде или указывать, или не указывать средства массовой информации и электронные сети» [6. С. 53–58]. Использование СМИ при совершении преступлений предполагает публичность и массовость, использование же информационно-телекоммуникационных сетей, позволяет помимо, этого действовать дистанционно, оставаться при этом анонимным. Не все те деяния, где в качестве квалифицирующего признака предусмотрено использование информационно-телекоммуникационных сетей, могут быть совершены с использованием СМИ чисто технически. Поэтому излишним является лишь упоминание «электронных сетей», в остальном же, на наш взгляд, данные признаки в какой-либо корректировке не нуждаются.

Заключение. Большинство ученых, исследовавших проблему влияния использования информационно-телекоммуникационных сетей на общественную опасность приходят к выводу о том, что использование информационно-телекоммуникационных сетей повышает общественную опасность деяния [4. С. 73; 7. С. 31]. Однако с таким суждением трудно согласиться. Повышенная общественная опасность деяния, совершенного с использованием информационно-телекоммуникационных сетей, будет иметь место в тех случаях, когда такое деяние причиняет или создает угрозу причинения вреда большего, чем если бы деяние совершалось без их использования. Полагаем, что именно поэтому законодатель весьма осторожно подошел к вопросу включения соответствующего квалифицирующего признака в действующее уголовное законодательство. В то же время использование информационно-телекоммуникационных сетей существенно упрощает процесс выполнения объективной стороны преступления. Дистанционный характер совершения преступлений позволяет сохранить анонимность, причинить вред не одному, а сразу нескольким потерпевшим, в том числе и несовершеннолетним. Указанные обстоятельства существенно повышают опасность причинения большего вреда. Вышеизложенное позволяет сделать вывод о том, что в одних случаях использование информационно-телекоммуникационных сетей не влияет на общественную опасность деяния, а в других – существенно ее повышает.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3448.

2. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». URL: https://www.vsrf.ru/documents/own/31913

3. Антипов А. И. Уголовно-правовое значение использования средств массовой информации и информационно-телекоммуникационных сетей при совершении преступлений с признаками призывов, склонения, незаконного оборота предметов и материалов: дис. … канд. юрид. наук. СПб., 2022. 248 с.

4. Дремлюга Р. Интернет-преступность. Владивосток: Изд-во Дальневосточного университета, 2008. 240 с.

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

6. Иногамова-Хегай Л. В. Современные тенденции криминализации и декриминализации в современном уголовном праве // Уголовное право. 2017. № 4. С. 53–58.

7. Летелкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей: дис… канд. юрид. наук. Нижний Новгород, 2018. 218с.

8. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. URL: https://doi.org/10.21202/jdtl.2023.28

М. Я. Жук,
аспирант,
Казанский (Приволжский) федеральный университет

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ УСТАНОВЛЕНИИ ОСНОВАНИЙ ДЛЯ НАЧАЛА УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ

Аннотация. Наступление XXI в. и вхождение России в часть общемирового информационного пространства ознаменовало доминирующее положение в среде источников информации цифровых носителей данных. С развитием новых технологий методы и формы преступности также меняются и эволюционируют. Количество преступлений, совершенных с использованием цифровых технологий, постоянно растет. В статье исследуется правовая природа цифровых доказательств в уголовном судопроизводстве, а также их значение и процедура фиксации при проведении проверки сообщения о преступлении.

Ключевые слова: право, уголовное преследование, возбуждение уголовного дела, проверка сообщений о преступлении, цифровые доказательства, компьютерная информация, электронная информация

THE USE OF NUMERICAL EVIDENCE IN ESTABLISHING THE GROUNDS FOR STARTING A CRIMINAL PROSECUTION

Abstract. The onset of the 21st century and Russia's entry into a part of the global information space marked the dominance of digital data carriers among information sources. With the development of new technologies, the methods and forms of crime are also changing and evolving. The number of crimes committed using digital technologies is constantly growing. The article examines the legal nature of digital evidence in criminal proceedings, as well as their significance and the procedure for recording when checking a crime report. The concepts of digital information and computer information are correlated, the author's classification of digital evidence is given.

Keywords: law, criminal prosecution, initiation of a criminal case, verification of crime reports, digital evidence, computer information, electronic information

С момента начала формирования понятия «цифровизация» в системе российского права появилась необходимость законодательного закрепления цифровых доказательств в уголовном процессе России. В связи с этим перед правоохранительными органами встал вопрос об использовании цифровых технологий не только для доказывания в уголовном судопроизводстве в целом, но и для установления оснований для возбуждения уголовного дела.

Единственное легальное определение компьютерной информации указано в примечании 1 к ст. 272 УК РФ, где под компьютерной информацией, по мнению законодателя, понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Несмотря на то, что в настоящий момент определение понятия «компьютерная информация» закреплено в примечании к ст. 272 УК РФ, ряд авторов предлагает использовать иную терминологию. Так, ряд авторов считают, что электронным доказательством является любая электронно хранимая информация, которая может быть использована в качестве доказательства [4. С. 253–254].

Некоторые правоведы считают, что цифровая информация, как средство доказывания, не особенно отличается от других видов доказательств. Чаще всего она рассматриваются как эквивалент традиционных доказательств. Высказываются мнения, что отличается лишь способ фиксации доказательств и сам носитель – бумага или электронное устройство.

Вместе с тем существуют особенности, не позволяющие считать цифровые доказательства аналогом обычных [5]. Они отличаются не только формой, но и содержанием. Цифровые доказательства зачастую требуют особой процедуры обработки данных и их получения.

Стоит отметить, что цифровая информация не может быть воспринята органами чувств человека напрямую. Следовательно, идентификация в любом случае может происходить только с помощью специальных устройств – персонального компьютера, мобильного телефона, планшета и т. д. Во всех этих случаях необходимо физическое наличие носителя информации [1. С. 68].

Также для цифровых доказательств обязательное сохранение первоисточника информации не является обязательным элементом, что качественно их отличает от

традиционных видов доказательств. Это происходит ввиду того, что цифровые доказательства могут при копировании менять своего носителя с полным сохранением свойств оригинала, тогда как для вещественного доказательства это невозможно. Вещественное доказательство (в виде какого-то материального объекта – орудия преступления, предмета посягательства и т. п.) уникально и другого такого в природе нет [2. С. 47].

Однако цифровые доказательства являются достаточно уязвимыми. Злоумышленники могут своевременно удалять следы своей активности в сетях. Пост в социальной сети, электронное письмо, сообщения в мессенджерах можно удалить до того, как эти данные попадут в руки следователя. И даже в том случае, если первичная фиксация уже была осуществлена (например, сотрудник правоохранительных органов сделал фототаблицу), преступник может их удалить, и в таком случае возникают проблемы с определением подлинности доказательства. Дополнительным аргументом здесь может служить и тот факт, что цифровые доказательства достаточно просто подделать. Например, изображения или видеозаписи относительно легко могут быть отредактированы. В связи с ограниченными сроками проведения проверки сообщения о преступлении порой бывает затруднительно установить истинность цифрового доказательства в случае его последующей модификации.

Касательно законодательства в настоящее время нет детальной правовой проработки и систематизации цифровых доказательств. При этом не всегда возможно использовать в материалах дела цифровое доказательство как аналог обычного доказательства, как, например, скриншот страницы в Интернете. Некоторая информация как цифровой след, данные с сервера или видеозапись при попытке переноса на бумагу могут потерять свое значение как первичной.

Цифровые доказательства следует подразделить на два вида, в зависимости от процедуры их фиксации.

В качестве первого вида цифровых доказательств могут выступать записи и документы, хранящиеся на электронных носителях информации (компьютере, мобильном телефоне). Их можно объединить в единую группу доказательств, которые можно непосредственно изъять, скопировать на другой носитель или иным образом с ними работать, используя только первичный носитель.

Ко второй группе цифровых доказательств следует отнести те, что хранятся только в Интернете, и доступ к ним можно получить через сервер интернет-ресурса или провайдера. Сюда следует включить записи в социальных сетях, сообщения на форумах, онлайн-переписку.

Существенным отличием второй группы доказательств от первой автор считает то, что доказательства из второй группы можно обнаружить и использовать не имея доступа к первичному носителю информации ввиду того, что она является общедоступной – фиксацию можно осуществить с любого другого устройства, и для этого понадобится только доступ к информационно-телекоммуникационной сети «Интернет».

Собирание совокупности цифровых доказательств в соответствии с нормами ч. 1 ст. 86 УПК РФ по преступлениям, совершенным в сети Интернет, происходит

двумя основными способами, исходя из классификации цифровых доказательств. К первому способу относится изъятие цифровой информации непосредственно с физического носителя данных. В данном случае это возможно как с согласия собственника носителя, так и без его согласия с привлечением специалиста для изъятия информации.

Второй способ заключается непосредственно в исследовании и фиксации общедоступной противоправной информации во время проведения проверки сообщения о преступлении. Сотрудники правоохранительных органов в случае обнаружения незаконной информации осуществляют ее фиксацию путем скриншота страницы и составления протокола осмотра интернет-ресурса с соответствующим приложением.

Отдельно следует отметить возможность восстановления цифровых доказательств в случае их повреждения заинтересованными лицами. При наличии специального оборудования удаленную информацию можно все еще изъять и прикрепить к материалам, однако для этого требуются специальные знания и оборудование. Например, удаленные данные с жесткого диска компьютера можно получить, однако расшифровка удаленных данных невозможна без привлечения специалиста, что значительно усложняет работу и может повлечь за собой увеличение сроков проверки сообщения о преступлении. В случае же когда информация содержалась в сети Интернет, правоохранительные органы могут направить запрос администраторам ресурса, которые предоставят данные из электронного архива. Эта особенность качественно отличает цифровые доказательства от вещественных ввиду того, что последние в случае уничтожения теряются окончательно.

По состоянию на сегодняшний день, одним из проблемных вопросов использования цифровых доказательств в процессе установления оснований для начала уголовного преследования остается затруднительность производства такого процессуального действия, как осмотр по преступлениям, совершаемым с использованием сети Интернет. В отличие от «традиционных» преступлений, где осмотр предмета возможно совершить визуально, осмотр предметов по преступлениям, совершенным в сети Интернет, подразумевает необходимость обладания уполномоченного лица специальными познаниями в сфере цифровых технологий, а также в ряде случаев использование технических средств с доступом в сеть Интернет.

Здесь же стоит затронуть проблему получения доступа к носителю цифровой информации при проведении проверки сообщения о преступлении. Ввиду того, что до принятия процессуального решения о возбуждении уголовного дела, свобода процессуальных действий следователя ограничена частью следственных и иных процессуальных действий, на практике бывает затруднительно использовать цифровые доказательства для установления оснований для возбуждения уголовного дела. Если цифровое устройство находится при лице, то законодатель допускает его изъятие и осмотр в качестве предмета. Однако если цифровой носитель информации находится в жилом помещении лица, то для изъятия данной информации и фиксации цифровых доказательств зачастую необходимо произвести обыск или выемку, однако действующий УПК не предусматривает такой возможности при проведении проверки сообщения о преступлении. Решить данную проблему можно только

разрешив производство обыска и выемки до принятия процессуального решения о начале уголовного преследования, аналогично тому, как УПК разрешает изъятие предметов во время проведения личного досмотра.

Подводя итог, следует отметить, что в настоящее время нормативное регулирование и научная проработка использования цифровых доказательств находятся на стадии развития, и не в полной мере отражают реальную объективную действительность. Вместе с тем число составов преступлений, совершаемых с помощью электронных устройств, постоянно расширяется. Установление оснований для возбуждения уголовного дела по таким составам преступлений не представляется возможным без фиксации цифровых доказательств. В связи с этим правоохранительные органы все активнее используют цифровые доказательства в ходе установления оснований для возбуждения уголовного дела.

Значительным правовым пробелом остается невозможность для правоохранительных органов в стадии возбуждения уголовного дела использовать все возможные способы фиксации цифровых доказательств. В ряде случаев законодательно ограничена возможность получения доступа к носителю информации. Если преступление было совершено с помощью электронного устройства, например, персонального компьютера, то для получения доступа к нему необходимо провести выемку предмета из жилого помещения или обыск в помещении, где этот компьютер находится. А данные следственные действия по текущему законодательству не могут проводиться до возбуждения уголовного дела.

Список литературы

1. Развитие информационных технологий в уголовном судопроизводстве: монография / С. В. Зуев, В. С. Балакшин, В. Б. Вехов, В. Н. Григорьев, А. И. Зазулин, О. А. Зайцев, М. О. Медведева, Е. В. Никитин, О. В. Овчинникова, П. С.,Пастухов В. А. Родицилина, И. В. Смолькова, В. Ю. Стельмах, А. А. Шаевич. М.: Юрлитинформ, 2018.

2. Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3(26).

3. Медведева М. О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: автореф. дис. … канд. юрид. наук. М., 2018.

4. Основы теории электронных доказательств: монография / под ред. д-ра юрид. наук С. В. Зуева. М.: Юрлитинформ, 2019.

5. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295. EDN SGAOKS.

Н. А. Жукова,
кандидат юридических наук, доцент,
Белгородский государственный национальный
исследовательский университет

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. Анализ трансформации уголовно-процессуального законодательства и правоприменительной практики приводит автора к выводу о неизбежности цифровизации уголовного судопроизводства в России. Цифровой формат уголовного судопроизводства должен способствовать непрерывности процесса производства по уголовному делу (при пандемии, карантинных мероприятиях, чрезвычайных ситуациях), сокращению сроков производства по уголовным делам за счет ускорения получения сведений, могущих иметь доказательственное значение, объективизации процесса и, как следствие, повышению доверия общества к органам уголовного преследования и правосудия. Цифровые технологии в уголовном судопроизводстве не должны подменять следователя, оперативного сотрудника, эксперта, но должны сокращать дистанцию между ними и другими участниками судопроизводства.

Ключевые слова: уголовное судопроизводство, цифровые технологии, доказательства, следственные действия, цифровые следы, предварительное расследование

DIGITAL TECHNOLOGIES IN CRIMINAL PROCEEDINGS

Abstract. The analysis of the transformation of criminal procedure legislation and law enforcement practice leads the author to the conclusion that the digitalization of criminal proceedings in Russia is inevitable. The digital format of criminal proceedings should contribute to the continuity of the process of criminal proceedings (in case of a pandemic, quarantine measures, emergency situations), reduce the time of criminal proceedings by speeding up the receipt of information that may have evidentiary value, objectification of the process and, as a result, increase public confidence in criminal prosecution and justice. Digital technologies in criminal proceedings should not replace an investigator, an operative, an expert, but should reduce the distance between them and other participants in the proceedings.

Keywords: criminal proceedings, digital technologies, evidence, investigative actions, digital traces, preliminary investigation

Цифровизация как приоритетное направление развития нашего государства не могла не затронуть сферу уголовного судопроизводства. Предпосылкой внедрения цифровых технологий в уголовное судопроизводство стал дистанционный формат работы, введенный в связи с пандемией COVID-19 и продолжающий применяться на отдельных территориях Российской Федерации в чрезвычайных ситуациях.

В научном мире разгорелась дискуссия о целесообразности внедрения цифровых технологий в уголовное судопроизводство и о создании цифрового уголовного процесса. Высказывались мнения о недопустимости трансформации классического уголовного процесса в цифровой формат в связи с особым видом этой государствен-

ной деятельности по осуществлению уголовного преследования и привлечению к уголовной ответственности, как наиболее существенно затрагивающего конституционные права и свободы граждан [1–5, 7–14, 16–18, 21–22].

Однако, по нашему мнению, этот процесс неизбежен. С 2010 г. в России цифровые технологии стали применяться судами и учреждениями службы исполнения наказаний. В начале это были технологии видеоконференцсвязи, в дальнейшем – смс-повестки, электронные порталы с возможностью размещения судебных решений и подачей исков и жалоб. В досудебном уголовном процессе цифровые технологии появились в этот же период, сначала в рамках экспертной деятельности, когда стали применяться программные комплексы (включающие в себя не только программное обеспечение, но и цифровое оборудование), позволяющие обходиться без понятых, проводить исследования и экспертизы, привлекать специалиста-криминалиста для оказания помощи при проведении следственных действий (например, при проведении видеозаписи), появились мобильные экспертные лаборатории, автоматизированные учеты, электронные базы данных.

«Развитие цифровых средств связи позволило в 2013–2015 гг. ввести в уголовное судопроизводство такой способ коммуникации, как отправление участникам судопроизводства СМС-сообщений о необходимости явки в органы расследования или в суд; была установлена обязанность потерпевшего сообщать адрес электронной почты для обеспечения более эффективной связи с ним (ч. 5.1 ст. 42 УПК РФ). С 2013 г. Правительством РФ определен перечень технических средств, которые могли бы применяться в уголовном судопроизводстве для контроля за поведением подозреваемого, обвиняемого, к которым применена мера пресечения в виде домашнего ареста» [1. С. 93].

В последние годы в досудебном уголовном процессе появилась необходимость изъятия цифровых следов, а с 2018 г. – и возможность получения цифровых доказательств [3]. Именно тогда в УПК РФ были внесены изменения, касающиеся порядка изъятия цифровых следов, а также производства отдельных следственных действий с применением цифровых технологий.

Все это лишь начало цифровой трансформации уголовного судопроизводства. По мере внедрения в уголовное судопроизводство цифровых технологий возникают вопросы законодательной регламентации нового понятийного аппарата и процедурных особенностей. Рассмотрим некоторые из них.

Глава 56 УПК РФ содержит положения об электронном документообороте. Однако понятия «электронный документ» и «усиленная квалифицированная электронная подпись» в УПК РФ отсутствуют как в самой статье 474.1, так и в статье 5.

Под электронным документом в соответствии с Законом «Об информации, информационных технологиях и о защите информации» [6, ст. 2 п. 11.1] понимается документ, выполненный с помощью электронной техники (компьютера, ноутбука, планшета, смартфона с использованием соответствующего программного обеспечения) для передачи по информационно-телекоммуникационным сетям или для обработки в информационных системах. Пленум Верховного Суда РФ внес в это определение небольшое уточнение: «Электронный документ – документ, созданный в электронной форме без предварительного документирования на бумажном

носителе, подписанный электронной подписью» [16]. В статье 474.1 УПК РФ наряду с электронным документом упоминается и электронный образ документа, под которым понимается электронная копия документа, изготовленного на бумажном носителе, заверенная электронной подписью.

Закон «Об электронной подписи» дает такое ее определение: «Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию». В постановлении Пленума Верхового Суда РФ сформулировано более понятное определение электронной подписи как информации в электронной форме, присоединенной к подписываемому электронному документу или иным образом связанной с ним и позволяющей идентифицировать лицо, подписавшее электронный документ [16]. «Проще говоря, электронная подпись подразумевает уникальную последовательность символов (персональный цифровой код), позволяющих установить лицо, подписавшее электронный документ. Электронная подпись может быть: простой, усиленной неквалифицированной и усиленной квалифицированной» [23].

Простая электронная подпись – это электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Усиленная неквалифицированная электронная подпись – это электронная подпись, позволяющая увидеть вносимые в электронный документ изменения после его подписания.

Усиленная квалифицированная электронная подпись – это электронная подпись, позволяющая увидеть вносимые в электронный документ изменения после его подписания и созданная с использованием сертифицированного ключа проверки электронной подписи, выданного удостоверяющим центром.

В уголовном судопроизводстве допустима только усиленная квалифицированная электронная подпись, что предполагает совершение участниками уголовного судопроизводства дополнительных действий по ее получению. Пока граждане нашей страны, не занимающиеся предпринимательством и не занимающие руководящую должность, предполагающую иметь усиленную квалифицированную подпись, такую подпись оформляют редко. А это значит, что подача электронных документов (заявлений, жалоб и ходатайств) для физических лиц – участников уголовного судопроизводства связана с определенной временной задержкой (для уголовного судопроизводства с ограниченными сроками это серьезная проблема) либо не возможна (отсутствие компьютерной техники и доступа в Интернет пока еще являются для отдельных территорий и людей проблемой). Следовательно, реализация ст. 474.1 УПК РФ имеет ограничения, пока уровень цифровой грамотности не охватит всю страну и получение усиленной квалифицированной подписи не станет обыденным явлением.

Следующим аспектом, на котором хотелось бы остановиться при рассмотрении вопроса о цифровых технологиях в уголовном судопроизводстве, является обнаружение, фиксация и изъятие цифровых следов. Под цифровыми следами

понимается криминалистически значимая компьютерная информация о событиях или действиях, отраженная в материальной среде в процессе ее возникновения, обработки, хранения и передачи [18. С. 179]. Цифровые следы возникают при совершении многих преступлений, сопряженных не только с неправомерным доступом к компьютерной информации, разработкой и использованием вредоносных программ, но и с совершением терактов, убийств, вымогательства, мошенничества, незаконной организацией торговли, азартных игр и оборотом наркотиков, клеветой, оскорблениями и др. В 2018 г. УПК РФ воспринял необходимость обнаружения, фиксации и изъятия цифровых следов путем введения статьи 164.1, устанавливающей возможность изъятия электронных носителей информации либо ее копирования на другие электронные носители в ходе проведения следственных действий с участием специалиста. Согласимся с законодателем, так как изъятие электронных носителей информации или копирование содержащейся на них информации возможно только с помощью специалиста, так как только он может грамотно описать изымаемый электронный носитель для протокола следственного действия либо выбрать безопасный для копирования способ, чтобы информация не была уничтожена или изменена.

Вопросом для правоприменителей остается специализация и квалификация специалиста, приглашаемого для изъятия электронного носителя информации или ее копирования. В одном случае нужно пригласить программиста, в другом IT-специалиста, в третьем инженера-электронщика, но как следователю, не обладающему специальными знаниями выбрать? Да и подобных специалистов в экспертно-криминалистических подразделениях не всегда удается найти, а гражданские специалисты не горят желанием помочь правоохранителям. Полагаем, что данную проблему можно решить организационно, путем введения соответствующих должностей в экспертно-криминалистические подразделения с учетом возрастающей потребности, оснащения лабораторий необходимым современным компьютерным оборудованием и программным обеспечением, а также подготовки (или найма) таких специалистов в кратчайшие сроки.

С 2012 г. в судопроизводстве уже используется возможность вызова участников процесса путем направления СМС-сообщений при условии получения письменного согласия на такой способ уведомления. В связи с расширением возможностей электронной почты арбитражные суды по аналогии стали применять и такой способ рассылки уведомлений. Однако в уголовном судопроизводстве (особенно на досудебных стадиях) эта альтернатива повестке не рассматривается ни законодателем, ни должностными лицами, ведущими производство по уголовным делам.

Возможность производства следственных действий с использованием видеоконференцсвязи позволила решить ряд проблем, связанных с удаленностью от места проведения расследования участников уголовного судопроизводства, с сокращением сроков расследования и минимизацией затрат на его производство. И здесь важно сохранить гарантии обеспечения прав участников таких следственных действий. Отметим, что возможность выбора способа производства допроса и очной ставки лично или с использованием видеоконференцсвязи является пра-

вом потерпевшего, свидетеля, гражданского истца, гражданского ответчика и их представителей, так как возможность выбора способа защиты своих прав и свобод закреплена в части 2 статьи 45 Конституции РФ. Следователь обязан разъяснить это право и обеспечить его реализацию. Что касается выбора способа допроса и очной ставки с участием подозреваемого, то в этом случае это право следователя, основанное на целесообразности выбора способа, экономии ресурсов и времени судопроизводства. Кроме того, дистанционный способ допроса не лишает подозреваемого, обвиняемого, подсудимого и защитника донести свою позицию по поводу расследуемого события, предъявленного обвинения и другим вопросам.

Опыт проведения следственных действий с применением видеоконференцсвязи необходимо использовать и на стадии возбуждения уголовного дела при проведении проверочных действий путем опроса.

Также полагаем целесообразным изучить пример некоторых стран ближнего зарубежья по введению электронной формы уголовного дела. Такая форма не только даст возможность экономии на бумаге и печати документов, но и решит проблему восстановления утраченных уголовных дел. Это, в свою очередь, позволит не прибегать к применению ч. 4 ст. 158.1 УПК РФ, а именно не освобождать обвиняемого в случае, если по утраченному уголовному делу истек предельный срок содержания под стражей.

Подводя итог, можно с уверенностью сказать, что цифровизация уголовного судопроизводства неизбежна, как неизбежно развитие цифровых технологий [23]. Не стоит отказываться от достижений научно-технического прогресса в уголовном процессе, тем более что преступный мир активно ими пользуется. Цифровой уголовный процесс должен способствовать повышению эффективности уголовного судопроизводства в установлении объективной истины, восстановлении нарушенных прав и привлечении виновных к ответственности. Переход к цифровому уголовному судопроизводству необходимо продолжить, создавая свои цифровые технологии, расширяя компетенции судей, следователей, дознавателей, оперативных сотрудников в IT-сфере и привлекая на работу в экспертно-криминалистические подразделения IT-специалистов, программистов и других специалистов по цифровым технологиям.

Список литературы

1. Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5 (150). С. 91–104.

2. Гаврилин Ю. В., Победкин А. В. Модернизация уголовно-процессуальной формы в условиях информационного общества // Труды Академии управления МВД России. 2019. № 3(51). С. 27–38.

3. Григорьев В. Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство // Академическая мысль. 2019. № 3(8). С. 57–61.

4. Григорьев В. Н., Максимов О. А. Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. 2018. № 1. С. 1–8.

5. Забавина А. Ю., Киселев Е. А. Проблемы законодательной регламентации использования данных спутниковых навигационных систем в раскрытии и расследовании преступлений // Российский следователь. 2015. № 4. С. 7–11.

6. Закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I). Ст. 3448.

7. Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118–123.

8. Зуев С. В., Титова А. С. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства // Правопорядок: история, теория, практика. 2019. № 1(20). С. 49–54.

9. Спиридонов, М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. EDN ACSQXH.

10. Ищенко, П. П. О путях реформирования и цифровизации начального этапа предварительного расследования // Вестник Университета имени О. Е. Кутафина. 2019. № 8(60). С. 89–99.

11. Овчинникова, О. В. Дистанционные следственные действия: современное состояние и перспективы // Юридическая наука и правоохранительная практика. 2019. № 1(47). С. 108–116.

12. Основы теории электронных доказательств / под ред. С. В. Зуева. М.: Юрлитинформ, 2019. 400 с.

13. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295. EDN SGAOKS.

14. Першин, А. Н. Электронный носитель информации как новый источник доказательств по уголовным делам // Уголовный процесс. 2015. № 5. С. 48–54.

15. Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // КонсультантПлюс, 1992–2023.

16. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. № 5(57). С. 31–44.

17. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности [Текст] / Е. Р. Россинская // Вестник Восточно-Сибирского института МВД России. 2019. № 2(89). С. 193–202.

18. Семикаленова, А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики [Текст] / А. И. Семикаленова, И. А. Рядовский // Актуальные проблемы российского права. 2019. № 6(103). С. 178–185.

19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

20. Федеральный закон от 27.12.2018 № 533-ФЭ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // СЗ РФ. 2018. № 53 (ч. I). Ст. 8459.

21. Шереметьев, И. И. Использование цифровых технологий при рассмотрении уголовных дел в суде: реальность и перспективы // Lex Russica. 2019. № 5(150). С. 117–131.

22. Борсук Н. А., Федорова В. А., Минина А. Д. Исследование вопроса внедрения электронной подписи на предприятии // Вопросы радиоэлектроники. 2019. № 3. С. 60–66.

23. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

Г. И. Загорский,
доктор юридических наук, профессор,
Российский государственный университет правосудия
Е. А. Костенюк,
помощник судьи Оренбургского районного суда Оренбургской области,
аспирант,
Российский государственный университет правосудия

ГЛАСНОСТЬ В АСПЕКТЕ УСОВЕРШЕНСТВОВАНИЯ ПРОЦЕДУРЫ ПРОВОЗГЛАШЕНИЯ ПРИГОВОРА В СЛОЖНЫХ ЧРЕЗВЫЧАЙНЫХ УСЛОВИЯХ

Аннотация. В статье рассматриваются нормы процессуального права, характеризующие такой особый сегмент отношений в рамках уголовного судопроизводства РФ, как провозглашение приговора в рамках сложившихся сложных чрезвычайных условий в контексте реализации гласных основ таковой процедуры. Проводится анализ действующей законотворческой практики, регулирующей порядок и правила провозглашения приговора с учетом сложившейся чрезвычайной ситуации и последних законодательных новелл. Подчеркивается важность отдельных концептуальных нормативно-правовых документов регулятивных отраслей права, таких как конституционное, информационное, уголовное, общественная безопасность и др. Обозначаются законодательные «огрехи», требующие дополнительного уточнения и обновления. Итогом проделанной работы стали предложения и рекомендации действующих «национальных нормативов», образовывающие новизну научных изысканий с учетом правовой специфики рассмотрения уголовного дела судом первой инстанции в условиях чрезвычайной ситуации в целом и военного положения, в частности, посредством использования инновационных систем видеоконференцсвязи.

Ключевые слова: чрезвычайная ситуация, приговор, уголовное судопроизводство, трансформация, гласность

GLASNOST IN IMPROVING THE PROCEDURE FOR THE PRONOUNCEMENT OF A SENTENCE IN COMPLEX EMERGENCY SITUATIONS

Abstract. The subject of research in this article is a set of norms of procedural law, characterizing such a special segment of relations in the framework of criminal proceedings of the Russian Federation as the proclamation of a verdict in the framework of the existing complex emergency conditions – emergency situation – in the context of the implementation of the transparent basis of such a procedure. The author analyzes the current lawmaking practice regulating the procedure and rules of proclamation of the verdict taking into account the existing emergency situation and the latest legislative novelties; opinions of famous proceduralists engaged in the study of the problem. The importance of certain conceptual normative-legal documents of regulatory branches of law, such as: constitutional, information, criminal, public security, etc. is emphasized. Legislative «faults» that require additional clarification and updating are outlined. The result of the work done became original author's proposals and recommendations of the current «national regulations», forming the novelty of scientific research, taking into account the legal specificity of consideration of a criminal case by the court of first instance in conditions of emergency in general, and martial law, in particular through the use of innovative videoconferencing systems.

Keywords: emergency situation, sentence, criminal proceedings, transformation, publicity,

Итоговым процессуальным актом, выносимым в суде первой инстанции по каждому из рассматриваемых уголовных дел, считается интегральное решение – приговор, постановленный на основании базисных конституционно-правовых и процессуальных норм, предусмотренных ст. ст. 50,123 Конституции РФ и главой 39 УПК РФ.

Обратившись к законодательным основам – п. 28. ст. 5 УПК РФ, а также аккумулировав точки зрения ученых разных лет на проблему понятийной нагрузки (К. А. Болденко [2. С. 88–91], А. А. Федуловой [9. С. 23–26]) – приговора, автор предлагает определить как «вынесенное именем РФ решение о признании подсудимого лица виновным либо невиновным, о назначении наказания, либо освобождении от него, постановленное судом первой или апелляционной инстанции».

Актуальность изысканий опосредована тем, что особенности самой процедуры постановления и провозглашения уголовного приговора в условиях образовавшейся чрезвычайной ситуации любого ее вида – техногенного, природного, военного и биолого-социального – характеризуется значительным своеобразием, предполагающем трансформацию традиционных в своем понимании институтов уголовного, и уголовно-процессуального закона с непосредственно неизменным базисом – нормативных установлений Конституции РФ, предполагающих гласное рассмотрение и разрешение дела, в том числе и постановление приговора правосудного на всех территориальных единицах РФ.

Прежде всего, обратим внимание на обновленно-общую процедуру провозглашения постановленного судом первой инстанции приговора, в части его вводной и резолютивной ст. 310 УПК РФ, что было прямо отражено в Федеральном законе от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» (http://sudact.ru/regular/court/0g4e8uis5qZ).

Данная новелла интересна по сей день. Отмена оглашения описательно-мотивировочной части уголовного приговора по убеждению таких авторов, как Д. В. Тихонов [7. С. 217–220], С. С. Арсентьева, А. Н. Савченко [1. С. 16–20] признается прогрессивно-современным явлением, сокращающим судебную нагрузку в части оглашения достаточно объемных описательно-мотивировочных его частей, называя их рудиментом уголовно-процессуального права.

Вместе с тем имеет место быть и позиция радикально противоположная. Так, Н. В. Ткачева [8. С. 208–220], С. А. Ворожцов [3. С. 22–25] относятся к ней – новелле – крайне негативно, считая, что оглашение приговора лишь в его части вводной и резолютивной влечет за собой нарушение конституционного права подсудимого на защиту (статьи 46 Конституции РФ) в части своевременного и эффективного его обжалования, поскольку сторона защиты минимум пять суток осведомлена не будет о самом содержании описательно-мотивировочной части провозглашенного приговора, мотивов отклонения либо опровержения тех либо иных доказательств, высказанной позиции защиты и т. д., что представляет собой с точки зрения процессуально-правовой нарушения норм уголовно-процессуального закона, являясь абсолютно не допустимым явлением в рамках действующего правового поля РФ.

Кроме того, вполне оправданной является и предложенная законодательной практикой инициатива о немедленном вручении приговора, после оглашения его как вводной, так и резолютивной частей, которыетак и не нашли своего отражения в УПК РФ (ст. 312).

Не вдаваясь в глубокую полемику по данному вопросу, поскольку предмет нашего исследования несколько иной – провозглашение приговора в рамках сложившихся сложных чрезвычайных условий (ЧС) – в контексте реализации гласных основ таковой процедуры, считаем, оба вышеизложенных суждения имеют право на свое существование в рамках современной уголовно-правовой доктрины, имея в своей основе вполне допустимые суждения.

Соблюдение комплекса правил провозглашения приговора в условиях чрезвычайной ситуации с учетом явления гласности, имеющей в своем сущностном содержании конституционно-правовой аспект, осложнено следующими обстоятельствами объективной реальности:

– во-первых, отсутствием правового регулирования названных юридических особенностей,

– и, во-вторых, тем, что понимание правовой специфики рассмотрения уголовного дела судом в условиях чрезвычайной ситуации связано с самой сущностью (правовой природой) гласности, одним из проявлений которой выступает именно право публичного оглашения приговора (от имени Российской Федерации), что не

представляется достижимым в отдельных практических случаях данной ситуации [6. С. 153–155].

Представляется, что с учетом проблем, возникающих во время образования чрезвычайной ситуации каждого из ее видов, в особенности, положения военного, опосредованного присутствием различного рода угроз, состояния защищенности жизненно важных интересов личности, общества, и государства, в том числе и непосредственно безопасности участников уголовного судопроизводства при рассмотрении уголовных дел, включая безопасность суда, – провозглашение приговора суда целесообразно осуществлять в режиме видеоконференцсвязи в согласованное (посредством уведомления) время, путем использования соответствующих информационных технологий цифрового общества и дигитального компонента.

На наш взгляд, использование при провозглашении приговора суда в сложных чрезвычайных ситуациях системы видеоконференцсвязи – прогрессивное явление ввиду того, что видеоконференцсвязь представляет собой предусмотренный источниками права процессуальных отраслей российской правовой системы комплекс программных и аппаратных средств, способных передавать актуальные информационные сообщения по гарантированным и безопасным каналам связи между различными субъектами процессуальной деятельности исключительно в рамках реального времени, что выступает в качестве правового гаранта механизма реализации ведущих принципов права, обеспечивающих максимально эффективное применение в судопроизводстве институции электронного правосудия [5. С. 10], не нарушая, при этом, открытости и доступности уголовного судопроизводства, разумно ее сочетая с его тайной.

Гласность в контексте провозглашения приговора суда в условиях чрезвычайной ситуации, целесообразно признать реализованной в законном порядке также в следующих случаях:

1. В связи с размещением провозглашенного в установленном законном порядке приговора суда на соответствующем Интернет-ресурсе (ст. 6 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»).

2. После направления участникам уголовного судопроизводства видеоматериала с провозглашенным в законном порядке приговором суда на соответствующий Интернет-ресурс, допуск к которому осуществляется через определенный юридический инструмент – легализованный именной электронный ключ, подтверждающий личность (ст. 14 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»), врученный в установленном порядке участнику судопроизводства на этапе принятия решения о проведении заседания суда посредством использования системы видеоконференцсвязи (веб-конференции), а при отсутствии такой возможности – Государственной фельдъегерской службой, наделенной таковыми полномочиями (Указ Президента РФ от 7 апреля 2014 г. № 213 «Вопросы Государственной фельдъегерской службы Российской Федерации»).

3. При непосредственным ознакомлении с текстом постановленного и провозглашенного приговора суда в суде как во время продолжения чрезвычайной ситуации, так и позднее.

Изложенная позиция в полной мере коррелирует положениям норм Уголовно-процессуального кодекса РФ, Федерального конституционного закона от 30 января 2002 г. № 1-ФКЗ «О военном положении», Федерального закона от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» и др. Находит поддержку среди таких авторов, как А. М. Галева [4. С. 652–655], Ю. А. Хоренко [11. С. 279–285].

С учетом всего вышеизложенного мы приходим к выводу о том, что перспективными направлениями реформирования уголовно-процессуального законодательства (УПК РФ) обновленного формата гласности в контексте провозглашения правосудного приговора в рамках сложившихся сложных чрезвычайных условий функционирования – ЧС техногенного, природного, военного и биолого-социального характера – следует признать следующие обновления:

– дополнение новой ч. 8 в сформулированной редакции «Приговор суда или иное решение, вынесенное по результатам судебного разбирательства, постановленный в условиях чрезвычайной ситуации, по постановлению суда провозглашается в судебном заседании путем использования систем видеоконференцсвязи» статьи 241 УПК РФ;

– внедрение ст. 310.1 «Провозглашение приговора в условиях чрезвычайной ситуации», представив ее текст в редакции:

«Провозглашение приговора суда в условиях чрезвычайной ситуации по постановлению суда осуществляется в соответствии с ч. 8 ст. 241, 310 настоящего Кодекса с использованием систем видеоконференцсвязи»;

– путем уточнений конкретизировать содержание ст. 312 «Вручение копии приговора», сформулировав в редакции:

«В течение 5 суток со дня провозглашения приговора его копии вручаются осужденному или оправданному, его защитнику и обвинителю. В тот же срок копии приговора могут быть вручены потерпевшему, гражданскому истцу, гражданскому ответчику и их представителям при наличии ходатайства указанных лиц.

При провозглашении приговора в чрезвычайной ситуации вручение приговора признается исполненным в случаях:

1) размещения приговора суда на официальном интернет-сайте суда;

2) после направления участникам уголовного судопроизводства оглашенного в законном порядке приговора суда на соответствующий интернет-ресурс участника уголовного судопроизводства, допуск к которому осуществляется через именной электронный ключ, врученный в установленном порядке участнику судопроизводства, а при отсутствии такой возможности – Государственной фельдъегерской службой, действующей в соответствии с Указом Президента РФ от 7 апреля 2014 г. № 213 «Вопросы Государственной фельдъегерской службы Российской Федерации»;

3) ознакомление с приговором суда в суде, который постановил и провозгласил приговор (во время продолжения и окончания чрезвычайной ситуации)».

Полагаем, что обозначенную позицию целесообразно отразить Верховному Суду РФ в новом Обзоре по отдельным вопросам судебной практики, связанным с уголовным судопроизводством, реализуемом в условиях чрезвычайной ситуации в целом и военного положения в частности.

Список литературы

1. Арсентьева С. С., Савченко А. Н. О приговоре как важнейшем акте правосудия и недопустимости нанесения ущерба его авторитету: анализ примеров судебной практики // Вестник экономической безопасности. 2022. № 4. С. 16–20.

2. Болденко К. А. Приговор как итоговое решение суда: понятие, сущность, виды // Проблемы применения уголовного закона и уголовно-процессуального законодательства в деятельности судов и органов предварительного расследования: сборник научных статей по итогам научно-практической конференции магистрантов. Симферополь, 2023. С. 88–91.

3. Ворожцов С. А. Порядок провозглашения приговора. Несовершенство закона и проблемы правоприменителей // Мировой судья. 2022. № 3. С. 22–25.

4. Галева А. М. Нарушение требования гласности как основание для отмены приговора // Регулирование правоотношений: проблемы теории и практики. Сборник статей XX Международной студенческой научно-практической конференции. Российский государственный университет правосудия. М., 2022. С. 652–655.

5. Миронова Ю. В. Реализация принципов гражданского процессуального права при использовании систем видеоконференц-связи: дис. ... канд. юрид. наук. 12.00.15. Саратов, 2021. С. 239.

6. Перепадя С. М., Кистанова М. А., Остапенко О. И. Поправки в Уголовно-процессуальный кодекс Р. оптимизация процедуры или повышение уровня правосудия и защиты прав граждан? // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник научных статей по материалам V Национальной заочной научно-практической конференции.Ставрополь, 2023. С. 153–155.

7. Тихонов Д. В. О некоторых вопросах провозглашения итогового и промежуточных решений в уголовном судопроизводстве // Правосудие на современном этапе. Новые вызовы времени: сборник материалов национальной научно-практической конференции. Чита, 2022. С. 217–220.

8. Ткачева Н. В. Условия производства в суде первой инстанции при рассмотрении и разрешении уголовных дел в общем порядке // Труды Института государства и права Российской академии наук. 2023. Т. 18, № 3. С. 208–222.

9. Федулова А. А. Приговор, его понятие и сущность как акта правосудия // Актуальные исследования. 2022. № 34 (113). С. 23–26.

10. ФПА выступила против законопроекта о сокращенном оглашении приговора. URL: https://pravo.ru/news/244018/ http://sudact.ru/regular/court/0g4e8uis5qZ

11. Хоренко Ю. А. Общие условия судебного разбирательства // Основные подходы к управлению знаниями в науке и образовании. Сборник научных трудов. Казань, 2023. С. 279–285.

Т. Г. Каракулов,
председатель суда,
Чаинский районный суд Томской области
А. Т. Вельтмандер,
кандидат юридических наук, судья,
Томский областной суд

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СФЕРЕ

Аннотация. В статье проводится комплексный анализ проблем, связанных с отдельными аспектами реализации политических мер уголовно-правового характера, направленных на борьбу с преступлениями, совершенными в информационно-коммуникационной сфере, способ совершения которых связан с использованием цифровых технологий, или предметом которых выступают электронные денежные средства и криптовалюта. В результате предлагается классификация данных преступлений на основе системного правового закрепления уголовно-правовых норм; определяются некоторые социально-криминологические основания и особенности криминализации соответствующих деяний и их пенализации.

Ключевые слова: уголовная политика, преступление, общественная опасность, криминализация, наказание, пенализация, цифровые технологии

ON SOME AREAS OF CRIMINAL LAW POLICY IN THE INFORMATION AND COMMUNICATION SPHERE

Abstract. A comprehensive analysis of the problems associated with certain aspects of the implementation of political measures of a criminal nature aimed at combating crimes committed in the information and communication sphere, for example, the method of commission of which is associated with the use of digital technologies, or the subject of which are electronic money and cryptocurrency. As a result of the study of scientific ideas, normative provisions of the criminal law, judicial practice: the classification of these crimes is proposed on the basis of a systematic legal consolidation of criminal law norms; some socio-criminological grounds and features of criminalization of the relevant acts and their penalization are determined.

Keywords: criminal policy, crime, public danger, criminalization, punishment, penalization, digital technologies

Значение информационно-коммуникационных технологий в современном обществе трудно переоценить. Как подобные технологии, так и в принципе наиболее общая категория инноваций определяются чуть ли не единственным фактором возможного развития национальных экономик [15. С. 163]. Право как неизменный элемент общественной жизни не в меньшей степени подвержено влиянию цифровизации и во многом вынуждено следовать за вновь формирующимися или уже сформировавшимися новыми общественными отношениями.

Термин «цифровизация» и его синонимы (цифровая трансформация, виртуализация), первоначально использовавшиеся применительно к экономическим преобразованиям, сегодня, став общеупотребимыми и в науке управления, и уголовном процессе, и при определении направлений развития уголовно-исполнительной системы, уже привычны для ученых-юристов. Цифровизация как сам процесс и результат такого процесса, как правило, указывает на позитивное развитие соответствующих правоотношений, не отстающих от «технологической» повестки дня [6. С. 53–54].

Стремительное развитие общественных отношений, связанное с возникновением новых областей человеческой деятельности и технологическим совершенствованием привычных практик и компетенций, позволяет говорить и об «обратной медали» таких позитивных социальных явлений и процессов. Речь идет о возможности использования указанных достижений в преступных целях, что обусловило введение в уголовный закон самостоятельной главы о преступлениях в сфере компьютерной информации» [4. С. 14] и внесение дополнений в другие статьи Особенной части Уголовного кодекса Российской Федерации, связанные с закреплением соответствующих квалифицирующих признаков составов ряда преступлений.

В указанных примерах отражены результаты криминализации и пенализации – важных форм уголовно-правовой политики в сфере борьбы с такими деяниями, что свидетельствует о трансформации уголовно-правовой политики, которая объективирует направления по применению государством мер уголовной ответственности в целях борьбы с преступными деяниями, совершаемыми в новых формах.

Полагаем наиболее обоснованным понимание криминализации как процесса и результата признания в уголовном законе уголовно наказуемым определенного общественно опасного деяния [11. С. 9–10].

Коль скоро основными для науки уголовного права категориями являются преступление и наказание, то наряду с вопросами о признании деяния общественно-опасным (дейнджеризации) [13. С. 65] и его криминализации (при наличии необходимых и достаточных социально-криминологических оснований), проблемой столь же важной является вопрос о пенализации преступлений, совершаемых с использованием цифровых (информационно-телекоммуникационных) технологий.

Пенализация определяется как деятельность законодателя по установлению (закреплению) в уголовном законе отдельных видов наказаний за предусмотренные им конкретные преступные деяния [3. С. 29; 13. С. 63–64; 14. С. 128].

Общественно опасные деяния, совершаемые с использованием цифровых (информационно-телекоммуникационных) технологий, и их признаки должны быть обстоятельно проанализированы на предмет необходимости и криминализации (установления нового уголовно-правового запрета (запретов) либо содержательного изменения уже существующего (существующих)), и адекватности установленных мер уголовной репрессии за совершение подобных действий (пенализации).

Такой анализ полагаем необходимым проводить на трех уровнях.

На **первом уровне** подобное изучение следовало бы начать с определения и четкого уяснения базовых, концептуальных уголовно-политических идей, ориентиров и векторов развития уголовного законодательства с учетом появления новых предметов уголовно-правовой охраны и противоправных посягательств на них.

Второй уровень указанного анализа имеет своей задачей формулирование научно обоснованного вывода о недостаточности имеющихся уголовно-правовых запретов для адекватной реакции государства на новые общественно-опасные посягательства и необходимых признаках новой уголовно-правовой нормы, устанавливающей преступность и наказуемость деяния.

Для **завершающего уровня** исследования необходимо аккумулировать правоприменительные (не только юрисдикционно-судебные) проблемы как уголовно-правовых норм, так и связанных с ними норм позитивного законодательства.

Такой обширный подход на третьем уровне исследования вопроса о возможности криминализации и пенализации общественно опасного деяния необходим, поскольку хоть уголовное законодательство и является единственным признанным монополистом констатации и преступности, и наказуемости, но и оно (уголовное законодательство) несвободно от известного влияния иных отраслей права, обильно используя термины и понятия, например, гражданского и семейного законодательства. Кроме этого, представляется обоснованным и вывод о том, что каждый правоприменительный субъект видит свое решение задач государства, исходя проблем, вытекающих из его деятельности [12. С. 63]. Значит, постановка разноплановых проблем, связанных с криминализацией и пенализацией деяния, безусловно, повысит вероятность принятия наиболее обоснованного итогового решения этого вопроса и в ряде случаев позволит избежать дефектности вновь принимаемых уголовно-правовых норм. Именно глубина проработки содержательных вопросов обоснованности криминализации и пенализации, а не функциональная чистота правоприменительной деятельности судов [9. С. 337–338] и иных государственных органов, лежит, по нашему мнению, в основе качественного изменения уголовного закона.

Оценивая адекватность государственно-принудительного воздействия на преступника в связи с уголовно-противоправным поведением можно говорить о наличии либо отсутствии необходимости изменения существующего уровня пенализации – отраженной в уголовном законе величине уголовной репрессии [3. С. 33–38, 47–48].

Как уже отмечалось криминализация и пенализация должны быть обусловлены социальными и криминологическими обстоятельствами, в том числе могут предопределяться изменением преступности [2. С. 60; 8. С. 73], например, появлением новых особых преступлений, совершаемых в отношении или с использованием криптовалюты и подобных цифровых финансовых активов, обобщенно именуемых «криптопреступностью» [10. С. 87].

Традиционно в юридической литературе под основанием криминализации деяния понимается необходимость в установлении новой уголовно-правовой нормы, продиктованная опасностью причинения вреда общественным отношениям в результате определенного поведения людей. Как правило, по аналогии с этим определяется и основание пенализации.

Содержание характера и степени общественной опасности преступления нашло свое отражение актах судебного толкования норм уголовного закона (в частности, посвященных практике назначения уголовного наказания). В соответствии с обозначенным толкованием характер такой опасности зависит от закрепленных при-

знаков преступления, направленности преступного посягательства на конкретные охраняемые уголовным законом социальные ценности и блага. А степень этой опасности определяется конкретными обстоятельствами учиненного – значим способ совершения преступления, форма вины, характер и размер вредных последствий, установленные судом и относящиеся к совершенному преступлению наказательные обстоятельства, как смягчающие (статья 61 Уголовного кодекса Российской Федерации), так и усиливающие (статья 63 Уголовного кодекса Российской Федерации) наказание.

При этом к наиболее общим критериям, влияющим на криминализацию (декриминализацию) и пенализацию (депенализацию) деяния, наряду с другими можно отнести:

– **опасность причинения вреда общественным отношениям** в результате поведения определенной категории людей, которая детерминирует как состав преступления, так и размер (меру) наказания за совершенное преступление;

– **относительную распространенность деяния** [11. С. 54], указывающую на невозможность борьбы уголовно-правовыми методами с единичными отклоняющимися от принятой нормы поступками;

– **увеличение значимости преступных последствий (вреда, ущерба) с учетом социально-экономических особенностей развития общества на отдельном историческом этапе.** Так, например, именно внушительное увеличение капитализации криптовалют [10. С. 86] определило судебную практику, фактически разделяющую позицию ученых об отнесении криптовалюты к предмету хищения в виду ее очевидной экономической ценности, несмотря на отсутствие физического признака [1]. Об этом, в частности, свидетельствует ряд кассационных определений, констатирующих возможность отнесения криптовалюты к предмету разбоя и вымогательства, в которых подчеркивается, что цифровая валюта как иное имущество может выступать предметом указанных составов преступлений в виду наличия экономического интереса и материальной ценности;

– **последовательная направленность лиц на совершение однородных проступков (административная преюдиция).** Использование модели административной преюдиции при установлении запрета в уголовном законе помогает скорректировать меры государственного принуждения при совершении деяний, не отличающихся значительной общественной опасностью по сравнению с иными преступлениями и способно решить не только проблему излишней криминализации уголовного закона, но и позволяет эффективно отграничить преступления от административных правонарушений, в том случае если наступление уголовной ответственности поставлено в зависимость от размера наступивших общественно опасных последствий, которые не всегда возможно точно установить [5. С. 8].

При анализе специфических особенностей, связанных с криминализацией и пенализацией преступлений, совершенных с использованием цифровых технологий, на первом месте должно стоять понимание их неоднородности, что объективно отражается в уголовном законодательстве.

В целом преступления, связанные с использованием цифровых технологий, в наиболее общем виде можно разделить на две группы.

К первой группе относятся преступления в сфере компьютерной информации (предметом указанных преступлений является информация и информационные системы).

Само появление данной группы преступлений было обусловлено оформлением новых общественных отношений, связанных с компьютерными технологиями.

На момент включения соответствующих статей в УК Российской Федерации в полной мере тенденции развития этой, в целом новой, сферы общественной жизни не были до конца понятны, поэтому смысловая нагрузка, которая была вложена в данные нормы, приобретала свою актуальность по мере развития информационных технологий.

Вместе с тем было бы неверным утверждение о том, что положения главы 28 УК Российской Федерации, в которой и закреплены соответствующие нормы, с учетом крайне динамично развивающихся общественных отношений также подвергались столь же динамичным изменениям.

В настоящий момент в главе 28 УК Российской Федерации закреплены следующие правовые нормы:

1. Неправомерный доступ к компьютерной информации (статья 272 УК Российской Федерации).

2. Создание, использование и распространение вредоносных компьютерных программ (статья 273 УК Российской Федерации).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК Российской Федерации).

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 2741 УК Российской Федерации).

5. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (статья 2742 УК Российской Федерации).

Ко второй группе относятся преступления, квалифицирующим признаком которых является их совершение с использованием информационно-коммуникационных технологий:

1. Преступления против государственной власти, мира и безопасности человечества (статьи 280, 282, 280^4, 354^1 УК Российской Федерации).

2. Преступления против личности (статьи 110, 110^2, 133, 128^1, 151^2 УК Российской Федерации).

3. Преступления против общественного порядка и безопасности (статьи 205^2, 222^1, 222, 222^2, 230, 228^1, 238^1, 242^2, 242, 258^1, 274^1, 274^2 УК Российской Федерации).

4. Экономические преступления (статьи 158, 159, 1712, 185^3 УК Российской Федерации).

Чаще всего наличие данного квалифицирующего признака отражает не только фактический рост количества соответствующих деяний, но и состояние общества, при котором «цифровизация реальности» является неотъемлемым ее элементом [4. С. 15].

Однако далеко не во всех случаях формальное увеличение числа деяний должно становиться безусловным основанием для констатации факта роста их общественной опасности и их криминализации и пенализации.

Наиболее явным примером в этом случае является установление в ст. 158 УК РФ в качестве квалифицирующего признака – кражи с банковского счета, а равно в отношении электронных денежных средств, когда хищение зачастую незначительных денежных сумм образует состав тяжкого преступления [4. С. 15–16].

Наряду с этим не вызывает сомнений, что в некоторых случаях рост общественной опасности отдельных деяний непосредственно связан со способом их совершения (с использованием информационно-коммуникационных технологий).

В частности, совершение незаконного производства или сбыта наркотических средств с использованием электронных или информационно-телекоммуникационных сетей, безусловно, упрощает совершение деяния, делает возможным реализацию наркотических средств массовой.

В некоторых случаях использование информационно-коммуникационных технологий обеспечивает возможность реализации публичного характера распространения информации при совершении преступления.

На это обстоятельство Верховный Суд Российской Федерации указал, например, в Обзоре по отдельным вопросам судебной практики, утвержденном 30.04.2022, определив, что публичный характер распространения заведомо ложной информации может проявляться в использовании информационно-телекоммуникационных сетей (в том числе в размещении лицом в сети «Интернет» материала, содержащего ложную информацию).

Кроме того, вопросам, связанным с использованием электронных или информационно-телекоммуникационных технологий при совершении отдельных категорий преступлений, Пленум Верховного Суда Российской Федерации посвятил отдельное постановление («О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»).

Указанное постановление посредством легального толкования во многом направлено на устранение существующих правовых пробелов в данной сфере, формирование единого понимания правовых категорий, связанных с информационно-телекоммуникационными технологиями, приведение уголовно-правового понимания указанных категорий с социальными реалиями.

Резюмируя, отметим, что в случае явного увеличения общественной опасности отдельных преступлений, способ совершения которых непосредственно связан с использованием информационно-коммуникационных технологий, они могут быть криминализированы с установлением уголовной наказуемости за их совершение. Это сделает возможным проявление адекватной и решительной реакции государства на соответствующее преступное поведение, связанной с назначением за содеянное справедливого наказания [7. С. 95].

Появление преступлений, совершаемых с использованием цифровых (информационно-телекоммуникационных) технологий, нередко новых только по способу

совершения, но не отличающихся от иных преступлений по характеру и степени общественной опасности, по нашему мнению, само по себе не является достаточным основанием криминализации или пенализации (изменению ее уровня) [6. С. 57] без учета иных, заслуживающих внимания обстоятельств.

Список литературы

1. Архипов А. В. Цифровые объекты как предмет хищения // Уголовное право. 2020. № 6(124). С. 16–23. DOI 10.52390/20715870_2020_6_16. EDN IBQMOF.

2. Бабаев, М. М., Пудовочкин, Ю. Е., Андрианов, В. К. Уголовная политика: учебное пособие. М.: РГУП, 2018. 74 с.

3. Валеев, М. Т. Свойства уголовного наказания в свете теории пенализации / под. ред. В. А. Уткина. Томск: Изд-во НТЛ, 2006. 168 с.

4. Вельтмандер А. Т. Общественная опасность преступлений, совершенных с использованием информационно-коммуникационных (цифровых) технологий // Уголовная политика в условиях цифровой трансформации: сборник статей материалов II Всероссийской научно-практической конференции, Казань, 27 апреля 2023 года; отв. ред. М. А. Ефремова. Казань: Отечество, 2023. С. 11–16.

5. Каракулов, Т. Г. Административная преюдиция в уголовном праве // Правовые проблемы укрепления Российской государственности: сборник статей по итогам Всероссийской научно-практической конференции, Томск, 26–28 января 2017 года. Том 74. Томск: Национальный исследовательский Томский государственный университет, 2017. С. 8–9. EDN ZHMCQH.

6. Каракулов, Т. Г. К вопросу о допустимости лишения специального, воинского или почетного звания, классного чина и государственных наград за киберпреступления // Уголовная политика в условиях цифровой трансформации: сборник статей материалов II Всероссийской научно-практической конференции, Казань, 27 апреля 2023 года; отв. ред. М. А. Ефремова. Казань: Отечество, 2023. С. 52–59.

7. Каракулов, Т. Г. Обстоятельства, учитываемые при назначении наказания в виде лишения специального, воинского или почетного звания, классного чина и государственных наград // Сб. ст. по итогам Всерос. науч.-практ. конф. «Правовые проблемы укрепления российской государственности» / ред. О. И. Андреева, А. С. Князьков, Н. В. Ольховик, Л. М. Прозументов, М. К. Свиридов, В. А. Уткин. Томск: Издательство Томского государственного университета, 2022. Ч. 92. С. 94–95.

8. Каракулов, Т. Г. Социально-криминологическая обусловленность наказания в виде лишения специального, воинского или почетного звания, классного чина и государственных наград // Всероссийская научно-практическая конференция «Iustiti. fundamentum regni / Правосуди. основа государства», посвященная 100-летию Верховного Суда Российской Федерации: сб. тезисов докладо. Томск: Дельта-план, 2022. С. 71–74.

9. Наумов А. В. Уголовный проступок или преступление небольшой тяжести: терминологическое или принципиальное различие? // Уголовное право: стратегия развития в XXI веке: материалы XVI Междунар. науч.-практ. конф. М.: Проспект, 2019. С. 335–338.

10. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников

[и др.] // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 85–93. DOI 10.17150/2500–4255.2019.13(1).85–93. EDN HRIXOZ.

11. Прозументов Л. М. Криминализация и декриминализация деяний. Томск: Изд-во Том. ун-та, 2012. 142 с.

12. Пудовочкин Ю. Е., Бабаев М. М. Верховный Суд Российской Федерации и уголовно-правовое нормотворчество // Правосудие. 2019. Т. 1, № 2. С. 51–72. DOI: 10.17238/issn2686–9241.2019.2.51–72

13. Уткин В. А. Проблемы теории уголовных наказаний: курс лекций. Томск: Издательский Дом Томского государственного университета. 2018. 240 с.

14. Уткин В. А. Факторы пенализации и международное уголовное право / В. А. Уткин // Вестник Томского государственного университета. Право. 2015. № 2(16). С. 128–137.

15. Bloom, Nicholas, John Van Reenen, and Heidi Williams. A Toolkit of Policies to Promote Innovation // Journal of Economic Perspectives. 2019. №33(3). Pp. 163–84.

Ю. С. Климович,
кандидат юридических наук, доцент,
Национальный центр законодательства
и правовых исследований Республики Беларусь

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА НАЦИОНАЛЬНЫЕ МОДЕЛИ УГОЛОВНОГО ПРОЦЕССА РЕСПУБЛИКИ БЕЛАРУСЬ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Исследование посвящено анализу влияния цифровизации уголовного процесса на стабильность национальной модели уголовно-процессуальной деятельности. На конкретном примере показано, как внедрение технических инноваций и неолиберальная идеология в некоторых случаях используются для радикализации дискурса по трансформации не только уголовно-процессуальной модели, но и организации государственной власти в целом. Аргументирована позиция о некорректности подобного приема, технический прогресс и цифровизация должны не ослаблять, а укреплять существующие институты государства и общества.

Ключевые слова: цифровизация, уголовный процесс, протокол, государство, следователь, звуко- и видеозапись, модель, неолиберальная идеология

INFLUENCE OF DIGITIZATION ON NATIONAL MODELS OF CRIMINAL PROCEDURE IN THE REPUBLIC OF BELARUS AND THE RUSSIAN FEDERATION

Abstract. The study is devoted to analyzing the impact of digitalization of the criminal process on the stability of the national model of criminal procedure. A specific example shows how the introduction of technical innovations and neoliberal ideology in some

cases is used to radicalize the discourse on transforming not only the criminal procedural model, but also the organization of state power as a whole. The position is argued that such a technique is incorrect, technological progress and digitalization should not weaken, but strengthen the existing institutions of the state and society.

Keywords: digitalization, criminal process, protocol, state, investigator, sound and video recording, model, neoliberal ideology

Введение. «К 2050 году под давлением требований рынка и благодаря новейшим техническим средствам мир объединится вокруг планетарной торговой площадки без центрального государства. Начнется то, что я называю гиперимперией. Сначала распадутся государственные службы, затем демократия, а потом и сами государства», – таким еще в 2009 г. в книге «Краткая история будущего» рисовал перспективы человечества известный экономист и политический деятель Европы Ж. Аттали [2].

Сегодня в уголовно-процессуальной науке Республики Беларусь и Российской Федерации наблюдается стремительный рост интереса ученых-процессуалистов к тематике технологического развития и цифровизации уголовного процесса. Активно обсуждаются перспективы появления электронного уголовного дела, использования блокчейна, разнообразных технических средств получения и хранения информации, а также внедрения искусственного интеллекта в процесс отправления правосудия [5]. В этой связи актуальным становится анализ влияния этих процессов на национальную модель уголовного процесса как важный элемент государственного механизма власти. Важно, чтобы технологические инновации способствовали поступательному развитию общества, вносили вклад в стабильность и суверенитет государства.

Основная часть. Рассмотрим это на частном примере технологизации уголовно-процессуальной деятельности, связанном с появлением в перечне источников уголовно-процессуальных доказательств их новой разновидности в виде звуко- и видеозаписи показаний (ч. 2 ст. 88 Уголовно-процессуального кодекса Республики Беларусь). Это новация придала еще большую актуальность давно дискутируемому вопросу обязательности протокола как основного способа хранения вербальной доказательственной информации. Появились предложения перенести на предварительное расследование практику судебного рассмотрения уголовных дел, когда все, что имеет доказательственное значение, посредством звуко- или видеозаписи сохраняется на электронный носитель информации, а в кратком протоколе отражаются преимущественно установочные сведения участников процесса и ключевые решения суда. При этом относительно письменного протокола как обязательного атрибута процессуальной формы следственного действия есть различные подходы. Одни белорусские ученые предлагают его сохранение и параллельное использование в безбумажной цифровой форме наряду с широким внедрением разнообразных технических средств фиксации информации.

«Развитие уголовно-процессуального законодательства государств постсоветского пространства главным образом сдерживается взглядом на письменную форму как на основную и незаменимую форму фиксации в уголовном процессе.

Но в условиях современного развития науки и информационных технологий, активной государственной политики в сфере электронного правительства этот взгляд может быть заменен на отношение к письменной форме как главной, но не единственной и заменимой форме фиксации информации в уголовном процессе», – пишет Т. А. Савчук [4. С. 149].

Другие идут дальше, считая возможным в принципе отказаться от протокола как обязательного элемента процессуальной формы. По их мнению, письменная форма производства уже несовременна и не соответствует уровню развития технологий, вся информация по делу может хранится на самых разнообразных технических средствах. «Развитие информационных технологий и совершенствование процессуального законодательства позволяют сделать вывод, что в ближайшем будущем существующие традиционные виды доказательств (протоколы следственных и иных процессуальных действий, другие письменные документы) будут заменены электронными носителями информации», – считает представитель Научно-практического центра Генеральной прокуратуры Республики Беларусь Ю. А. Никитин [3].

После прочтения указанных точек зрения складывается впечатление, что письменный протокол следственного действия мыслится отечественными исследователями как всего лишь более архаичный по сравнению с новыми техническими средствами способ хранения и передачи информации, когда вопрос «прощания с бумагой» становится делом времени. Аналогичные воззрения массово присутствуют и среди представителей российской науки.

Считаем такой взгляд поверхностным и, как следствие, в корне неверным. На самом деле все не так просто, протокол – одно из ключевых звеньев национальной модели процесса, исключение которого неминуемо по принципу окна Овертона откроет путь к ее глубинной трансформации. К сожалению, в наше время многие ученые-правоведы часто теряют из вида доктринальные основания своей области знания и утрачивают возможность критического мышления, когда попадают под «очарование» технологических инноваций. Такая лояльность к цифровым технологиям может быть объяснена особенностями человеческой психики, когда на ней сказывается эффект всеобщей моды на диджитализацию общества.

Нельзя забывать, что в основании отечественного уголовного процесса лежит публичное начало и архетип следственной формы производства по делу, оказавший значительное влияние на всю организацию его стадий и основных процессов. Центральной фигурой досудебного производства является следователь, во многом с ним законодатель связывает возможность достижения объективной истины – главного ценностного ядра, фундирующего остальную процессуальную материю. Под следователя выстроена вся досудебная уголовно-процессуальная инфраструктура в виде институтов уголовного дела, следственных действий, предмета и пределов доказывания. В этих условиях протокол следственного действия не просто инструмент сбора и хранения доказательственной информации, это sine qua non процессуальной функции следователя, то без чего он из органа, ведущего уголовный процесс, превратиться всего лишь в субъекта полицейского дознания, займет принципиально иную позицию во властных отношениях предварительного расследования. Через концепт «источник доказательства» и, главным образом,

через процессуальную форму протокола в отечественной доказательственной теории обосновано право следователя получать полноценные, а не так называемые «полицейские доказательства».

Будем говорить откровенно, в отличие от компьютерного носителя данных, нейтрального по отношению к фиксируемой информации, протокол следственного действия имеет конкретного автора, поэтому в нем отражается то содержание следственного действия и та информация, которая по субъективному мнению следователя соответствует стандартам всестороннего, полного и объективного исследования обстоятельств дела. Лишая следователя права формировать протокол, мы лишаем его самого главного – власти по формированию процессуальных доказательств. Далее он закономерно должен утратить права на реализацию юрисдикционных решений, применение мер принуждения и т. д. Безусловно, у части научного сообщества, выступающего за цифровизацию процесса, на самом деле именно такие цели и присутствуют, так как для них по идеологическим причинам неприемлема модель с сильной государственной составляющей.

В стремлении отдельных авторов избавиться от протокольной формы производства прослеживается желание отказаться не только от следователя, но и в целом от той модели уголовного процесса, которая сейчас существует и которая уполномочивает компетентное лицо от имени государства устанавливать обстоятельства совершения преступления. И в этом мы видим большую опасность, так как слишком велика значимость сложившегося уголовно-процессуального механизма противодействия преступности в механизме государственной власти, слишком велики риски поспешных реформ. В качестве альтернативы в большинстве случаев предлагается состязательная модель досудебного производства с полицейским дознанием, где концепт производства по уголовному делу заменяется параллельным расследованием полиции и стороны защиты. Не объективная истина, а состязательность теперь должна стать главным критерием справедливости процесса.

На постсоветском пространстве подобная конструкция в наиболее законченном, фактически повторяющем американский образец, виде реализована в Грузии, и нельзя сказать, чтобы результаты реформы оценивались однозначно положительно. Уже сегодня отдельные авторы инициируют упразднение Следственного комитета Российской Федерации и связанной с ними модели доказывания, построенной вокруг монополии следователя на составление протокола следственного действия. Однако самое главное, что сверхзадачей цифровизации уголовного процесса становится ослабление самого государства, сведение его к концепту сервиса или цифровой площадки, что, по прогнозам упомянутого нами ранее Ж. Аттоли, на определенном этапе приведет к упразднению традиционного государства как такового.

«Мы считаем актуальным и полезным осмыслить роль государства в качестве создателя и управляющего цифровой платформой, на которой располагается уголовный процесс. Государство как цифровая платформа трактуется нами в виде набора сервисов (услуг), представляемых населению, бизнесу для разрешения правовых вопросов… Государство – это даже не чиновник, не государственный орган, а тот обезличенный «некто» (Другой), с кем я выступаю в диалог на цифровой платформе с запросом: принять заявление, исковое заявление – обвинение,

доказательство и пр.», – прямо пишут представители Нижегородской научной школы А. С. Александров и А. А. Александрова [1. С. 25–26].

Признаем, что в Республике Беларусь пока что мы не фиксируем распространения таких откровенно глобалистских подходов, в основном цифровые технологии рассматриваются как средство оптимизации производства по делу, оказания технологической помощи субъекту расследования и другим участникам процесса. Очевидно, сказываются особенности политического устройства, для которого децентрализация правоохранительных органов власти абсолютно неприемлима. Хотя мы и отдаем себе отчет в том, что рано или поздно вопрос в этой плоскости будет поставлен, ибо идеям свойственно находить себе дорогу.

Фактически мы наблюдаем, как внедрение технических инноваций используется для радикализации российского юридического дискурса для трансформации уголовно-процессуальной модели и организации государственной власти в целом. Считаем такой подход манипулятивным и неприемлемым, особенно в условиях текущей политической обстановки, когда страна находится в условиях санкционного противостояния и общество как никогда нуждается в стабильной централизованной власти. Мы, конечно, можем вести речь о совершенствовании порядка ведения уголовного процесса, имеем право сравнивать достоинства и недостатки состязательного и следственного порядка производства по делу, однако дискуссия должна вестись корректно. Эти модели должны сопоставляться автономно, без каких-либо идеологических предпочтений и навешивания ярлыков. Неправда, что технические инновации применимы только в состязательном процессе, который, кстати, в своей частно-исковой (обвинительной) форме является исторически наиболее архаичным. На самом деле посредством использования технического прогресса происходит очередная активизация антиэтатистского импульса на уровне уголовно-процессуальной деятельности. Глубинно это является следствием доминирования у определенной части общества неолиберальной идеологии, в центре которой находится идея «прав человека» и атомарный индивид, максимально освобожденный от «оков» государства и всех форм коллективной индентичности. Субъекты этой идеологии исходят из того, что традиционное государство с сильными институтами власти является априори авторитарным и должно уйти в прошлое, уступив место «гражданскому обществу», лишенному каких-либо религиозных, нравственных, и этических «предрассудков» прошлых эпох. Со временем оно должно эволюционировать в своего рода корпорацию или предприятие, где вместо политиков ключевые решения будут реализовываться менеджерами и цифровыми приложениями. Для этого они активно привлекают высокие технологии, которые весьма удобны, так как по своей природе выступают эффективным средством распределения коммуникативных каналов, предоставляя индивиду пространство максимальной свободы, делая его более «невидимым» для институтов власти государства. Хотя, как показывает практика капиталистического производства, в конечном итоге использование современными корпорациями технических средств приводит к кратному увеличению степени эксплуатации индивида и контроля за его поведением.

Заключение. Считаем, что технический прогресс и цифровизация должны не ослаблять, а укреплять институты государства, общества и права, трансформа-

ция которых возможна, но не на основе копирования бизнес-процессов, а исходя из более фундаментальных оснований, традиций и национальных интересов. В конечном итоге вопросы политического устройства нужно обсуждать не в связи с проблематикой технологизации и цифровизации уголовного процесса, они к ней прямого отношения не имеют.

В основе уголовного процесса любого государства находят свое отражение идеи и ценности его политического, социального и культурного устройства. Смешанный характер и российского, и белорусского уголовного процесса, когда досудебное производство построено на следственных началах, где определяющую роль в познании события преступления играет представитель публичной власти, есть выражение патерналистской логики развития обоих государств.

Испокон веков наши народы жили общиной, именно она формировала их особый менталитет и поведенческие нормы, где служение общему благу, справедливости и «миру» превалировало над интересами отдельной личности. В общине человек находил свою защиту, его вечевым решениям он должен был подчиняться.

В последующем более близкие к нам формы государства унаследовали функцию по решению ключевых вопросов общественной жизни. История обоих наших народов свидетельствует, что именно с сильным государством связаны периоды их наибольшего развития.

Государство всегда находилось в центре общественно-политических и правовых процессов. Россия вообще долгое время де-юре имела имперское устройство. Поэтому в сильной следственной власти, как и в сильном традиционном, а не платформенном государстве мы видим закономерности нашего исторического процесса и необходимое условие стабильного развития в будущем.

Список литературы

1. Александров А. С., Александрова И. А. Судебный процес – источник права и справедливости // Правовое государство: теория и практика. 2022. № 1. С. 11–29.

2. Аттали Ж. Краткая история будущего. URL: https://royallib.com/read/attali_gak/kratkaya_istoriya_budushchego.html#0

3. Никитин Ю. А. Интернет как источник информации в расследовании уголовных дел (часть 2): доказательства // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2023.

4. Савчук Т. А. Использование информационных технологий в уголовном процессе // Актуальные вопросы развития правовой информатизации в условиях формирования информационного общества: сб. науч. ст. / Нац. центр правовой информ. Респ. Беларусь. Минск, 2017. С. 147–153.

5. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

Д. В. Кривин,
экономист по бухгалтерскому учету и хозяйственной деятельности,
ООО «Консорциум строительных компаний»

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ ПЕРЕМЕН: ЗАКОНОДАТЕЛЬНЫЕ ВЫЗОВЫ

Аннотация. Статья посвящена анализу составов преступлений Уголовного кодекса Российской Федерации, совершенных с использованием сети «Интернет», а также судебной практики по компьютерным преступлениям. Киберпреступность определяется как совокупность способов совершения преступлений в отношении компьютерной информации, ее составляющих и иных киберпосягательств, которые могут совершаться в отношении личности, общества и государства. Увеличение киберпреступлений сказалось на росте экономических преступлений в период пандемии COVID-19, росте преступлений экстремистской направленности, обусловленном российско-украинским конфликтом и начавшейся специальной военной операцией. Делается вывод о необходимости совершенствования отдельных положений уголовного закона в части действий, посягающих на национальные интересы России и воспрепятствованию реализации отечественных национальных приоритетов.

Ключевые слова: киберпреступность, Интернет, компьютерная информация, кибертерроризм, COVID-19, административная преюдиция, информационная безопасность, национальная безопасность, национальные интересы, национальные приоритеты

CYBERCRIME IN THE WORLD OF CHANGE: LEGISLATIVE CHALLENGES

Abstract. The article is devoted to the analysis of crimes using the Internet, provided for by the Criminal Code of the Russian Federation, as well as judicial practice on computer crimes. Cybercrime is defined as a set of ways of committing crimes against computer information, its components and other cyber-attacks that can be committed against an individual, society and the state. The increase in cybercrime affected the growth of economic crimes during the COVID-19 pandemic, the growth of extremist crimes caused by the Russian-Ukrainian conflict and the beginning of a special military operation (hereinafter referred to as SMO). The author also pays attention to the gap in the lack of formal certainty and the presence of evaluative concepts in Article 280.4 of the Criminal Code. It is concluded that it is necessary to improve this article in terms of actions that infringe on the national interests of the Russian Federation and hinder the implementation of the national priorities.

Keywords: cybercrime, internet, computer information, cyberterrorism, COVID-19, administrative prejudice, information security, national security, national interests, national priorities

Актуальность темы обусловлена тем, что в связи с происходящей компьютеризацией и интернетизацией общества все же встречается часть людей, особенно

пенсионного возраста, которые не владеют компьютерной грамотностью. В связи с этим у преступников не вызывает большого труда использовать их персональные данные в личных целях, что приводит к росту преступности в информационной сфере.

Киберпреступность охватывает единое информационное пространство и затрагивает не только науку информационного права, но также уголовного права и криминологии. Киберпреступность всегда была неразрывно связана с развитием электронно-вычислительных машин, с помощью которых уже стало возможно совершать различные незаконные действия с большим количеством информации, хранящейся в файлах и системах [8. С. 133]. Вследствие этого в науке и возникают различные термины с приставкой «кибер-» (киберинциденты, кибератаки, киберустойчивость, кибербезопасность, киберпространство и т. д.), чтобы обозначить принадлежность юридического факта к виртуальному миру. Ю. М. Батурин и С. В. Полубинская рассматривают виртуальный мир в тесной взаимосвязи с реальным миром, поскольку противоправные деяния в виртуальном мире порождают правовые последствия уже в мире реальном. Авторы отмечают, что в виртуальном мире действуют «нормы, установленные разработчиком, обычаи виртуального делового оборота, но применяются и правовые нормы реального мира, хотя и достаточно неопределенные ввиду множественности правовых систем» [4. С. 21]. Из этого следует, что ввиду отсутствия системы законодательства виртуальный мир является не самостоятельной правовой системой, а частью реального мира. Россия принадлежит к романо-германской правовой семье, основным источником права в которой является закон.

Преступлениям в сфере компьютерной информации посвящена глава 28 УК РФ, и все они имеют общий видовой объект – компьютерную информацию. 14.07.2022 было принято два федеральных закона: согласно Федеральному закону № 260-ФЗ включена в УК РФ статья 274.2, а Федеральный закон № 259-ФЗ дополнил Кодекс Российской Федерации об административных правонарушениях статьями 13.42 и 13.42.1, в которых предусмотрен штраф в зависимости от вида субъекта предпринимательской деятельности за нарушение требований к пропуску трафика через технические средства. Обязательным условием для привлечения субъекта к уголовной ответственности является наличие:

– признаков субъекта преступления – им должно быть должностное лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации;

– административной ответственности, что указывает на наличие такой меры, как административная преюдиция.

Статьей 274.2 УК РФ предусмотрены более суровые санкции в сравнении с административным штрафом и отличаются они уже более широким разнообразием – самым строгим наказанием являются принудительные работы и лишение свободы на срок до трех лет [1]. Судебная практика по данным уголовным делам еще только начинает формироваться, но при качественном расследовании, преду-

преждении и своевременном предотвращении таких противоправных деяний будет велика вероятность сокращения их совершения.

15 декабря 2022 г. было принято Постановление Пленума Верховного Суда РФ № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». Речь в данном постановлении прямо идет о киберпреступлениях, а использование сети «Интернет» рассматривается как способ их совершения. В частности, в пункте 2 дается определение компьютерной информации, под которой понимаются любые сведения, представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. В том же пункте идет конкретизация предмета компьютерных преступлений – к ним относятся любые электронные устройства, к признакам которых относятся:

а) способность выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов;

б) оснащенность встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации [10]. Одним из признаков такой информации является конфиденциальность в силу неизвестности ее третьим лицам. В Уголовном кодексе Республики Азербайджан (статья 271) описан состав преступления, выражающегося в форме неправомерного доступа к компьютерной системе. В данном случае субъект, подключающийся к компьютерной системе без авторизации, нарушает неприкосновенность информации, к которой он не имеет доступа [12. С. 40]. Данная информация может в дальнейшем использоваться без согласия лица, право которого нарушается, что приводит к совершению так называемых кибермошенничеств.

В разгар пандемии COVID-19 резко возросло количество мошенничеств в сфере компьютерной информации, что в конечном счете сказалось на общей статистике выявления лиц, совершивших преступления экономической направленности (рис. 1). Темп роста составил почти 22 % в 2021 г. (53 717 человек) относительно 2020 (44 072 человек), что является самым высоким показателем за анализируемый период. Самыми распространенными случаями компьютерных преступлений в России являются сбои в работе компьютера: медленная загрузка операционной системы, замедление работы компьютера или подключенных устройств, медленные и неверные реакции компьютера на команды пользователя и т. д. И поскольку каждый случай такого киберпреступления уникален сам по себе, то на стадии их расследования преступлений часто допускаются ошибки, сводящиеся к ненадлежащей сборке доказательств, которые впоследствии могут быть признаны судом недействительными. На наш взгляд, одной из причин низкого качества предварительного расследования киберпреступлений является отсутствие качественных методических разработок, при реализации которых в полной мере использовались бы информационные технологии.

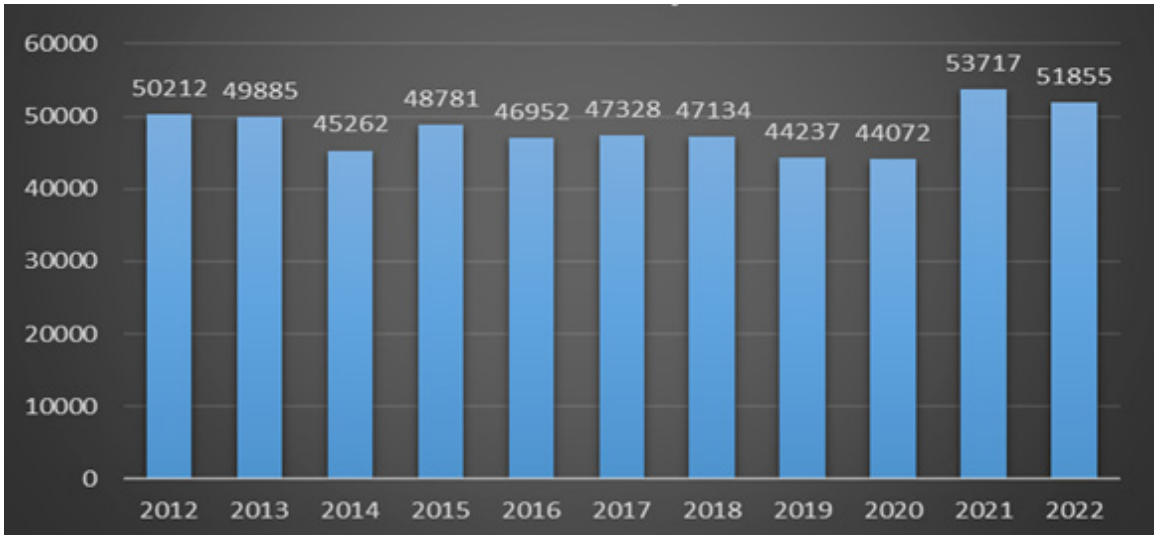


Рис. 1. Статистика выявления лиц, совершивших преступления экономической направленности

Пандемия COVID-19 послужила катализатором роста киберпосягательств на организации здравоохранения, об их предметах пишут Л. Р. Клебанов и С. В. Полубинская. Они выделяют такие устройства медицинского назначения, как носимые и не носимые устройства, соединенные с Интернетом (например, CYCORE), цифровые платформы для сбора данных о пациентах (например, DART), чат-боты и «умные помощники». Под последними понимаются технологии на основе искусственного интеллекта и нейросети, дающие ответы на голосовой запрос (Amazon's Alexa, Google's Assistant, Microsoft's Cortana, Apple's Siri) [7. С. 248]. Все они представляют собой программы, созданные на основе искусственного интеллекта, искажающие данные о здоровье человека. В таких случаях велика вероятность возникновения ситуаций, когда здоровому человеку могут выдать ложную картину заболевания (ошибки первого рода) и случаев, когда отсутствуют признаки заболевания (ошибки второго рода), когда, например, на снимках отсутствуют следы онкологии или рака при наличии таковых.

Таким образом, мы можем увидеть яркий пример посягательства на такой объект уголовного права, как здоровье населения и общественная нравственность. Их родовым объектом, как и преступлений в сфере компьютерной информации, является общественная безопасность и общественный порядок – он также присущ экологическим преступлениям, терроризму, вандализму, массовым беспорядкам и иным преступлениям, которые приобретают массовый характер и международные масштабы. В связи с этим появилось такое понятие, как «кибертерроризм», характеризующийся тем, что компьютерные преступления становятся элементами террористической деятельности.

Современный кибертерроризм широко использует достижения науки и техники, последние инновационные технологии, благодаря чему существенно возрастают его негативные последствия. А. А. Карцхия, рассматривая данное киберправонарушение, выделяет так называемый кибервойн, под которым понимает «использование ложной, фейковой информации, обработка сознания человека и общества, целью

которого может быть конкретное лицо (государственный или общественный деятель, популярный политик и др.), а также получение глобального результата (массовых беспорядков или гражданского неповиновения, формирование негативного образа публичной власти и др.) [6. С. 87]. Довольно часто посредством Всемирной сети возникают пропагандические моменты, связанные с ненавистью на национальной почве и иные негативные проявления.

Экстремистская деятельность является разновидностью преступлений против основ конституционного строя и безопасности государства, к которым также относятся государственная измена, шпионаж и диверсия. Родовым объектом таких преступлений является государственная власть и это означает, что информационная составляющая становится частью национальной безопасности Российской Федерации. Использование информационно-телекоммуникационных сетей, включая сеть «Интернет», является квалифицирующим признаком преступлений, предусмотренных ч. 2 ст. 280, ч. 2 ст. 280.1, п. «в» ч. 2 ст. 280.4, ст. 282, п. «в» ч. 2 и ч. 4 ст. 354.1 УК РФ. При квалификации таких преступлений особое значение имеет не только форма выражения своих убеждений, но и способы, место и обстоятельства распространения информации и ее содержание. Пункт 19 Постановления Пленума Верховного Суда РФ закрепляет, что, если предметом преступления, совершенного с использованием сети «Интернет», является переносное (в том числе и мобильное) устройство, то местом совершения данного противоправного деяния является место совершения лицом действий, входящих в объективную сторону состава преступления. Речь идет о территориальной подсудности уголовного дела, т. е. территории, на которой субъект использовал переносное устройство для совершения киберпреступления или размещал информацию экстремистского характера.

Статья 282 УК РФ в своем названии содержит прямое указание на цель преступления – возбуждение ненависти либо вражды, а также унижение достоинства человека либо социальной группы. Верховный Суд РФ в Постановлении Пленума от 20.09.2018 № 32 прямо разъясняет, случай когда деяние может быть квалифицировано по статье 282 УК РФ, а именно когда установлено, что «лицо осознавало направленность деяния на нарушение основ конституционного строя, а также имело цель возбудить ненависть или вражду либо унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе» [11]. Таким образом, цель должна содержать в себе реальную возможность совершения действий из перечня, предусмотренного диспозицией статьи 282 УК РФ. Умысел может быть только прямым и иметь отношение к той социальной группе, на нематериальные блага которой направлено посягательство. Данный состав, равно как и состав описанной ранее статьи 274.2 УК РФ, является формальным, бланкетным и содержит в себе административную преюдицию.

Основная задача уголовного закона состоит в первую очередь в предупреждении и установлении справедливого наказания за преступное деяние. Но при этом современная уголовная политика не должна быть статичной, так как с учетом прогнозирования реальных и перспективных рисков и угроз национальной безопасности, включая изменение состояния, структуры и динамики преступности, необходимо качественно реагировать на происходящие изменения.

Одним из таких направлений является совершенствование уголовно-правовых норм в рамках законотворческого процесса, в частности введение в УК РФ статей 280.3 и 280.4.

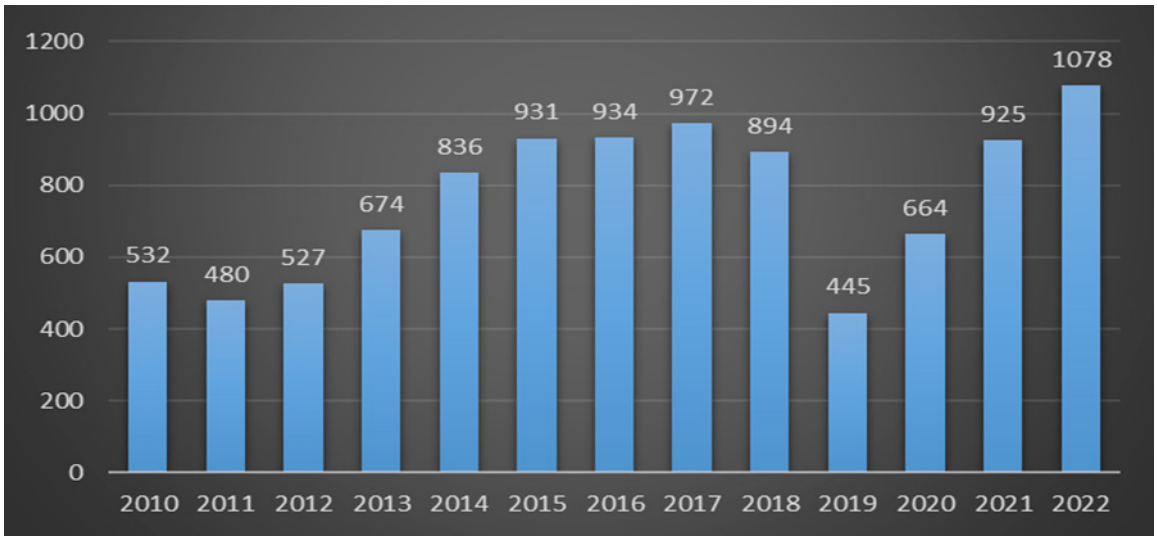


Рис. 2. Статистика выявления лиц, совершивших преступления экстремистской направленности

На основании представленных данных следует отметить, что резкий рост преступлений экстремистской направленности с 2019 г. увеличил количество расследованных преступлений и непосредственно направленных в суд (рис. 2, табл. 1). С ростом числа преступлений количество нераскрытых и ненаправленных дел в суд уголовных дел не изменилось, но в 2022 г. их доля составила 7 % против 18,5 % в 2019 г., что может свидетельствовать, во-первых, о высокой раскрываемости преступлений экстремистской направленности и во-вторых о наиболее частом варианте использовании административной преюдиции, о которой говорилось ранее.

Таблица 1

Данные о преступлениях экстремистской направленности в России за 2019–2022 гг.

Категория/год	Год			
	2019	2020	2021	2022
Выявлено лиц, совершивших преступления экстремистской направленности	445	664	925	1078
Предварительно расследовано преступлений экстремистской направленности	454	677	908	1257
Количество преступлений экстремистской направленности, уголовные дела о которых направлены в суд	370	590	819	1166
Процент не направленных дел в суд	18,5	12,85	9,8	7,2

В отношении статьи 280.3 УК РФ также действует административная преюдиция. Переходя к анализу диспозиции статьи 280.4 УК РФ, можно увидеть,

что ее формулировка в части «деятельности, направленной против безопасности Российской Федерации», является оценочной и формально не определенной, что по справедливому замечанию некоторых авторов, не отвечает конституционным требованиям ясности, определенности и недвусмысленности правовых норм [5. С. 93]. Останавливаясь на названии статьи – «Публичные призывы к осуществлению деятельности, направленной против безопасности государства» – следует отметить, что в уголовном законодательстве не содержится понятия «публичность», в связи с чем его толкование представляется крайне затруднительным в плане определения признаков деяния, совершенного в данной форме. Состав диспозиции статьи 280.4 УК РФ, как и статьи 280.3, позволяет отнести их к числу преступлений террористической направленности, на что косвенно указывает отграничение перечисленных в части 1 статьи 280.4 УК от квалифицированного состава терроризма части 2 статьи 205.2 УК РФ. Использование сети «Интернет» (п. «в» ч. 2 ст. 280.4 УК РФ) делает состав преступления квалифицированным, придавая ему более широкий масштаб. Использование сети «Интернет» является одним из способов совершения преступления в публичной форме, так как результат деяния становится хорошо видным и известным большинству простых людей.

В диспозиции анализируемой статьи не конкретизирована форма совершения такой деятельности, не указан также перечень деяний, который будет считаться посягательством на безопасность РФ, что на наш взгляд, требует законодательной доработки. Следует дополнить диспозицию части 1 статьи 280.4 УК РФ, «иными действиями, посягающими на национальные интересы и реализацию национальных приоритетов Российской Федерации» – объективно значимыми потребностями личности, общества и государства в обеспечении их защищенности и устойчивого развития.

Перечень национальных интересов и приоритетов РФ обозначен в пунктах 25 и 26 Указа Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [2]. Одним из таких приоритетов как раз является информационная безопасность, выделенная в Указе Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [3]. Пункт 8 закрепляет национальные интересы РФ в информационной сфере, к которым относятся: обеспечение получения и использования информации гражданами России, неприкосновенности частной жизни при использовании информационных технологий, обеспечение функционирования критической информационной инфраструктуры, развитие информационных технологий и укрепление суверенитета РФ в информационном пространстве. Любые посягательства на данные национальные интересы и воспрепятствование их реализации должны регулироваться статьей 280.4 УК РФ.

По мере развития технологий и производства на отечественный и международный рынки выходит новое компьютерное оборудование и другие формы электронно-вычислительной техники, обладающие более широкими возможностями, в результате чего появляются новые виды киберпреступности. Для дальнейшего расследования подобных дел невозможно обойтись без привлечения грамотного специалиста в сфере информационных технологий, с которым необходимо работать сотрудникам правоохранительных органов.

Тем не менее распространенность данных деяний требует уже от правоохранительных органов хотя бы базового уровня компьютерной грамотности с целью более точного понимания сути дела и улучшения качества работы. Роль специалиста в расследовании киберпреступлений на сегодняшний день очень сильно преувеличена, потому как он не является полноценным участником расследования, он лишь помогает провести его качественно и точно. Таким образом, мы можем видеть в данном случае наличие в роли следователя лишь наблюдательской позиции, хотя должно быть понимание нюансов работы с отдельными следственными действиями. Это является одним из главных законодательных вызовов сегодняшнего времени, поэтому необходимо тщательно подойти к разработке порядка действий следователя к расследованию киберпреступлений.

Широкая распространенность киберпреступлений, сопряженная со значительной турбулентностью современного мира, делает уголовное законодательство более гибким и в то же самое время поднимает вопросы, требующие законодательной доработки. К основным таким направлениям относится формальная неопределенность преступных деяний, определенных статьей 280.4 УК РФ, диспозиция которой содержит оценочный характер и не несет в себе содержательной части, фактически регулируя общественные отношения в аспекте государственной безопасности в рамках указанной статьи по остаточному принципу.

Использование технических средств стало относительно новым способом, выраженным в форме размещения призыва к осуществлению конкретных действий или деятельности, направленной на подрыв безопасности государства. Проблема также заключается и в том, что судебная практика по таким делам, как, впрочем, и по иным составам киберпреступлений еще не успела до конца сформироваться. Поэтому как законодателю, так и сотрудникам правоохранительных органов и иным правоприменителям уголовного закона очень важно обратить внимание на данные факторы, поскольку киберпреступления на сегодняшний день являются одной из самых актуальных уголовно-правовых категорий и включают общественно опасные посягательства с использованием сети «Интернет», совершаемые в отношении личности, общества и государства.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699

2. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271

3. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191

4. Батурин Ю. М., Полубинская С. В. Что делает виртуальные преступления реальными // Труды Института государства и права Российской академии наук. 2018. Т. 13, № 2. С. 9–35.

5. Ермолович Я. Н. Научно-практический комментарий к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-

процессуальный кодекс Российской Федерации» от 14 июля 2022 года № 260-ФЗ // Право в Вооруженных Силах. 2022. № 11. С. 89–102.

6. Карцхия А. А. Правовые аспекты современной киберпреступности // Правовая информатика. 2023. № 1. С. 83–92.

7. Клебанов Л. Р., Полубинская С. В. Цифровое здравоохранение, пандемия COVID-19 и проблемы кибербезопасности // Вестник Томского государственного университета. 2021. № 468. С. 243–252.

8. Кривин Д. В. Киберпреступность в системе преступлений особенной части уголовного права и ее особенности в современном обществе // материалы III Международной научно-практической конференции, приуроченной ко Дню Конституции РФ. Воронеж, 2019. С. 132–141.

9. Решение Верховного Суда Российской Федерации от 17.11.2014 по делу № АКПИ14–1292С // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=414233&ysclid=lm933gkpws258766306#E 5RaApTxWCCeGbKM

10. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/?ysclid=lm935fe2gn709237747

11. Постановление Пленума Верховного Суда РФ от 20.09.2018 № 32 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 года № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности». URL.: https://vsrf.ru/documents/own/27145/?ysclid=lm937rsibo201032077

12. Musayev E. Features and characteristics of information crimes in Azerbaijan criminal law // German International Journal of Modern Science. 2023. № 56. С. 40–43.

М. Е. Кубрикова,
кандидат юридических наук, судья,
Заднепровский районный суд города Смоленска

АКТУАЛЬНЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ ПРИ РАССМОТРЕНИИ УГОЛОВНОГО ДЕЛА В СУДЕ

Аннотация. В связи с расширяющейся информатизацией уголовного судопроизводства правоприменительная практика сталкивается с несовершенством правового регулирования. Цель настоящего исследования – проанализировать особенности разрешения вопроса о самоотводе судьи при автоматизированном распределении уголовных дел, аудиопротоколирования судебного заседания и публикации судебных актов на интернет-сайтах судов. В результате исследования сформулированы практические рекомендации и предложения по дальнейшему совершенствованию

существующего порядка, предоставив судье возможность устраниться от принятия уголовного дела к производству путем подачи мотивированной служебной записки руководителю суда; освободив секретаря судебного заседания при наличии аудиозаписи судебного заседания от обязательного указания в протоколе подробного содержания показаний, выступлений в прениях и последнего слова подсудимого; исключив расширительное толкование деперсонификации судебных актов, которые подлежат опубликованию на интернет-сайтах судов, путем удаления юридически значимой информации.

Ключевые слова: цифровизация, информатизация, уголовное судопроизводство, самоотвод судьи, протокол судебного заседания, аудиопротоколирование, секретарь судебного заседания, деперсонификация судебных актов, публикация судебных актов

CURRENT ISSUES OF DIGITALIZATION DURING THE CONSIDERATION OF A CRIMINAL CASE IN THE COURT

Abstract. Due to the expanding informatization of criminal proceedings, law enforcement practice faces imperfection of legal regulation. The purpose of this study is to analyze the specifics of resolving the issue of judge recusal in the automated distribution of criminal cases, audio recording of the court session and publication of judicial acts on the Internet sites of courts. In conclusion, the article formulates practical recommendations and proposals for further improvement of the existing procedure, giving the judge the opportunity to eliminate the adoption of a criminal case for production by submitting a reasoned memo to the head of the court; freeing the secretary of the court session in the presence of an audio recording of the court session from the mandatory indication in the protocol of the detailed content of testimony, speeches in the debate and the last word of the defendant; excluding the expansive interpretation of depersonification of judicial acts that are subject to publication on the Internet sites of courts by deleting legally relevant information.

Keywords: digitalization, informatization, criminal proceedings, judge's recusal, court session protocol, audio recording, court session secretary, depersonalization of judicial acts, publication of judicial acts

Введение. Цифровая трансформация является национальной целью развития России до 2030 г. [8]. В этой связи 15.02.2021 приказом Председателя Верховного Суда РФ № 9-П была утверждена Концепция информатизации Верховного Суда Российской Федерации, согласно положениям которой между судами преобладает бумажная форма коммуникации, однако электронная форма должна постепенно стать основной по отношению к бумажной, для чего требуется ускорить автоматизацию электронного судопроизводства [2].

Использование информационных технологий предусмотрено в Уголовно-процессуальном кодексе Российской Федерации (по далее – УПК РФ). В данной статье остановимся подробнее на некоторых проблемных аспектах, возникающих в связи с информатизацией уголовного судопроизводства.

Основная часть. 1. Согласно ч. 1 ст. 30 УПК РФ для рассмотрения уголовного дела состав суда формируется с помощью автоматизированной информационной системы с учетом нагрузки и специализации судей. В целях реализации вышеуказанных требований все уголовные дела, поступившие в суд, после их регистрации распределяются посредством Государственной автоматизированной системы «Правосудие» «Модуль распределения дел».

Например, на официальном сайте Заднепровского районного суда города Смоленска в разделе «Организация деятельности, документы суда» размещен Регламент автоматизированного распределения дел в Заднепровском районном суде г. Смоленска, пункт 6.2 которого предусматривает, что в случае невозможности рассмотрения дела (материала) переданного судье (при наличии конфликта интересов, нарушении установленной специализации либо иным основаниям, предусмотренным ст. ст. 61, 62, 63 УПК РФ) судья по делам (материалам) с сокращенными сроками рассмотрения незамедлительно (в остальных случаях – не позднее следующего дня) дело (материал) со служебной запиской передает председателю либо лицу, исполняющему обязанности председателя суда, в целях решения вопроса о его перераспределении, после чего дело (материал) передается в соответствующий отдел для дальнейшего перераспределения в автоматизированном режиме [7].

Таким образом, при поступлении уголовного дела (материала) судье более не требуется в порядке ст. 65 УПК РФ выходить в судебное заседание для рассмотрения заявления о самоотводе. Судья обязан во исполнение требований ч. 1 ст. 62 УПК РФ устраниться от принятия уголовного дела к производству путем подачи мотивированной служебной записки руководителю суда. После чего уголовное дело подлежит перераспределению в автоматизированном режиме с указанием в комментарии информации о причине и авторе распоряжения о перераспределении дела с последующей передачей дела в порядке, установленном Регламентом.

Ситуация отказа в удовлетворении просьбы о перераспределении дела (материала) Регламентом не предусмотрена. По нашему глубокому убеждению, отказ руководителя суда в удовлетворении просьбы судьи о перераспределении дела (материала) недопустим, поскольку фактически приведет к оказанию давления на судью по рассмотрению конкретного уголовного дела вопреки независимости и субъективной беспристрастности судьи при осуществлении правосудия.

Процедура самоотвода судьи, предусмотренная Регламентом, не противоречит действующему уголовно-процессуальному законодательству, в частности ч. 1 ст. 62 УПК РФ, а, напротив, способствует оптимизации и ускорению уголовного судопроизводства. Предусмотренный ст. 65 УПК РФ порядок рассмотрения заявления о самоотводе применяется лишь в ситуации, когда о возникновении оснований для отвода судье становится известно после принятия уголовного дела к производству (например, непосредственно в ходе самого судебного заседания).

2. Согласно ч. 1 ст. 259 УПК РФ в судах первой и апелляционной инстанций осуществляется аудиопротоколирование судебного заседания, за исключением случаев закрытого судебного разбирательства, предусмотренных ч. 2 ст. 241 УПК РФ.

Тем самым аудиопротокол стал обязательным наряду с традиционным протоколом в письменной форме.

По мнению Е. С. Милициной, «очевидно, что целью аудиопротоколирования является повышение точности фиксации хода судебного заседания и снижение количества возможных ошибок, допускаемых при сжатом письменном изложении в интерпретации работника аппарата суда, ведущего письменный протокол. Можно также заметить, что ведение аудиопротокола дисциплинирует всех участников судопроизводства (в том числе и сам суд) как в части неукоснительного соблюдения процессуальных норм, так и в части недопущения некорректных высказываний и поведения» [3].

Одновременно с этим введение аудиопротоколирования привело к тому, что рабочая нагрузка на сотрудников аппарата суда выросла, поскольку перед ними встала задача по составлению фактически стенограмм судебного заседания. При наличии аудиозаписи секретарь судебного заседания либо помощник судьи не освобождены от подробного изложения в протоколе показаний; вопросов и ответов; обстоятельств, подлежащих занесению в протокол по просьбе участников процесса; основного содержания выступлений в прениях и последнего слова подсудимого (пункты 10, 11, 13, 14 ч. 3 ст. 259 УПК РФ).

На IX Всероссийском съезде судей отмечалось, что «сменяемость кадрового состава в крупных регионах России составляет от 150 до 400 % в год» [6].

Полагаем, что при наличии аудиозаписи судебного заседания ведение по сути стенограмм судебного заседания излишне, в этом случае протокол в письменной форме должен являться лишь дополнительным средством фиксации данных:

– о месте и дате заседания, времени его начала и окончания;

– о том, какое дело рассматривается;

– о наименовании и составе суда, о помощнике судьи, секретаре, переводчике, обвинителе, защитнике, а также о потерпевшем, гражданском истце, гражданском ответчике, их представителях и других вызванных в суд лицах;

– о личности подсудимого и об избранной в отношении его мере пресечения;

– о разъяснении участникам уголовного судопроизводства их прав, обязанностей и ответственности;

– о ходатайствах и заявлениях, сделанных участвующими в деле лицами в устной форме;

– об определениях, вынесенных судом без удаления из зала судебного заседания;

– о мерах воздействия, принятых в отношении лица, нарушившего порядок в судебном заседании;

– о применении технических средств, трансляции судебного заседания по радио, телевидению или в информационно-телекоммуникационной сети «Интернет»;

– о дате изготовления и подписания протокола.

Опрос работников аппарата суда указывает на то, что выдвигаемое нами предложение будет способствовать оптимизации деятельности суда, поскольку снизит нагрузку на секретаря, помощника судьи, ускорит процесс составления протокола, а также позволит сторонам без «затяжки во времени» ознакомиться с протоколом и аудиозаписью в порядке, который предусмотрен ч. 7 ст. 259 УПК РФ.

Предлагаемая инициатива не приведет к нарушению прав и свобод участников уголовного процесса, поскольку они всегда могут ознакомиться с аудиозаписью, с помощью которой обеспечивается объективная и полная фиксация судебного разбирательства.

Анализируя вопрос аудипротоколирования судебного заседания, нельзя оставить без внимания проблемные аспекты ознакомления с аудиозаписью лиц, которые содержатся под стражей.

Например, приказом председателя Заднепровского районного суда г. Смоленска № 3-осн от 09.01.2020 утвержден порядок [5], пункт 2.2 которого регламентирует, что в течение трех суток с момента поступления соответствующего ходатайства должно быть обеспечено ознакомление с аудиозаписью. Для лиц, находящихся под стражей, с учетом направления требования в конвой для доставки подсудимого (осужденного).

Пункт 2.3 вышеуказанного Порядка предусматривает, что для лиц, находящихся под стражей, ознакомление с аудиозаписью судебного заседания производится в зале судебного заседания № 2 и № 3, либо в ином помещении, которое соответствует нахождению в нем содержащихся под стражей лиц.

Однако не во всех регионах Российской Федерации порядок ознакомления с аудиозаписью определен одинаково. Так, в Республике Мордовия Верховным судом и УФСИН совместно было принято решение об оборудовании СИЗО № 1 в г. Саранске специальным помещением для ознакомления с аудиозаписями, копия которых на оптическом диске доставляется в СИЗО. Подсудимые и осужденные имеют техническую возможность в любой день на месте знакомиться с аудиопротоколами [1. С. 35].

3. В целях соблюдения открытости и гласности уголовного судопроизводства в соответствии с Положением о порядке размещения текстов судебных актов на официальных сайтах Верховного Суда Российской Федерации, судов общей юрисдикции и арбитражных судов в информационно-телекоммуникационной сети «Интернет», утвержденным Постановлением Президиума Верховного Суда РФ от 27.09.2017 (по тексту – Положение), судебные акты подлежат опубликованию на интернет-сайтах судов [4].

В силу п. 2.3 вышеуказанного Положения не подлежат публикации акты, которые приняты судом, в частности, по делам, затрагивающим безопасность государства; возникающим из семейно-правовых отношений, делам, касающимся несовершеннолетних; о преступлениях против половой неприкосновенности и половой свободы личности [4].

Данные, которые указаны в пункте 3.2 Положения, не исключаются из текстов подлежащих публикации судебных актов. Вместе с тем, в силу п. 3.3 указанного Положения в целях соблюдения безопасности участников судебного процесса подлежат исключению персональные данные. Вместо них используются инициалы, псевдонимы и другие обозначения, не позволяющие идентифицировать участников судебного разбирательства. Также подлежат исключению положения, составляющие охраняемую законом тайну [4].

Однако мониторинг публикуемых судебных актов (приговоров, постановлений о прекращении уголовного дела, апелляционных постановлений) свидетельствует об их избыточной деперсонификации, когда из судебного акта зачастую удаляется юридически значимая информация, что приводит к непониманию смысла текста, неинформативности опубликованного судебного акта и, как следствие, искажению принципов открытости и гласности судопроизводства.

Заключение. Резюмируя вышесказанное, констатируем, что на сегодняшний день сложилась ситуация, при которой все большее использование информационных технологий в судопроизводстве влечет возложение дополнительной нагрузки на аппарат суда.

В целях упрощения рабочего процесса, его оптимизации следует:

– при наличии оснований для самоотвода судья обязан во исполнение требований ч. 1 ст. 62 УПК РФ устраниться от принятия уголовного дела к производству путем подачи мотивированной служебной записки руководителю суда. После чего дело подлежит перераспределению в автоматизированном режиме;

– при наличии аудиозаписи судебного заседания протокол, оформляемый в письменной форме, должен стать лишь дополнительным средством фиксирования без обязательного подробного изложения показаний; выступлений в прениях и последнего слова подсудимого;

– при деперсонификации судебных актов, подлежащих публикации на интернет-сайтах судов общей юрисдикции, не должна удаляться юридически значимая информация, за исключением персональных данных и положений, составляющих охраняемую законом тайну.

Список литературы

1. Кияйкин В. М. Без передовой инфраструктуры сложно реализовать общественный запрос на эффективное онлайн-правосудие // Судья. 2022. № 10. С. 34–37.

2. Концепция информатизации Верховного Суда Российской Федерации, утв. приказом Председателя Верховного Суда РФ от 15.02.2021 № 9-П // СПС «КонсультантПлюс». URL: https://clck.ru/36osRY

3. Милицина Е. С. Соотношение протокола и аудиопротокола в гражданском процессе // Мировой судья. 2022. № 9 // СПС «КонсультантПлюс». URL: https://clck.ru/36osQ9

4. Положение о порядке размещения текстов судебных актов на официальных сайтах Верховного Суда Российской Федерации, судов общей юрисдикции и арбитражных судов в информационно-телекоммуникационной сети «Интернет», утвержденное Постановлением Президиума Верховного Суда РФ от 27.09.2017 // СПС «КонсультантПлюс». URL: https://clck.ru/36osN6

5. Порядок ознакомления с аудиозаписью судебного заседания, изготовления и выдачи копии аудиозаписи в Заднепровском районном суде г. Смоленска, утвержденный приказом председателя Заднепровского районного суда г. Смоленска № 3-осн от 09.01.2020. URL: http://zadnepr.sml.sudrf.ru/modules.php?name=docum_sud&rid=19

6. Постановление IX Всероссийского съезда судей от 08.12.2016 № 1. URL: http://www.ssrf.ru/siezd-sudiei/22596

7. Регламент использования ПС ГАС «Правосудие» «Модуль распределения дел» в Заднепровском районном суде, утвержденный приказом председателя Заднепровского районного суда г. Смоленска № 14-осн от 20.06.2022. URL: http://zadnepr.sml.sudrf.ru/modules.php?name=docum_sud&rid=19

8. Указ Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // СПС «КонсультантПлюс». URL: https://clck.ru/36osML

Ю. Н. Кулешов,
директор,
Казанский институт (филиал)
Всероссийского государственного университета юстиции
(РПА Минюста России)

ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ СТРОИТЕЛЬСТВА И МЕТОДЫ ИХ ПРЕДУПРЕЖДЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. В статье проводится анализ наиболее частых преступлений, совершающихся в сфере строительства. Предложены рекомендации по предупреждению совершения подобных преступлений с учетом использования цифровых технологий при их расследовании.

Ключевые слова: цифровые технологии, строительство, экономические преступления, методы расследования

TYPES OF CRIMES IN THE FIELD OF CONSTRUCTION AND METHODS FOR THEIR PREVENTION IN THE CONTEXT OF DIGITALIZATION

Abstract. In the article, the author analyzes what crimes are most often committed in the construction industry. The author identifies both economic crimes and analyzes the forms of organized crime in this area. The author offers some recommendations for preventing the commission of such crimes, as well as the use of digital technologies in their investigation.

Keywords: digital technologies, construction, economic crimes, investigative methods

Строительная отрасль очень подвержена преступности. Такие факторы, как постоянная текучесть кадров, мобильность рабочей силы и временный характер проектных работ сделали строительную отрасль легкой мишенью для мелких преступников и серьезной организованной преступности. Преступность в этой отрасли разнообразна и часто зависит от местоположения проекта. В ходе статистических опросов установлено, что строительные площадки, как правило, чаще подвергаются нападениям те, которые расположены в густонаселенных районах городов, где происходит множество криминальных деяний – от воровства до охранного рэкета. Характер строительной рабочей силы также является важным фактором обеспечения безопасности, что необходимо учитывать при расследовании преступлений в данной индустрии.

Исследование указывает на то, что часто возникают конфликты с субподрядным персоналом и что именно эти временные элементы рабочей силы часто участвуют в кражах на месте. Результаты показывают, что непосредственно нанятые сотрудники менее склонны к совершению преступных деяний.

Строительная отрасль несет убытки из-за вандализма и краж, хотя трудно получить точную цифру ущерба, так как многие из таких преступлений остаются незамеченными. Кража представляет собой особую проблему для данной отрасли; замена дорогостоящего оборудования на дешевое и менее качественное может

привести к тому, что строительный проект в будущем потребует существенных и непредвиденных затрат. В нынешней экономической ситуации органы следствия предупреждают строительные компании об обеспечении защиты своего оборудования. Также в ходе следствия используется технология идентификации, связанная с базой данных, которая поможет отслеживать строительные установки и оборудование. Соблюдение таких мер предосторожности значительно снизит риск кражи на месте и увеличит шансы на возвращение украденного оборудования.

Соблюдение требований охраны труда и техники безопасности должно быть приоритетом в строительной отрасли, в которой часто имеют место несчастные случаи, произошедшие в результате пренебрежения. Отрасль должна больше соблюдать правила охраны труда и техники безопасности, оценивать риски до начала работ и обеспечивать предупреждение несчастных случаев. Это поможет снизить количество инцидентов и свести к минимуму штрафы и возможные тюремные сроки.

Случаи организованной преступности в строительной отрасли, судя по всему, достаточно редки. Преступные организации в некоторых государствах часто выполняли функции охранных предприятий, вывоза мусора и компаний, обеспечивающих дешевый труд. Оплата услуг, предлагаемых этими организациями, способствует серьезному преступлению. Обычно такие организации навязывают свои услуги на строительных площадках, у которых нет другого выбора, кроме как принять предлагаемое обеспечение.

Для предупреждения преступлений в сфере строительства, необходимо учитывать следующие моменты:

– во-первых, менеджеры подобных объектов и проектов должны знать, как бороться с подобной преступностью. Обучение должно включать основные вопросы предупреждения таких преступлений, они должны знать, как лучше бороться с происходящей преступностью.

– во-вторых, ИТ-системы должны использоваться для контроля доступа к строительным объектам и реестрам строительного оборудования. Должна быть создана ИТ-система, которая будет поддерживать актуальную информацию базы данных сотрудников. Использование электронных входных систем подключение к базе данных предотвратит незаконный доступ. Реестры электронного оборудования также полезны для ведения записей о том, кто и когда последний раз пользовался оборудованием; это позволит отслеживать оборудование в случае его пропажи.

– в-третьих, обо всех преступлениях следует сообщать. Налицо явное занижение преступности в строительстве. Хотя данные свидетельствуют о том, что многие считают, что сообщение о преступлении не будет иметь успешного результата, это не поможет предотвратить его повторение.

Возможность использования цифровых анонимных технологий об оповещении о преступном деянии в строительной сфере поможет своевременно раскрыть такое преступление и предотвратить совершение новых преступлений.

Цифровые технологии должны более активно использоваться именно при непосредственном расследовании преступлений в сфере строительства, как в круп-

ных населенных пунктах, так и при строительстве небольших объектов в менее населенных областях.

Список литературы

1. Кулешов Ю. Н. Методика расследования экономических преступлений в сфере строительства. М.: Юрлитинформ, 2022. 184 с.
2. Кустов А. М. Механизм преступления: теория и практика: монография. М.: Академия управления МВД России, 2001. 213 с.
3. Сараев П. Н. Экономические преступления в сфере строительства: методологические основы расследования // Российский следователь. 2012. № 15.

О. Н. Куликова,
кандидат юридических наук, доцент,
Саратовская государственная юридическая академия
(Смоленский филиал)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УГОЛОВНО-ИСПОЛНИТЕЛЬНЫХ ПРАВООТНОШЕНИЯХ

Аннотация. Целью исследования выступает определение роли цифровых технологий в современных правоотношениях государства и лица, отбывающего наказание. Определяется сложность обеспечения отдельных уголовно-исполнительных отношений, где ключевым ядром выступает человек, который без помощи государственных органов не способен реализовать отдельные виды прав в период изоляции от общества.

Ключевые слова: права осужденных, цифровые технологии, лишение свободы, уголовно-исполнительные правоотношения

DIGITAL TECHNOLOGIES IN CRIMINAL AND EXECUTIVE LEGAL RELATIONS

Abstract. The purpose of the study is to determine the role of digital technologies in modern legal relations between the state and a person serving a sentence. A feature of the material is its presentation through the prism of the realization of the rights of convicted citizens serving a sentence of imprisonment. The author defines the complexity of ensuring individual penal relations, where the key core is a person who, without the help of state bodies, is not able to realize certain types of rights during the period of isolation from society.

Keywords: the rights of convicts, digital technologies, deprivation of liberty, criminal and executive legal relations

Уголовно-исполнительные правоотношения возникают в связи с назначением виновному в преступлении лицу меры уголовно-правового характера, отраженной в обвинительном приговоре суда. Назначаемая мера выступает гарантией

и правовым критерием реализации принципов законности и справедливости, положенных в основу отечественного уголовного законодательства. В свою очередь, Уголовно-исполнительный кодекс Российской Федерации регулирует общественные отношения, возникающие по поводу отбывания назначенного наказания, применения условного осуждения, а также осуществления контроля за освобожденными из мест изоляции гражданами. Тем самым уголовно-исполнительные отношения реализуются силой государства и обеспечиваются органами принудительного исполнения в соответствии с действующим в России законодательством.

Субъектами таких правоотношений выступает, с одной стороны, государство в лице компетентных правоохранительных органов, основной функцией которых выступает обеспечение исполнения приговора суда, а, с другой – таким участником становится лицо, которое по приговору суда обязано претерпеть воздействие в связи с противоправным поведением.

Период отбывания уголовного наказания обусловлен рядом предусмотренных для осужденных лиц ограничений, которые в большей их мере распространяются на места лишения свободы. Пределы применяемых ограничений прав и свобод граждан определяется не сроком отбывания назначенного наказания, а видом определенного судом вида исправительного учреждения. При этом его вид зависит от степени и характера общественной опасности совершенного преступления и является ядром принудительного воздействия со стороны суда. Отбывая наказание в виде лишения свободы, лицо имеет ряд правоограничений, таких как свобода передвижения, выбор места нахождения, установление социальных связей по собственному выбору человека и пр. Особенно эти права еще более сузились в период распространения с декабря 2019 по апрель 2023 г. массового заболевания острым респираторным заболеванием – коронавирусной инфекции (2019-nCoV).

Изучая материалы правоприменительного значения, остановимся на рассмотрении социально-правовых аспектов реализации осужденными, находящимися в изоляции от общества, их права на образование, социальную адаптацию, связь с внешним миром посредством актуальных к применению цифровых способов коммуникации.

Цифровые технологии, в отличие от информационных, представлены не только программным обеспечением, но и технологией цифровой обработки информации, используемой для деловых операций. Из этого следует, что реализовать их в условиях изоляции от общества без доступа к таким технологиям, осужденному невозможно. В свою очередь, информационные методы использования компьютера в связи с обработкой и хранением информации выступают законно запрещенными на период лишения гражданина свободы. Это обусловлено назначением области IT – использование не в развлекательных или личных целях, а для проведения деловых операций.

Цифровые технологии современной уголовно-исполнительной системы, необходимые для цифровой обработки информации, представлены аудиовизуальными, электронными и иными техническими средствами надзора и контроля. Об этом прямо гласит ст. 83 Уголовно-исполнительного кодекса России, определяя целью

их применения в местах лишения свободы предупреждение общественно опасных действий – побега, нарушения режимных требований, нападения на сотрудников учреждения или других осужденных, а также в случае иных преступных деяний. Технические средства могут использоваться и для получения информации в отношении поведения осужденных. Об их применении администрация учреждения уведомляет гражданина под роспись (ч. 2 ст. 83 УИК РФ).

Образовательный процесс в местах лишения свободы представляется комплексным обучением лиц, отбывающих определенный срок в исправительных учреждениях, по месту фактического пребывания. Для этого администрацией учреждения организуется соответствующая материально-техническая база с комплексом строений, помещений, включая компьютерные классы, предназначенных для учебного процесса. Согласно действующему уголовно-исполнительному законодательству в образовательной деятельности, проводимой учителями с осужденными, использование ресурсов, способных осуществлять свободное общение с внешним миром, запрещено. В этом контексте мы говорим и о «выходе» в коммуникационную сеть «Интернет». Такая ситуация распространяется на все виды образовательной деятельности, включая уроки информатики. В этой связи правоограничения свободного пользования технологиями беспроводной связи обусловлены фактом изоляции от общества по решению суда.

Социальная адаптация осужденных представляет собой процесс подготовки лиц к последующему возвращению к жизни из мест лишения свободы. Социальной адаптации осужденных к лишению свободы способствует общественно полезный труд, получение общего образования, высшего образования, профессиональное обучение, общественное воздействие, а также поддержание связи с внешним миром [2. С. 77]. Социальная связь реализуется путем предоставления свиданий осужденного и его родственников, супругов, получение посылок, передач, телефонных разговоров, переписки стандартного формата, передвижение без конвоя для бытовых и трудовых нужд за пределами колонии. Такая связь выступает актуальным направлением при проведении ежегодно исправительным учреждением дней открытых дверей, которые вправе посетить родственники, представители общественности и средств массовой информации. Мероприятия имеют высокую социально-человеческую ценность в виду обогащения личности за счет получения новой информации семейно-родственного, культурного, правового, политического, социального и иного характера.

Социальная связь поддерживается при реализации права осужденного на вероисповедание путем общения со священнослужителем, участием в религиозных обрядах (крещение, исповедь, молитва), изучения соответствующей литературы. Литература может быть выполнена на бумажном носителе, представлена иллюстрацией и иметь иную материальную оболочку.

Общение с родственниками, священнослужителями, педагогами школы колонии, общественниками, сотрудниками средств массовой информации происходит путем прямого визуального общения, общение при помощи IT осужденным запрещено. Исключение из правил составляет видео свидание с родственниками (при невозможности их личного приезда в учреждение) и участие в следственных действиях в соответствии с законом. Так, положения ст. 241.1 Уголовно-процессуального

кодекса устанавливают, что при наличии технической возможности суд вправе по ходатайству подсудимого принять решение о его участии в судебном заседании путем использования систем видеоконференцсвязи [1]. Общение осуществляется посредством терминалов, один из которых установлен в исправительном учреждении, другой – в публичном месте [3].

Также с 2018 г. действует удобный сервис ФСИН-письмо, благодаря которому по Интернету отправляются электронные письма [4]. Пандемия, обусловленная 2019-nCoV, также внесла цифровую корректировку в деятельность суда. Как отмечает одна из контентных платформ: «Если раньше к использованию систем видеоконференцсвязи (ВКС) прибегали, в основном, для обеспечения участия в судах подследственных, находящихся в СИЗО, сегодня практически повсеместно можно организовать таким образом и опрос свидетелей, и работу защиты, и многие другие процессуальные действия» [5].

В условиях распространения 2019-nCoV, осужденные были ограничены в получении свиданий с близкими лицами (родственниками, супругами), в подготовке и участии в дне открытых дверей исправительного учреждения, посещении колонии священнослужителями, общественными наблюдательными комиссиями, родительскими комитетами и попечительскими советами. И при этом альтернативной заменой указанным правам видеоконференцсвязь не выступила в виду невозможности ее такого количественного использования.

В указанный период до фактически весны 2023 г. снизилось количество прокурорских надзоров исправительных колоний и иных мест принудительного содержания граждан, что естественным образом повлияло на реализацию прав граждан, предоставляемых уголовно-исполнительным законодательством.

При реализации права осужденных, отбывающих в местах лишения свободы, на обращение с жалобами в соответствующие инстанции, если исчерпаны средства правовой защиты в самом исправительном учреждении, при направлении заявлений, жалоб путем использования почтовой связи или при направлении электронного письма, с них взимается плата. Электронный формат обращения подлежит предварительному изучению и сканированию текста, который проверяется в целях интересов правосудия, обеспечения прав и законных интересов граждан в Российской Федерации.

Вопросы цифровизации в местах лишения свободы, остается открытым и достаточно актуальным. Это связано с тем, что осужденные, которым, например, ограничен доступ к консультации у врача-психиатра, психолога или сексолога, ограничены в социализации и поддержании в период отбывания срока лишения свободы социальных связей.

В целях успешной социализации при помощи цифровых технологий осужденные могли бы умственно развиваться путем участия в мониторингах, опросах общественного мнения на социальные темы, переписи населения.

Естественным образом мы говорим о законном правоотношении лица, отбывающего наказание, по реализации права доступа к цифровым технологиям, которые должны контролироваться и обеспечиваться администрацией учреждения. Сложность реализации такого права обусловлена недостаточным финансированием и материально-техническим обеспечением колоний, а также сложностью обладания кадрового персонала знаниями соответствующей IT-квалификации.

Следует отметить, что ряд цифровых технологий, является сложно доступным благом к приобретению и использованию уголовно-исполнительной системой в настоящее время. Например, об установлении новых производственных технологий, компонентов сенсорики, виртуальной реальности, искусственного интеллекта и иных технологий, для упрощения реализации ряда прав осужденных в местах изоляции от общества, в настоящих условиях говорить не приходится. Введение возможного использования отдельных видов технологий положительно влияет на воспитательно-культурную социализацию личности, облегчая работу сотрудников исправительного учреждения.

Цифровые технологии относятся к возможностям государства, выступающего в уголовно-исполнительных отношениях ключевым фигурантом, обеспечивающим права другого их участника – человека, осужденного за преступление, обязанного претерпеть меры государственного воздействия. Таким образом, развивая данные технологии в обществе, необходимо внедрять их и в места принудительного содержания граждан, путем кадрового обеспечения и материально-технического оснащения.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481

2. Борсученко С. А. Ресоциализация и социальная адаптация осужденных к лишению свободы: понятие, содержание, правовое регулирование // Научный журнал КубГАУ. 2017. № 126 (02). С. 386–402.

3. Процедура проведения видеосвидания ФСИН с заключенными. URL: http://ugolovnyi-expert.com/videosvidanie-fsin-rf

4. Способы связи с заключенными: письма и свидания. URL: https://fsin-pismo.com/svyaz-s-zaklyuchennymi

5. Судебное заседание по видеосвязи (ВКС. как такое возможно. URL: https://dzen.ru/a/YZvh3ju9sWm6sMn2

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Э. М. Гильманов,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ РЕСУРСОВ ПРИ ОХРАНЕ АРХИТЕКТУРНЫХ ПАМЯТНИКОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Архитектурные памятники Российской Федерации величественны и прекрасны, однако далеко не все они находятся в достойном состоянии, регулярно подвергаются реконструкции, в достаточной степени защищены от действий вандалов или «черных копателей». Особенно это характерно для памятников

архитектурного наследия, расположенных в российской глубинке. В то же время нельзя считать, что охрана архитектурных памятников должна осуществляться любыми средствами. В ряде случаев охранительными действия являются лишь внешне, а реально интерес направлен на иные блага. В статье анализируются возможности использования цифровых ресурсов при охране памятников культурного наследия Российской Федерации, а также определены, могут ли такие ресурсы посягать на общественную и государственную безопасность Российской Федерации.

Ключевые слова: цифровые ресурсы, архитектурные памятники, культурное наследие, памятники истории и культуры, уголовная ответственность за шпионаж

THE USE OF DIGITAL RESOURCES IN THE PROTECTION OF ARCHITECTURAL MONUMENTS OF THE RUSSIAN FEDERATION

Abstract. The architectural monuments of the Russian Federation are majestic and beautiful. However, not all of them are in decent condition, regularly undergo reconstruction, are sufficiently protected from the actions of vandals or «black diggers». This is especially true for architectural heritage monuments located in the Russian hinterland. At the same time, it cannot be assumed that the protection of architectural monuments should be carried out by any means. In some cases, protective actions are only externally, but in reality the interest is directed to other benefits. In this article, we will analyze the possibilities of using digital resources in the protection of cultural heritage monuments of the Russian Federation, and also determine whether such resources can encroach on the public and state security of the Russian Federation.

Keywords: digital resources, architectural monuments, cultural heritage, historical and cultural monuments, criminal

Введение. Охрана памятников культуры Российской Федерации, в том числе архитектурных, является одной из ключевых позиций применительно к сохранению культурного наследия России. В последнее время очень актуальным направлением становится популяризация различных объектов культурного наследия через различные социальные сети, страницы и сайты как отдельных зданий, так и ценных архитектурных комплексов. Одной из идей создания такого рода информационных источников является попытка сохранения их внешнего облика хотя бы на фотоснимках и электронных (цифровых) изображениях. Полагаем, что такая идея заслуживает поддержки, так как позволяет ознакомиться с памятниками архитектуры не только непосредственно туристов, но и лиц, которым по тем или иным причинам недоступно посещение данных археологических жемчужин, например, лиц с инвалидностью [1] или проблемами с опорно-двигательным аппаратом.

Однако приходится констатировать, что в некоторых случаях возникают злоупотребления при размещении информации об архитектурных и иных памятниках в сети Интернет, что может повлечь уголовную ответственность. При этом некоторые преступления уже имеют закрепление в нормах Уголовного кодекса РФ [2], а иные нуждаются в осмыслении их как потенциально общественно опасных деяниях.

Основная часть. Начиная с 2010 г. ежегодно на сайте Wikipedia[1] проводится Международный фотоконкурс Wiki Loves Monuments (пер. с англ. – «Вики любит памятники» [3]. Первостепенной задачей проведения данного мероприятия ставится «привлечение внимания к архитектурному наследию участвующих стран» [3]. Первый конкурс проведен еще в 2010 г., а впоследствии был поставлен мировой рекорд (согласно Книге рекордов Гиннеса) как фотоконкурса с самым большим количеством участников [4]. Сейчас в данном конкурсе принимают участие фотографы из 35 стран. Участие в конкурсе бесплатное.

Участвующая страна должна представить список памятников (с их адресами и идентификаторами), участники конкурс загружают фото с первого по 30 сентября. Фото загружаются в Викисклад (соответственно, фотографии присваивается учетная запись). Фото может быть сделано в любое время, однако выгружено должно быть именно в сентябре под свободной лицензией CC-BY-SA 3/0 (или иной, совместимой: например, CC-BY или CC-0). Публикация безотзывная.

Особенностью конкурса является тот факт, что выложенные фотографии обязательно должны иметь официальный идентификатор и указание на географические координаты места съемки объект (памятника архитектуры) с указанием долготы и широты. При этом участник конкурса может и не знать о том, что предоставляет эту информацию, нужная информация добавляется в процессе загрузки фотографий через сайт конкурса либо при использовании мобильного приложения. Полагаем, что в некоторых случаях возможно пересечение данной информации с содержанием частной тайны или неприкосновенностью частной жизни (в плане неразглашения информации о месте нахождения конкретного человека) [5]. Списки с предоставленными данными уточняются в течение года или на протяжении конкурса.

Заметим, что ряд стран считают, что проведение данного конкурса незаконно, соответственно, незаконным является и опубликование конкурсных листов. Однако в России сайт с конкурсными листами создан и поддерживается веб-дизайнерами компании «Теплица социальных технологий», финансовую поддержку которой оказывает «Ростелеком».

Идейная составляющая конкурса «Вики_любит_памятники» акцентирует внимание на вкладе каждого участника в сохранение культурного наследия России [6]. Также транслируется желательность пополнения электронной базы объектов российского культурного наследия, включая памятники истории, архитектуры, археологии монументального искусства. Результатом, по задумке организаторов, должно стать иллюстрирование статей и путеводителей Википедии. Также констатируется, что тем самым создается негосударственный реестр памятников истории, архитектуры, археологии монументального искусства, созданный силами волонтеров и независящий от государства, при этом существенно превосходящий реестры государства как по количеству, так и по качеству.

При этом никаких требований о сообщении персональной информации нет. Вместо них могут быть ник или псевдоним, которые могут быть указаны в дипломе

[1] Примечание: Роскомнадзор обозначил Википедию как «ресурс, распространяющий недостоверную информацию».

участника. Идентификация авторства также не требуется. Соответственно, узнать автора могут только организаторы (либо вообще не интересоваться данной информацией, так как интерес могут представлять не индивидуальные данные фотографа, а само содержание фотографии).

Выделены две ключевые темы – идеи: «Культурное наследие под угрозой» и «Усадьбы Северо-Запада». Именно последняя тема нас особенно заинтересовала.

В условиях проводимой специальной военной операции передача иностранным заинтересованным лицам географических данных с координатами объектов истории, архитектуры, археологии монументального искусства может способствовать тому, что данные объекты могут стать целями для нападений извне (с помощью дронов или иных средств), что может привести к утрате данного объекта культурного наследия [7, 8].

При этом организаторы фотоконкурса предлагают выкладывать в Интернет фото с максимально возможным разрешением (не менее 2 МП, фотографии с меньшим разрешением жюри оставляет за собой право не рассматривать), полагаем, что в этом случае параллельно может решаться и иная задача, разведывательная. На представленных фотографиях может быть случайно размещен секретный объект (напомним, что интересуют усадьбы Северо-Запада, по сути, это линия соприкосновения с Прибалтийскими странами и Финляндией). Также очень спорной выглядит рекомендация выкладывать фото, полученные с дронов, хотя полеты данных аппаратов над определенными территориями может быть запрещен. Однако организаторы прямо указывают, что они не несут никакой ответственности за действия участников данного конкурса, как гражданско-правовую в случае нарушения авторских прав или ненадлежащее исполнение обязательств, и могут изменять правила в ходе проведения конкурса. Применительно к авторским правам интересна оговорка в Правилах: авторские права на изображение включают права автора фотографии и права архитектора или скульптора того объекта, изображение которого снимает фотографирующий. При этом с самой съемкой все ясно – это плод труда фотографа, а вот авторские права на объект съемки могут быть нарушены. Однако организаторы, прямо указывая на данное обстоятельство, все равно призывают проводить съемки, указывая, что «изображения скульптур и других подобных объектов нам тоже нужны, призываем вас их фотографировать» [9], по сути, предлагая нарушить законодательство об авторском праве, за что в российском законодательстве предусматривается ответственность, вплоть до уголовной в рамках ст. 146 УК РФ. В то же время запрещается указывать на фотографии дату съемки, размещать водяные знаки или иные подписи, которые могут быть использованы для идентификации автора, так как прямо презюмируется, что предоставленные изображения будут использоваться в качестве иллюстраций для различных проектов Фонда Википедиа.

Более того, в Правилах проведения рассматриваемого конкурса прямо указано, что организаторам известно о наличии зон боевых действий, а равно о наличии стратегических объектов на данных территориях, и организаторы не рекомендуют проводить фотосъемку данных объектов, так как это небезопасно, но не исключают возможности получения фотографий из таких регионов и загрузку их на сайт конкурса (хотя и предлагается выкладывать старые фотографии). То же самое касается фотографий с воздуха, сделанных при помощи квадрокоптеров [3], либо

фотографий стратегических объектов из других регионов. Полагаем, что фактически здесь присутствует неким образом легализованный шпионаж на территории Российской Федерации.

Выводы и предложения. В ходе проведенного исследования мы пришли к выводу о том, что отдельные положения фотоконкурса «Вики любит памятники 2023» может посягать на объекты культурного и архитектурного наследия России путем тиражирования изображений данных объектов без учета мнения авторов (архитекторов, скульпторов), с одной стороны, и иметь потенциальную опасность в связи с наличием реальной опасности повреждения или уничтожения памятников истории и культуры России путем сообщения иностранным гражданам и заинтересованным иностранным организациям точных географических координат фотографируемых объектов культурного наследия – с другой. В ситуации, когда на передаваемом на конкурс изображении присутствуют, пусть и случайно, объекты военной или иной инфраструктуры, обеспечивающей национальную безопасность, действия могут подпадать под состав посягательства на общественную или государственную безопасность. Полагаем, что органы прокуратуры или Федеральной службы безопасности РФ должны проверить организацию данного конкурса на предмет нарушения законодательства Российской Федерации.

Список литературы

1. Гильманов Э. М., Гильманов Р. Э. О мошенничестве в сфере охраны объектов культурного наследия // Образование, воспитание и право в контексте глобальных вызовов: сборник материалов Международной научно-практической конференции / Чувашский государственный университет имени И. Н. Ульянова. Чебоксары, 2023. С. 209–213.

2. Гильманов Э. М. Об уголовной ответственности за уничтожение либо повреждение воинских захоронений, обелисков, других мемориальных сооружений или объектов, увековечивающих память погибших при защите отечества или его интересов либо посвященных дням воинской славы России // Правовые и нравственные аспекты функционирования гражданского общества: сборник материалов Международной научно-практической конференции, посвященной памяти заслуженного деятеля науки Российской Федерации, доктора юридических наук, профессора В. П. Малкова. В 2-х частях. Чебоксары, 2020. С. 157–161.

3. URL: https://ru.wikipedia.org/wiki/Вики_любит_памятники

4. Guinness World Records, Largest photography competition // Архивная копия от 27 августа 2014 на Wayback Machine, 2012.

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

6. Фотоконкурс «Вики любит памятники 2023». URL: https://foto-konkursy.ru/viki-lyubit-pamyatniki

7. Гильманов Э. М. Некоторые вопросы уголовной ответственности за повреждение или уничтожение объектов культурного наследия // Oeconomia et Jus. 2019. № 1. С. 47–55.

8. Гильманов Э. М. Объекты мирового культурного наследия: вопросы их уничтожения или повреждения во время военных действий / В сборнике: Татищевские чтения: актуальные проблемы науки и практики. Материалы XV Международной научно-практической конференции. В 3-х томах. Тольятти, 2018. С. 197–202.
9. Wikivoyage: Вики_любит_памятники_2023. URL: https://ru.wikivoyage.org/wiki/Wikivoyage: Вики_любит_памятники_2023/Правила

Э. Ю. Латыпова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СРЕДСТВ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ОТНОШЕНИИ ДОМАШНИХ ЖИВОТНЫХ

Аннотация. Мошеннические и прочие преступные схемы, связанные с домашними животными, являются часто применяемыми, так как позволяют воздействовать на потенциальную жертву с разных сторон – воздействовать как на душеные качества (жалость, забота и т. п.), так и на экономические потребности (например, выгоду от приобретения породистого животного по низкой цене и т. п.). Научные исследования преступлений, совершаемых в отношении домашних животных, в основном сосредотачивается на двух направлениях – анализе жестокого обращения с животными, повлекшего их гибель или причинение вреда здоровью, либо анализе мошеннических схем [2], в которых домашние (и не только) животные выступают в качестве предмета. Однако в отношении домашних животных могут совершаться и иные преступления (кража, присвоение, контрабанда и т. п.). Активно в таких преступлениях используются различные цифровые средства. Отдельные преступления, совершаемые в отношении домашних животных, анализируются в данной статье.

Ключевые слова: цифровые средства, мошенничество, мошенничество в отношении домашних животных, жестокое обращение с животными, домашнее животное, обман, злоупотребление доверием

THE USE OF DIGITAL MEANS IN THE COMMISSION OF CRIMES COMMITTED AGAINST PETS

Abstract. Fraudulently and other criminal schemes related to pets are often used, as they allow you to influence a potential victim from different sides – to influence both the soulful qualities (pity, care, etc.) and economic needs (for example, the benefit of acquiring a thoroughbred animal at a low price, etc.). Scientific research of crimes committed against domestic animals mainly focuses on two areas – the analysis of cruelty to animals that caused their death or injury to health, or the analysis of fraudulent schemes [2] in which domestic (and not only) animals act as a subject. However, other crimes may be committed against pets (theft, embezzlement, smuggling, etc.). Various digital means are actively used in such crimes. Individual crimes committed against pets will be analyzed further.

Keywords: digital tools, fraud, fraud against pets, animal abuse, pet, deception, abuse of trust

Введение. Домашние животные давно сопровождают человека, выполняя самые разнообразные функции. Изначально одомашенное животное выполняло сугубо утилитарные потребности – являлось источником питания (коровы, лошади, овцы и прочие), являлось средством передвижения (лошадь, осел и прочие), охраняло от внешних опасностей (собака от посторонних людей, кошка, хорек – от грызунов и т. п.). Однако сейчас ярко выделилась группа сугубо домашних животных, которые особой утилитарной нагрузки не несут, выполняя больше функции компаньона (те же собаки и кошки, а также ежики, крысы, мыши и др.). И на этой потребности в заботе и уходе за живым существом активно развиваются разнообразные мошеннические схемы. О том, что животные являются быстрым и надежным средством зарабатывания денег, было известно с древнейших времен [6]. Использование цифровых технологий во многом позволяют облегчить процесс реализации животных путем их рекламы в социальных сетях с использованием Интернета, параллельно приводя и к росту различного рода преступных схем в их отношении.

Основная часть. Активное поступательное развитие цифровых технологий, проникновение социальных сетей во все сферы человеческой жизни приводит к тому, что продажа различных товаров, в том числе и животных, активно происходит через сеть Интернет.

Изучение научной литературы приводит к выводу, что обычно предполагается совершение мошеннических действий только во время оплаты покупки (со счета покупателя списываются деньги при оплате банковской картой, при этом животное реально к нему не поступает [5]; это возможно, если животное находится в другом городе и приобретается дистанционно), либо вместо заявленного животного могут привезти другое: так, покупатель на фото, размещенном в социальной сети, видит одного щенка или котенка, а привозят ему другого, менее породистого, или вообще фенотипичного (похожего внешне на представителя определенной породы, но таковой не являющегося или являющегося метисом / дворняжкой). Соответственно, проблема мошенничества, совершаемого в отношении домашних животных, является намного более широкой, чем только вопросы его оплаты при приобретении [2, 9].

Подробное исследование различных вариантов мошенничества в отношении домашних животных (на примере собак) проводилось нами ранее. Так, мы отмечали, что «на этапе приобретения щенка могут следующие варианты мошенничества: 1) щенок продается как имеющий документы, тогда как соответствующие документы, подтверждающие происхождение, отсутствуют; 2) родители щенка (или один из них) по документам не являются биологическими родителями; 3) щенок, который был выставлен на продажу в Интернете, и фото/видео которого размещалось в социальных сетях, заменяется на другого щенка той же породы; 4) щенок продается как имеющий выставочные или племенные перспективы, тогда как он не соответствует им по своему качеству (так называемый пэт-класс); 5) продавец дает гарантии, что щенок будет иметь заданные параметры (рост, вес, объем шерсти, количество зубов после смены и т. п.), тогда как гарантировать соблюдение этих параметров невозможно, возможно только предположение об их проявлении (иногда с высокой

долей вероятности); 6) предоставляется недостоверная информация о породных особенностях (порода гипоаллергенна; обучать щенка нет необходимости, порода умная; не нужно ухаживать за шерстью, хотя это не так и т. п.)» [2]. Итогом таких продаж часто является разочарование покупателя приобретением в дальнейшем, и либо передача (продажа) его далее, либо собака оказывается на улице, где шансы на выживание очень невелики, либо собаку могут усыпить, чтобы избавить такого горе-владельца от «страданий».

Сегодня в качестве решения проблемы «выкидывания» домашних животных на улицу достаточно часто предлагается их чипирование, при этом чип в цифровой форме может содержать не только данные о владельце и его адресе, но и иную необходимую информацию – данные о прививках, о перенесенных заболеваниях и т. п. Однако здесь уместно напомнить, что чипирование на территории Российской Федерации породистых собак проводится достаточно давно и является рутинной процедурой [7], однако широкого распространения так и не получило, что объясняется несколькими факторами – относительная дороговизна (сделать татуировку гораздо дешевле), и использование разных систем чипирования, когда сканер рассчитан только на конкретный тип чипа, и другой тип «не прочитает». Более того, на территории Москвы и Московской области чипирование планируют сделать обязательным для всех собак и кошек [8]. Также возможна «потеря» чипа, когда сканер не может обнаружить чип на собаке, либо его «подмена» (замена на другой чип с какой-либо целью).

Индивидуализация домашнего животного с помощью татуировки также активно применяется достаточно дано (более двадцати пяти лет), однако также имеет существенные недостатки:

1) татуировка делается в достаточно «юном» возрасте (обычно в возрасте одного-двух месяцев), и с ростом животного может «размыться», т. е. потерять четкие очертания (если она была нанесена в область паха);

2) недобросовестный владелец может «перебить» татуировку, поменяв буквы и цифры;

3) даже наличие татуировки не всегда дает возможность определить реального владельца – так, по правилам РКФ (Российская кинологическая федерация, объединяющая большинство владельцев породистых собак), в татуировке указывается шифр питомника / клуба (три буквы) и цифры порядкового номера щенка в помете (или номер из общего списка полученных щенков в данном клубе / питомнике).

Соответственно, есть общая база присвоенных номеров клеймения в электронном виде (обычно на сайте РКФ или породного клуба), однако не всегда можно узнать конкретного владельца, так как эти данные в электронную базу не вносятся. Если собака выставлялась, то при регистрации на выставку обязательно внесение номер клейма в электронную базу, однако если собака в выставках не участвовала, «найти» ее в электронной базе практически невозможно. Сами заводчики / владельцы клубов / питомников также не всегда знают, кому были переданы их подопечные, особенно в случае, если щенок в дальнейшем перепродавался.

Решением в данном случае, как один из возможных вариантов, может быть обязательность внесения в электронную базу не только номеров клеймения, но и данных о владельце проданных собак (сделать это можно, когда сдается общепометная

карточка), однако это утопично, так как часть щенков «засиживается», т. е. продается в возрасте четыре – шесть месяцев и далее, а часть перепродается, соответственно, данные о хозяине нужно будет менять. Если же брать собак без документов, то их вообще никто не клеймит, соответственно, и найти такую собаку по клейму не получится. Можно констатировать, что на текущий момент времени ведение электронной базы клейм больше на совести заводчика, и единой централизованной работы в данном направлении пока не проводится.

Применительно к проблемам противодействия мошенническим действиям в отношении домашних животных можно указать, что наличие клейма и его «читаемость» в определенной степени подтверждает, что животное с клеймом соответствует документам (родословной или выставочным титулам). При этом участие в выставках и зоотехнических мероприятиях, а также в спортивных соревнованиях с собаками возможно только после проверки клейма (или чипа – при его наличии).

Возвращаясь к анализу мошеннических действий, можно предположить, что и в выставочной деятельности мошенничество возможно:

1) выставляется вместо заявленного другое животное той же породы с целью получить «разводную» оценку;

2) животному водятся определенные медицинские препараты с целью его «успокоить», если животное агрессивно (агрессия в отношении судьи может повлечь дисквалификацию), или, наоборот, «развеселить», если животное излишне пассивно;

3) присутствует «договорняк», когда хендлер или владелец договариваются о необходимой оценке или титуле (это уже имеет признаки коррупционного правонарушения);

4) животному проводятся различного рода косметические или пластические операции, для коррекции имеющихся недостатков или пороков (например, неправильный постав ушей или хвоста), что также является мошенничеством (хотя и не влечет уголовную ответственность) и может повлечь деградацию породы, если такой «оттюнингованный» ее представитель будет в дальнейшем активно использоваться в разведении. Возможны и другие злоупотребления [2].

В то же время наличие у собаки клейм или чипа в определенной мере позволяет минимизировать указанные явления.

Отдельной проблемой можно назвать и использование животных с увечьями, либо старых, для виртуального «вымогательства» [4] денежных средств на оказание им помощи. И здесь очень трудно разобраться, действительно животное нуждается в поддержке, и денежные средства собирают реальные волонтеры, либо это способ «заработка», когда пострадавшее животное есть только в виртуальном пространстве, а реально уже погибло / усыплено / вылечено.

Выводы и предложения. В значительной части приведенных примеров можно выявить признаки мошенничества, однако привлечение за них к уголовной ответственности затруднительно как в силу отсутствия достаточных доказательств наличия именно преступления, так и в силу отсутствия необходимой правоприменительной практики. Однако нужно учитывать, что стоимость породистого щенка или котенка может достигать нескольких десятков тысяч рублей (в среднем от тридцати до восьмидесяти тысяч рублей в зависимости от породы, но может быть

еще выше), что по своим последствиям в виде причинения имущественного ущерба уже переводит проблему из разряда гражданско-правовых в уголовно-правовую сферу, особенно в случае умышленного введения в заблуждение относительно пользовательских, племенных или выставочных перспектив продаваемого домашнего питомца. Достоверно подтвердить происхождение конкретного животного может только генетическая экспертиза [1]. Кроме того, приобретение больного животного или животного с генетическими проблемами, которые приведут к заболеванию в дальнейшем, часто приводит к моральным и нравственным страданиям [3] ее владельца, особенно, если владельцем является ребенок или несовершеннолетний, так как домашнее животное часто выполняет функцию домашнего любимца.

Заявленная проблема является новой и требует своей дальнейшей разработки относительно как мер противодействия мошенническим схемам с использованием цифровых технологий и средств, так и использования возможностей цифровизации для минимизации последствий таких действий.

Список литературы

1. Гребенчук А. Е. Псовые как объект экспертного ДНК-анализа: криминалистические и генетические аспекты // Вопросы криминологии, криминалистики и судебной экспертизы. 2016. № 2 (40). С. 135–140.

2. Латыпова Э. Ю. О способах мошенничества, совершенного в отношении домашних животных // Образование, воспитание и право в контексте глобальных вызовов: сб. материалов Междунар. науч.-практ. конф., Чебоксары, 21–22 апреля 2023 г. / Чуваш. гос. ун-т им. И. Н. Ульянова. Чебоксары, 2023. С. 439–444.

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

4. Латыпова Э. Ю., Ключникова К. Е. Проблемы уголовной ответственности за вымогательство с использованием виртуального шантажа // Информационные технологии в деятельности органов прокуратуры: сборник материалов II Всероссийской научно-практической конференции. Казань: Казанский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2019. С. 110–113.

5. Латыпова Э. Ю., Мусина Р. Р. Некоторые проблемы мошенничества с помощью использования банковской карты с голосовым помощником // Информационные технологии в деятельности органов прокуратуры: сборник материалов II Всероссийской научно-практической конференции. Казань: Казанский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2019. С. 107–109.

6. Першин Е. А., Миронюк И. В. Мошенничество в сфере торговли домашними животными в России // Уральский научный вестник. 2022. Т. 1, № 11. С. 105–114.

7. Чипирование. Казанская ветеринарная больница. https://kazvethospital.net/

8. Что значит закон об обязательной регистрации собак в Московской области: Нужно ли чипировать животных? // Комсомольская правда. URL: https://www.mosobl.kp.ru/daily/27506/4767360

9. Юрченко И. А. Уголовная ответственность за мошенничество с домашними животными в России и за рубежом // Юридическая наука. 2022. № 7. С. 105–114.

А. И. Литовченко,
аспирант,
Кубанский государственный университет

DEEPFAKE КАК УГРОЗА ОБЩЕСТВЕННОЙ НРАВСТВЕННОСТИ

Аннотация. Развитие искусственного интеллекта, применяемого для генерации аудио-, фото- и видеоматериалов, дошло до этапа, когда грань между созданной и реальной информацией стирается, что вызывает обеспокоенность и влечет необходимость усиления противодействия такой форме дезинформации, как DeepFake. Целью данной статьи является оценка DeepFake как угрозы общественной нравственности. Быстрое совершенствование генеративных нейронных сетей и их массовое распространение, в том числе в простых для использования программных приложениях, позволяют с легкостью создавать реалистичные материалы, способные нанести ущерб правам и интересам личности и общества, выступая элементом «порнографических» преступлений.

Ключевые слова: DeepFake, преступление, нейронные сети, искусственный интеллект, порнографические материалы, общественная нравственность, сеть Интернет

DEEPFAKE AS A THREAT TO PUBLIC MORALS

Abstract. The development of artificial intelligence used to generate audio, photo and video materials has reached a stage when the line between created and real information is blurred, which causes concern and entails the need to strengthen counteraction to such a form of disinformation as DeepFake (from deep learning and fake). The purpose of this article is to assess DeepFake as a threat to public morality. The rapid improvement of neural networks using generative models and their ubiquity, including easy-to-use programs and applications, facilitates production of realistic materials that can harm the rights and interests of the individual and society, acting as an element of «pornographic» crimes.

Keywords: DeepFake, crime, neural networks, artificial intelligence, pornographic materials, public morality, Internet

За последние десятилетия наметилось четкое направление диджитализации множества сфер деятельности, приносящих доход их создателям, в том числе речь идет о нелегальном секторе экономики, связанном с оборотом запрещенных к распространению на территории нашего государства предметов, в частности порнографии. Распространение порнографических материалов становится более удобным и коммерчески выгодным для их создателей с приходом «информационной эры», так как большая часть такого контента потребляется с помощью информационно-телекоммуникационной сети Интернет.

Так, например, по данным глобальной платформы Statista, на конец 2022 г. Pornhub являлся четвертым по количеству посещений сайтом в мире: в месяц его посещали более 10,2 млрд человек [8]. Сеть Интернет позволяет лицам осуществлять распространение, публичную демонстрацию и рекламирование порнографии

в упрощенном формате из-за чего стала основным путем трафика порнографии, что отображается также и на данных официальной статистики, в соответствии с которыми число осужденных лиц за преступления, предусмотренные ст. 242–242.2 УК РФ [5], совершенные с использованием Сети в разы превышает иные способы совершения (рис. 1).

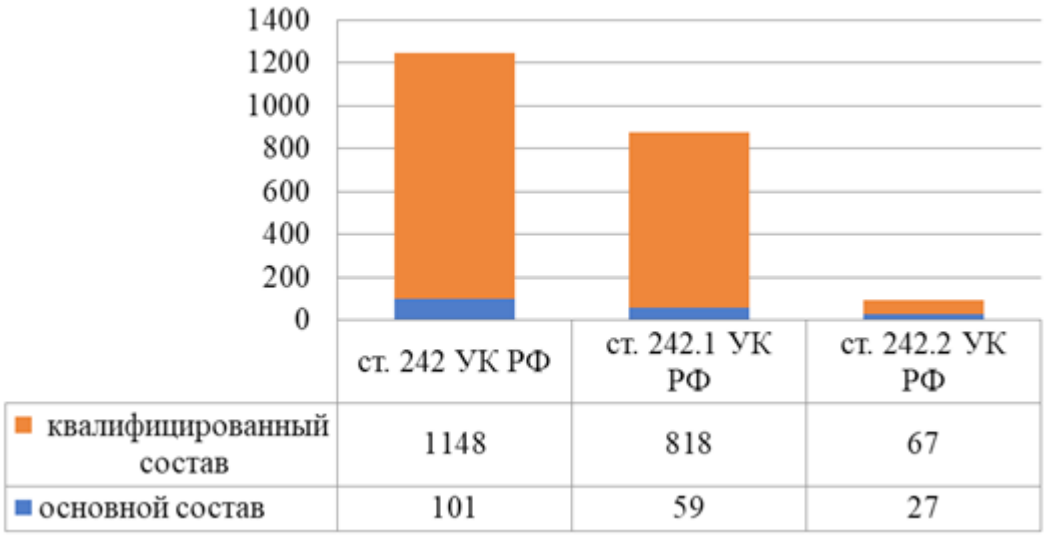


Рис. 1. Данные Судебного департамента при Верховном суде Российской Федерации о количестве осужденных лиц за преступления, предусмотренные ст. 242–242.2 УК РФ за 2017–2022 г.

Источник: URL: http://cdep.ru/?id=79

Важно также учитывать, что, помимо созданной с помощью реальных актеров порнографии, в секс-индустрии появляется новый вид синтетического контента – DeepFake, полностью или в части сгенерированный машинным интеллектом, также влияющий на общественную нравственность и нормальное психическое развитие населения в области сексуальных отношений. Данные материалы, хотя и могут создаваться без привлечения реальных людей для фото- и видео- съемок, имеют воздействие подобное традиционным формам порнографии, к примеру, из-за невозможности без специализированных программ по распознаванию отличить настоящее видео от сфабрикованного.

Иначе говоря, для лица, потребляющего DeepFake порнографию, не будет иметь значение способ ее создания. Виртуальная копия любого человека, чье изображение загружено в приложение или иной инструмент, работающий с технологиями искусственного интеллекта, может быть использована для изготовления порнографических материалов, в том числе с применением воссозданных индивидуальных характеристик мимики, движений и голоса, что повышает степень их негативного влияния.

Итак, погружение зрителей в синтезированный виртуальный контент может вызывать серьезные негативные последствия, такие как отрицательное влияние на межличностные отношения, укрепление стереотипов гендерного неравенства

и объективизации [8. С. 11], нормализацию психических парафилий и перверсий, и даже повышенную вероятность совершения в отношение других лиц преступлений против половой свободы.

Следовательно, DeepFake порнография способна нанести вред разными способами, но ее основная негативная направленность определяется причинением вреда общественной нравственности. Указанный термин имеет множество трактовок, определяющих моральные ценности господствующие в конкретном обществе [2. С. 4], особую форму общественного сознания, основанную на нормах, обычаях, взглядах на основные категории этики [1. С. 481], однако любая из названных позиций требует конкретизации через определение в том числе границ половой свободы и половой неприкосновенности как области охраны уголовного закона. Нейронные сети в рассматриваемой сфере служат инструментом, реконструирующим идентичность человека, либо моделирующим несуществующую в реальности ситуацию, что создает также угрозу безопасности и благополучия, через создание материалов с изображением сексуального насилия и преждевременную сексуализацию несовершеннолетних.

В связи с усилением за последние десятилетия «культа» искаженных представлений о сексуальности в общественном поле негативное влияние порнографии становится более отчетливым через формирование у людей самообъективации, психологических расстройств, неразвитой и ограниченной сексуальной самооценки, влияющей в том числе на формирование психических отклонений.

Сдерживающий характер от совершения преступлений в реальности или наступление ремиссии половых парафилий после просмотра порнографии, в настоящее время не доказаны, а с учетом выводов некоторых исследователей и вовсе отвергаются [8. С. 26], что наводит на мысль об увеличении потенциальной угрозы стать жертвой преступления в реальной жизни для лиц, явившихся прообразами DeepFake изображений. Помимо прочего доступность и неограниченное потребление порнографии, в том числе из-за ее быстрой генерации с помощью нейросетей, становится «подготовкой» индивида к ассоциированию девиантных форм сексуальной стимуляции.

Учитывая описанный выше вред, который могут нанести DeepFake материалы особенно в отношении несовершеннолетних, в науке высказана позиция к урегулированию применения такой формы машинного обучения [3. С. 115], в том числе через принятие конвенции о регулировании DeepFake технологий на международном уровне [4. С. 63–64].

Подводя итог сказанному, хотелось бы отметить, что повсеместное и регулярное потребление порнографического контента, упрощенное производство которого обусловлено применением искусственного интеллекта, вызывает серьезные опасения о последствиях таких действий, связанных с ухудшением физического и психического здоровья зрителей, в особенности несовершеннолетних.

Технология, которой посвящена данная работа, являясь достижением в методах глубокого обучения, сделала возможным генерирование реалистичных образов в злонамеренных целях. Опора на ранее существовавшие данные и проведенные исследования позволила нам обнаружить закономерности между злоупотреблением технологией DeepFake и ее влиянием на общественную нравственность, а также прийти к выводу о необходимости не только саморегулирования нейро-

сетей, но и государственного вмешательства, чтобы попытаться восстановить доверие к рассматриваемой технологии. Использование постоянно развивающихся и совершенствующихся автоматизированных систем искусственного интеллекта представляет в некоторой части угрозу охраняемым уголовным законом интересам ведь даже несмотря на отсутствие уголовной ответственности за их применение, тем не менее должны быть учтены при квалификации деяния ввиду их широких возможностей, порой опережающих человеческие.

Список литературы

1. Готчина Л. В. Глава 12. Преступления против здоровья населения и общественной нравственности // Уголовное право. Особенная часть: учебник. СПб., 2020.

2. Гусарова М. В. Преступления в сфере незаконного оборота порнографической продукции: анализ уголовно-правовых норм с учетом последних изменений в уголовном кодексе Российской Федерации // Вестник Казанского юридического института МВД России. 2013. № 13. С. 1–5.

3. Добробаба М. Б. Дипфейки как угроза правам человека // Lex Russica (Русский закон). 2022. Т. 75, № 11(192). С. 112–119.

4. Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64.

5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699

6. Al-Alosi, Hadeel. The criminalisation of fantasy material: law and sexually explicit representations of fictional children // London and New York: Routledge. 2018. URL: https://doi.org/10.4324/9780203701829

7. Most popular websites worldwide as of November 2022, by unique visitors // Statista. URL: https://www.statista.com/statistics/1201889/most-visited-websites-worldwide-unique-visits

8. Zheng R., Stear N.-H. Imagining in Oppressive Contexts, or What's Wrong with Blackface? Ethics. 2023. № 133(3).

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

О ЦИФРОВИЗАЦИИ УГОЛОВНОГО ПРОЦЕССА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВНЕДРЕНИЯ ЭЛЕКТРОННОГО УГОЛОВНОГО ДЕЛА

Аннотация. В статье поднимаются дискуссионные вопросы о цифровизации производства по уголовному делу на стадии предварительного расследования. Приведены мнения некоторых авторов о проблемах, способных препятствовать внедрению цифровых технологий в данный этап уголовного процесса на современном этапе, проведен анализ некоторых опасений по применению цифровых

способов осуществления производства по уголовному делу. Выводы указывают на неизбежность трансформации уголовного дела в цифровую среду.

Ключевые слова: блокчейн, цифровизация уголовного процесса, электронное уголовное дело, уголовный процесс, VR-технологии, виртопсия

DIGITIZATION OF THE CRIMINAL PROCEDURE: CURRENT ISSUES IN IMPLEMENTING ELECTRONIC CRIMINAL CASE

Abstract. The article raises controversial issues about the digitalization of criminal proceedings at the stage of preliminary investigation. The article presents the opinions of some authors about problems that can hinder the introduction of digital technologies at this stage of the criminal process at the present stage, and analyzes some concerns regarding the use of digital methods of carrying out criminal proceedings. The findings indicate the inevitability of the transformation of criminal proceedings into the digital environment.

Keywords: blockchain, digitalization of the criminal process, electronic criminal case, criminal process, VR technology, virtopsy

Повсеместное внедрение цифровых технологий во все сферы жизни человека, а также в общественные отношения, подталкивает к переходу от привычных форм их регулирования к новым, электронным формам.

Отечественная юриспруденция в этом вопросе не остается в стороне [6, 7, 8]. Переход процессуальных отраслей в электронную среду занимает уже более десятка лет, однако, по сравнению с темпами развития самих технологий, изменения протекают медленно. Так, если в судопроизводстве активно используется информационная среда и электронный документооборот, то в уголовном судопроизводстве и, в частности, досудебном уголовном судопроизводстве пока серьезные преобразования по внедрению информационных технологий не ощущаются.

Появились информационные базы, система обмена данными между органами, осуществляющими предварительное расследование, надзорными и контрольными органами. И все же это не говорит о цифровизации уголовного процесса. Это всего лишь первый шаг перехода в информационную среду. Для начала необходимо разобраться в понятиях электронная среда и цифровая среда. Зачастую, авторы смешивают эти понятия, когда за цифровизацию выдается электронный документооборот.

Так, Л. В. Санникова и Ю. С. Харитонова указывают: «Опасность смешения понятий «электронная» и «цифровая», заключается в том, что применение цифровых технологий для решения задач, стоящих перед государством и бизнесом, обеспечивает гораздо большую эффективность, чем простое использование электронной формы вместо бумажной» [5. С. 213].

И действительно, можно ли считать перевод из бумажного в электронный документооборот настоящей цифровизацией уголовного процесса? По нашему мнению, цифровизация уголовного расследования, должна подразумевать не только электронное копирование уголовного дела и возможность собирания справок, получение ответов на запросы от органов государственной власти посредством доступа к базам данных.

Цифровизация уголовного процесса – это полный переход к электронному уголовному делу. Оно должно подразумевать создание специальной платформы по типу «Э-уголовное дело». Вся информация по расследуемому делу переводится в электронное дело с момента первого этапа расследования, вносятся данные регистрации сообщения о преступлении (иного повода для возбуждении уголовного дела) и все последующие протоколы, постановления и документы.

В целом, тема исследования цифровизации уголовного процесса свидетельствует о высоком интересе ученных-процессуалистов в этой области. Так, проблемами перевода уголовно-процессуальных отношений в цифровую среду занималась А. Ю. Чурикова, которая говорит о возможных проблемах на современном этапе с внедрением такой формы. В частности, дублирование «бумажного» уголовного дела и электронного, отсутствие программного обеспечения и разный уровень подготовленности кадров [7. С. 209–216]. В то же время она указывает и на неизбежность внедрения цифровых технологий в уголовный процесс, что позволит повысить эффективность работы правоохранительной системы.

В. В. Синкевич проанализировал зарубежный опыт внедрения цифровых технологий в уголовный процесс [6. С. 129–134]. Указывается, что в числе стран, внедряющих такую форму процессуальной деятельности, есть и страны ближнего зарубежья. Выводы автора сводятся к тому, что цифровизация уголовного судопроизводства – это своевременный вопрос и данность современных правовых отношений. Профессор В. И. Пржиленский рассматривает вопросы цифровизации уголовного судопроизводства с позиции теоретико-познавательных основ уголовного судопроизводства. В исследовании им «критически разбираются тезисы о замене человека машиной в процессе раскрытия преступлений» [4. С. 17–29], рассматриваются проблемы научного подхода с философской стороны. Как видим, вопросы перехода в цифровую среду уголовно-процессуальных отношений в наше время являются очень обсуждаемыми и дискуссионными.

Однако общий вывод сводится к тому, что цифровизация уголовного процесса на стадии предварительного расследования – это в большей степени необходимость, чем нечто фантастическое. Хотя внедрение электронной формы производства по уголовному делу может содержать риск доступа и взлома посторонними лицами. Система может функционировать на базе алгоритмов выстроенных по примеру блокчейн, что поможет защитить ее от несанкционированного доступа и изменений посторонними лицами.

Данные по всем следственным действиям, производимым следователем могут быть внесены непосредственно в электронное уголовное дело. В этом случае цифровая среда должна предполагать возможность составления протоколов, постановлений, приобщения медиа файлов (фото-, аудио- и видеоизображений с места производства следственного действия). Цифровизация расследования уголовного дела позволит расширить возможности приобщения к материалам первичных электронных файлов, что исключит вероятность их изменений и фальсификации в дальнейшем.

Так, например, запись, сделанная при контроле телефонных переговоров подозреваемого, будет содержать данные о дате и времени их изготовления, что

не потребует проверки на предмет ее монтажа, внесения в нее изменений. В электронное уголовное дело могут вноситься результаты лазерного 3D-сканирования, когда будет производиться оцифровка места происшествия или место производства обыска, виртопсия (виртуальная аутоапсия).

Ряд авторов утверждают, что внедрение VR-технологий (одной из разновидностей систем создания цифровых копий визуальной обстановки следственного действия) «по своему информационному потенциалу значительно превосходят графические схемы, фотографии и видеозапись по уголовному делу и фактически являются логическим продолжением традиционной процедуры закрепления сведений, имеющих доказательственное и ориентирующее значение» [1. С. 56].

Виртуальная аутоапсия представляет «алгоритмы использования в следственном процессе результатов компьютерного моделирования трупа» [3. С. 183–192]. Такие результаты электронной фиксации могут быть применены при расследовании преступлений, где необходимо установление времени смерти, обстоятельств получения ранения, расследовании врачебных ошибок, а также при обследовании неопознанных трупов.

Доступ участников уголовного судопроизводства к электронному уголовному делу может быть обеспечен за счет предоставления пароля через интеграцию с системой государственных баз данных «Портал государственных услуг Российской Федерации «Госуслуги», а также специальных ключей, цифровой подписи. Так, адвокат, вступающий в уголовное дело в качестве защитника, имея квалифицированную электронную цифровую подпись, может получить доступ к той части информации в уголовном деле, которая доступна на определенном этапе расследования. В случае необходимости он может обжаловать действия (бездействия) должностного лица путем подачи жалобы посредством данной электронной площадки. Аналогично может быть подано ходатайство. Прокурор может получить материалы без соответствующего запроса самого уголовного дела и не отвлекать следователя от хода расследования. Свои представления он также может вносить в электронное дело. Таким образом будет налажен постоянный контроль за ходом расследования как со стороны защиты, так и со стороны надзорного органа.

Подозреваемый, обвиняемый, потерпевший, гражданский истец и гражданский ответчик, их представители также будут иметь право на доступ к электронному уголовному делу в любое время по специальному электронному ключу, с ограничениями исходя из их статуса в деле. Это упростит работу следователя в части обязанности предоставления копии материалов уголовного дела участникам, отправки уведомлений и вызова их к следователю.

Каждое действие участников уголовного процесса будет фиксироваться отображением информации, кто и когда входил в базу электронного уголовного дела, какие изменения вносил. Это не позволит вносить в него несанкционированные изменения, убережет от проникновения в систему посторонних лиц.

Система может быть запрограммирована на предоставление информации по истекающим срокам уголовного судопроизводства, информировать участников уголовного дела о необходимости явиться в органы власти, предоставить необходимые документы.

С точки зрения расследования также есть положительные моменты. Например, передача дела по подследственности и (или) территориальности будет намного ускорена. Сократится риск утраты документов, возможно быстрое установление ответственных за расследование. Объединение нескольких уголовных дел или выделение дел в отдельное производство будет также эффективно, поскольку будет возможность доступа ко всем оригинальным материалам дела по каждому из них.

Реализация в полной мере данной системы повлечет множество вопросов, решение которых будет необходимо заблаговременно. Так, в первую очередь, возникает вопрос о разработке программного обеспечения, учитывающего все нюансы и возможности создания такой площадки. Есть необходимость содержания специалиста в штате органа предварительного расследования, который будет оказывать техническую поддержку в тех случаях, когда это необходимо участникам уголовного производства. В части доступа к электронному уголовному делу подозреваемого, обвиняемого, потерпевшего и иных лиц также может быть множество проблемных моментов. Так, эти лица могут не обладать специальными навыками работы в электронной среде. В связи с этим дублирование материалов уголовного дела в бумажном виде может еще оставаться актуальной. С другой стороны, сама система может предусматривать виртуальную помощь таким участникам, указывать на возможность подать заявление, ходатайство, жалобу в электронном режиме, подсказать варианты действий.

Подводя итоги, можно сделать выводы, о том, что цифровизация уголовного процесса – это не простой, но необходимый шаг в развитии уголовного судопроизводства. Проблемой внедрения такой системы на сегодняшний день остается разработка комплексной государственной программы, которая по мнению Ю. Новолодского, должна учитывать не только сам непосредственный процесс перехода в «цифру», но и произвести детальный анализ действующего законодательства с целью его подготовки. «Без определения современных недостатков ожидаемая цифровизация будет неспособна принести пользу обществу и на многие годы может «законсервировать» сложившиеся недостатки для будущих поколений» [2].

Реализация государственной программы цифровизации должна проходить поэтапно. На начальном этапе – разработка понятийного аппарата для терминов и определений, используемых в информационных системах. Далее подготовка законодательной базы путем введения новой Главы в Уголовно-процессуальный кодекс Российской Федерации в Раздел XIX, который может быть переименован как «Использование в уголовном судопроизводстве электронной формы расследования уголовного дела». В дальнейшем постепенный полный переход от бумажной формы к цифровому документообороту и производству расследования уголовных дел с применением цифровых технологий.

Опасения относительно угроз несанкционированного доступа к материалам уголовного дела могут быть решены за счет внедрения алгоритмов блокчейн, на базе которого будет функционировать система. В конце концов, бумажный вариант уголовного дела имеет больше рисков попасть в руки лиц, не имеющих права доступа к нему, или быть уничтоженным, поврежденным.

Еще одной проблемой является низкая подготовленность кадров, сложность интеграции с действующим законодательством. Повышение квалификации и подготовка будущих следователей на этапе профессионального образования уже сейчас должна вестись в ключе изучения дисциплин профессионального цикла с уклоном на внедрение цифровых технологий. Для иных участников процесса должна быть выстроена система понятного интерфейса работы с алгоритмами цифрового уголовного дела по примеру систем «Госуслуги» или личного кабинета налогоплательщика.

Конечно, перечисленные вопросы и опасения далеко не единственные. С внедрением системы электронного уголовного дела появятся и другие, но все это есть развитие человечества и оно должно быть направлено на повышение эффективности в регулировании общественных отношений.

Список литературы

1. Антонов И. О., Клюкова М. Е., Кугуракова В. В., Верин А. Ю. Процессуальные особенности и перспективы использования по уголовному делу цифровых копий визуальной обстановки следственного действия // Евразийская адвокатура. 2022. № 4(59). URL: https://cyberleninka.ru/article/n/protsessualnye-osobennosti-i-perspektivy-ispolzovaniya-po-ugolovnomu-delu-tsifrovyh-kopiy-vizualnoy-obstanovki-sledstvennogo

2. Новолодский Ю. Цифровизация уголовного процесса //Официальный портал Федеральной палаты адвокатов Российской Федерации. URL: https://fparf.ru/polemic/opinions/tsifrovizatsiya-ugolovnogo-sudoproizvodstva

3. Оракбаев Асхат Бакытулы, Курмангали Жанар Куанышбайкызы, Бегалиев Ернар Нурланович, Сырбу Александр Владимирович, Бегалиев Бахытбек Адильханович К вопросу об использовании результатов виртуальной аутопсии (виртопсии) в ходе расследования преступелний: научный обзор // Судебная медицина. 2023. № 2. URL: https://cyberleninka.ru/article/n/k-voprosu-ob-ispolzovanii-rezultatov-virtualnoy-autopsii-virtopsii-v-hode-rassledovaniya-prestupleniy-nauchnyy-obzor

4. Пржиленский В. И. Теоретико-познавательные основы уголовного судопроизводства в контексте возможностей его цифровизации // Журнал российского права. 2019. № 7. URL: https://cyberleninka.ru/article/n/teoretiko-poznavatelnye-osnovy-ugolovnogo-sudoproizvodstva-v-kontekste-vozmozhnostey-ego-tsifrovizatsii

5. Санникова Л. В., Харитонова Ю. С. Цифровые активы: правовой анализ: монография. М.: 4 Принт, 2020. 304 с.

6. Синкевич В. В. Цифровизация уголовного процесса: зарубежный и отечественный опыт // Вестник Волгоградской академии МВД России. 2022. № 1(60). URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-ugolovnogo-protsessa-zarubezhnyy-i-otechestvennyy-opyt

7. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

8. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник СГЮА. 2021. № 6 (143). URL: https://cyberleninka.ru/article/n/problemy-tsifrovizatsii-rossiyskogo-ugolovnogo-protsessa

Х. У. Маматкулова,
преподаватель,
Ташкентский государственный юридический университет

ПОНЯТИЕ ДОКАЗАТЕЛЬСТВ И ИХ СВОЙСТВА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В статье на основании изучения зарубежного опыта рассматривается понятие доказательств в уголовном процессе. Отмечена современная специфика и свойства доказательств. Предложено определение понятия доказательств, а также критерии допустимости доказательств по уголовным делам.

Ключевые слова: уголовный процесс, доказательства, свойства доказательств, относимость, допустимость, достоверность, достаточность, обстоятельства, подлежащие доказыванию

THE CONCEPT AND PROPERTIES OF EVIDENCE IN CRIMINAL PROCEEDINGS

Abstract. The article discusses some issues of the concept of evidence in criminal proceedings, studied and discussed the foreign experience of countries on the institution of evidence (Kazakhstan, Georgia, Azerbaijan). The specifics and properties of evidence, relevance, admissibility, reliability and sufficiency of evidence are also discussed. The author gives judgments on the criteria of evidence in criminal proceedings, formed the actual definition of the concept of evidence, as well as the admissibility of evidence in criminal cases.

Keywords: criminal process, evidence, properties of evidence, relevance, admissibility, reliability, sufficiency, circumstances to be proved

В академическом контексте тема доказательств в уголовном процессе и доказательственной теории занимает ключевое место. Проблематика доказательств продолжает оставаться релевантной. Этот вопрос выступает в центре внимания как в научных исследованиях, так и в практической сфере уголовного судопроизводства.

Уголовно-процессуальный кодекс Республики Узбекистан формулирует определение доказательств как «фактические данные, на основе которых уполномоченные органы и суд определяют наличие или отсутствие преступления, виновность лица и другие релевантные аспекты для компетентного рассмотрения уголовного дела» [1]. Законодательство подразумевает под доказательствами все фактические данные, при условии, что эти данные соответствуют установленным стандартам. Перед детальным изучением этих стандартов рассмотрим, как другие юрисдикции определяют доказательства.

Уголовно-процессуальный кодекс Республики Казахстан утверждает: «Доказательства в уголовном деле представляют собой законно собранные фактические данные, на основании которых уполномоченные органы и суд определяют совершено ли деяние, предусмотренное Уголовным кодексом Республики Казахстан, и другие существенные аспекты для объективного рассмотрения дела» [2].

Стоит отметить, что акцент делается на законность процедуры сбора фактических данных, что становится ключевым критерием в определении доказательства.

Также представляет интерес и формулировка данного понятия в Уголовно-процессуальном кодексе Грузии: «Доказательства – информация, представленная в суд в установленном законом порядке, содержащие эту информацию предметы, документы, вещества или иные объекты, на основе которых стороны в суде подтверждают или отрицают факты, дают им правовую оценку, выполняют обязанности, защищают свои права и законные интересы, а суд устанавливает наличие или отсутствие факта или деяния, ввиду которого осуществляется уголовный процесс, совершение или несовершение этого деяния определенным лицом, его виновность либо невиновность, а также обстоятельства, влияющие на характер и степень ответственности обвиняемого, характеризующие его личность. Документ – доказательство, если он содержит сведения, необходимые для установления фактических и правовых обстоятельств уголовного дела. Документом считается любой источник, в котором информация запечатлена в словесно-знаковой форме или (и) в виде фото-, кино-, видео-, звуко- или иной записи, либо с применением других технических средств» [3]. Заслуживает внимания тот факт, что представлен подробный детальный разбор данного понятия, что дает глубокое понимание доказательств и устраняет потенциальные двусмысленности.

Что касается Уголовно-процессуального кодекса Азербайджана [4, статья 124], доказательствами по уголовному преследованию признаются заслуживающие доверия улики (сведения, документы, вещи), полученные судом или сторонами уголовного процесса. Такие доказательства:

1) должны быть получены с соблюдением требований уголовно-процессуального законодательства без ограничения конституционных прав и свобод человека и гражданина либо с ограничением по постановлению суда (а в случаях, не терпящих отлагательства, – по постановлению следователя);

2) должны показывать, имело ли место событие преступления, имеются ли признаки преступления в совершенном деянии, было ли совершено данное деяние обвиняемым, его виновность или невиновность, а также иные обстоятельства, имеющие значение для правильного разрешения обвинения. Таким образом, Уголовно-процессуальный кодекс Азербайджана предоставляет как конкретное определение доказательства, так и четко прописанные требования к его получению, что подчеркивает важность защиты прав и свобод индивида в уголовном процессе.

В эпоху развития цифровых технологий актуальность рассмотрения электронных доказательств в уголовном праве возрастает. Электронные доказательства представляют собой информацию в электронном виде, применяемую для подтверждения или опровержения определенных утверждений в контексте уголовно-правовой процедуры.

Основные характеристики электронных доказательств:

Цифровая основа: Эти доказательства преимущественно имеют цифровую структуру, включая, но не ограничиваясь, текстовые документы, графические изображения, аудиовизуальные записи, электронные журналы и базы данных.

Потенциал модификации: Цифровые материалы обладают свойством легкой копируемости и модифицируемости, что делает их подверженными внешнему воздействию. Отсюда вытекает необходимость обеспечения их аутентичности и неповрежденности.

Временное сохранение: Электронная информация часто характеризуется ее кратковременностью и может быть быстро изменена или удалена, что создает сложности в ее сохранении или реконструкции.

Многократное применение: Одни и те же электронные доказательства могут быть актуальны в разнообразных юридических контекстах.

Требование технической экспертизы: Работа с электронными доказательствами предполагает наличие специфических технических компетенций и средств для их анализа, восстановления и аутентификации.

С точки зрения правоприменения, ключевым аспектом при работе с электронными доказательствами является их правомерное получение и обеспечение их аутентичности. Неправомерно полученные электронные доказательства могут быть признаны судом недопустимыми, а сомнения в аутентичности могут подорвать их убедительность.

Обобщая вышесказанное можно сформулировать собственное определение по доказательствам в уголовном судопроизводстве, а именно: доказательствами по уголовному делу служат сведения, фактические данные, которые получены законным путем без нарушения конституционных прав и свобод человека и гражданина и которые служат установлению истины по уголовному делу, а также служат подтверждению или опровержению обвинения или защиты в уголовном деле.

Следует отметить, фактические данные устанавливаются: показаниями свидетеля, потерпевшего, подозреваемого, обвиняемого, подсудимого, заключением эксперта, вещественными доказательствами, материалами звукозаписи, видеозаписи и кинофотосъемки, протоколами следственных и судебных действий и иными документами (ч. 2 ст. 81 УПК РУз). В современной эпохе информационные технологии и цифровые носители становятся неотъемлемой частью доказательственного процесса. Так, Ш. Собиров относит к потенциальным источникам цифровых доказательств персональные устройства, такие как смартфоны, компьютеры, которые содержат огромное количество информации; журналы звонков, текстовые сообщения, электронные письма, история просмотров, данные о местоположении и файлы и др. [5. С. 68–71].

В соответствии с Уголовно-процессуальным законодательством [1, ст. 82], к числу обстоятельств, требующих обоснования в рамках уголовного расследования (для направления дела в суд с обвинительным заключением или обвинительным актом и для постановления обвинительного приговора), включаются:

1) объект преступления; характер и размер вреда, причиненного преступлением; обстоятельства, характеризующие личность потерпевшего;

2) время, место, способ, а также другие указанные в Уголовном кодексе обстоятельства совершения преступления; причинная связь между деянием и наступившими общественно опасными последствиями;

3) совершение преступления данным лицом;

4) совершение преступления с прямым или косвенным умыслом либо по небрежности или самонадеянности; мотивы и цели преступления;

5) обстоятельства, характеризующие личность обвиняемого, подсудимого.

Фактические материалы, которые применяются в качестве доказательственной базы, должны соответствовать строгим критериям. К основным свойствам доказа-

тельства относятся: относимость, допустимость и достоверность. Исследователи также акцентируют внимание на важности достаточности собранных доказательств.

Относимость доказательства в одних источниках трактуется как пригодность устанавливать факты, являющиеся предметом доказывания, т. е. определить логическую связь между сведениями, которые составляют содержание доказательства, и тем, что нужно установить для правильного разрешения уголовного дела. В других источниках относимость понимается как связь между содержанием доказательства и обстоятельствами, подлежащими доказыванию, дающая возможность использовать то или иное доказательство для установления указанных обстоятельств [6. С. 168–169]. Конкретно, Уголовно-процессуальный кодекс Республики Узбекистан определяет, что доказательство признается относящимся к уголовному делу, если оно представляет собой сведения о фактах или предметах, которые подтверждают, опровергают или ставят под сомнение выводы о существовании обстоятельств, имеющих значение для дела [1, статья 95].

Допустимость доказательства обозначает его соответствие установленным законодательным требованиям. Так, согласно Уголовно-процессуальному законодательству доказательство признается допустимым, если оно собрано в установленном порядке и соответствует условиям, изложенным в статьях 88, 90, 92–94 УПК Республики Узбекистан. Отдельные юрисдикции определяют свои требования к допустимости доказательств. В Узбекистане, например, информация, полученная незаконными способами или с нарушением законодательно установленных прав участников уголовного процесса, не может быть принята в качестве доказательства [1, статья 951]. Кроме того, не могут быть признаны доказательствами фактические данные, полученные:

1) с применением пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания в отношении участников уголовного процесса либо их близких родственников;

2) путем их фальсификации (подделки);

3) с нарушением прав подозреваемого, обвиняемого или подсудимого на защиту, а также права пользования услугами переводчика;

4) в результате проведения процессуального действия по уголовному делу лицом, не имеющим права осуществлять производство по данному уголовному делу;

5) от неизвестного источника либо от источника, который не может быть установлен в процессе производства по уголовному делу;

6) из показаний потерпевшего, свидетеля, подозреваемого, обвиняемого, подсудимого в ходе дознания, предварительного следствия, которые не нашли своего подтверждения в суде совокупностью имеющихся доказательств.

Исходя из вышеприведенного, для признания доказательства допустимым по уголовному делу, оно должно быть получено: из законных источников, без применения запрещенных видов обращения и насилия, с соблюдением компетенции лица, которое уполномочено на проведение того или иного действия, с соблюдением процессуальных прав участников уголовного процесса, а также которые могут быть подтверждены в суде совокупностью имеющихся доказательств.

Обеспечение допустимости электронных доказательств в уголовном процессе стоит в центре внимания юридической практики. В контексте допустимости основное

внимание уделяется легитимности, релевантности, достоверности и целостности представленных материалов. Рассмотрим основные аспекты в этой области:

Легальность получения: Важно удостовериться, что электронные доказательства были получены в соответствии с законодательством, учитывая такие моменты, как правила проведения обыска и законы о защите личных данных.

Аутентификация: Необходимо убедиться, что представленное электронное доказательство действительно соответствует его первоначальному источнику и не было искажено.

Обеспечение целостности: Очень важно подтвердить, что с момента фиксации доказательство не подвергалось изменениям или повреждениям. Применение методов, таких как криптографическое хеширование, может обеспечить такое подтверждение.

Продолжительность сохранности: Следует гарантировать, что с момента фиксации доказательства до их представления в суде они были надлежащим образом сохранены и не подвергались внешнему воздействию.

Релевантность: Среди огромного объема электронной информации важно выделить только ту, которая имеет отношение к данному уголовному делу.

Привлечение экспертов: В сложных случаях может потребоваться экспертное мнение, чтобы определить допустимость или особенности интерпретации электронного доказательства.

Предварительное рассмотрение: Некоторые суды проводят специализированные слушания, целью которых является определение допустимости представленных электронных доказательств.

Международный контекст: При работе с данными, которые пересекли государственные границы, необходимо учитывать особенности законодательства соответствующих стран.

Допустимость электронных доказательств является предметом многочисленных исследований и обсуждений, что подчеркивает важность строгого следования законодательству и стандартам при их применении в судебном порядке.

Следующее свойство доказательств в уголовном процессе – достоверность доказательств означает соответствие их действительности. Достоверные доказательства правильно отражают события и обстоятельства, имевшие место в прошлом и подлежащие установлению по делу. Недостоверными являются доказательства, в искаженном виде отражающие события или обстоятельства, подлежащие доказыванию. Недостоверными следует считать показания потерпевшего, свидетеля, заключение эксперта, если они в силу ошибки или по иной причине такого рода неверно восприняли или воспроизвели увиденное и услышанное, либо когда эксперт допустил ошибку при исследовании [7. С. 35]. Достоверность – это критерий, который устанавливается различными способами и предполагает полную и тщательную проверку доказательства для обеспечения соответствия действительности. Таким образом, данный критерий является фундаментом для установления правды в рамках уголовного процесса.

Еще один критерий, который большинство ученых считают обязательным, – это критерий «достаточность доказательств». Достаточность доказательств играет

критически важную роль в уголовном процессе. Это обеспечивает, что принятое судебное решение базируется на обширном, детальном и объективном рассмотрении всех доступных доказательств по делу. Совокупность доказательств признается достаточной для разрешения дела, если собраны все относящиеся к делу достоверные доказательства, неоспоримо устанавливающие истину о всех и каждом из обстоятельств, подлежащих доказыванию. Именно достаточность обеспечивает полноту материалов для признания лица виновным по уголовному делу. Ответственность за обеспечение достаточности доказательств по уголовным делам лежит на должностных лицах, ответственных за собирание и закрепление доказательств (дознаватель, следователь, прокурор, суд). В случае необеспечения достаточности материалов для обвинения, лицо должно быть оправдано. Недостаточность доказательств является основанием для вынесения оправдательного приговора (ст. 469 УПК), а также основанием для отмены судом апелляционной инстанции обвинительного приговора суда первой инстанции (ст. 497[27] УПК: собранные по делу доказательства недостаточны для признания подсудимого виновным и возможности собирания дополнительных доказательств исчерпаны).

Резюмируя вышесказанное, обозначим ключевые моменты нашего научного материала:

1. Доказательствами по уголовному делу служат сведения, фактические данные, которые получены законным путем без нарушения конституционных прав и свобод человека и гражданина и которые служат установлению истины по уголовному делу, а также подтверждению или опровержению обвинения или защиты в уголовном деле.

2. Электронные доказательства представляют собой информацию в электронном виде, применяемую для подтверждения или опровержения определенных утверждений в контексте уголовно-правовой процедуры.

3. Свойствами доказательства являются относимость, допустимость, достоверность и достаточность. Данные критерии взаимосвязаны и в совокупности обеспечивают вынесение обвинительного или оправдательного решения по уголовному делу.

4. Для признания доказательства допустимым по уголовному делу, оно должно быть получено из законных источников, без применения запрещенных видов обращения и насилия, с соблюдением компетенции лица, которое уполномочено на проведение того или иного действия, с соблюдением процессуальных прав участников уголовного процесса, а также которые могут быть подтверждены в суде совокупностью имеющихся доказательств.

Список литературы

1. Уголовно-процессуальный кодекс Республики Узбекистан от 22.09.1994. URL: https://lex.uz/docs/111463#186096

2. Уголовно-процессуальный кодекс Республики Казахстан. URL: https://online.zakon.kz/Document/?doc_id=31575852

3. Уголовно-процессуальный кодекс Грузии.URL: https://www.matsne.gov.ge/ru/document/download/90034/37/ru/pdf

4. Уголовно-процессуальный кодекс Азербайджана. URL: https://www.migration.gov.az/content/pdf/f5875139b52568b64830edb7a3d5855d.pdf

5. Собиров Ш. Уголовно-процессуальное значение цифровых сведений в системе доказательственного права. Взаимодействие науки и обществ. путь к инновационному развитию. 2023. № 1(1). С. 68–71. URL: https://inlibrary.uz/index.php/interaction-science-society/article/view/22406

6. Амирбекова Г., Асельдеров М. К вопросу о допустимости, относимости, достоверности и достаточности доказательств в уголовном судопроизводстве // Государственная служба и кадры. 2020. № 5. С. 168–169. URL: https://cyberleninka.ru/article/n/k-voprosu-o-dopustimosti-otnosimosti-dostovernosti-i-dostatochnosti-dokazatelstv-v-ugolovnom-sudoproizvodstve

7. Савельева Н. В. Проблемы доказательств и доказывания в уголовном процессе: учеб. пособие. Краснодар: КубГАУ, 2019. С. 35.

Ю. А. Мартынов,
старший преподаватель,
БИП-университет права и социально-информационных технологий

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОКОНЧАНИИ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

Аннотация. В статье предпринята попытка осмысления возможностей использования новейших информационных технологий участниками уголовного процесса на этапе окончания предварительного расследования уголовного дела. Цель исследования – выработка предложений по оптимизации процедуры ознакомления участников уголовного процесса с материалами уголовного дела и уведомления заинтересованных лиц об окончании предварительного расследования. В ходе исследования использовались историко-правовой, статистический методы, метод анализа и синтеза. Вносятся предложения о совершенствовании уголовно-процессуального законодательства в данной сфере с целью оптимизации процедур уведомления участников процесса об окончании предварительного расследования и ознакомления их с материалами уголовного дела, в том числе с применением цифровых технологий.

Ключевые слова: предварительное расследование, цифровые технологии, ознакомление с материалами дела, участник уголовного процесса, электронный документооборот

FEATURES OF USING INFORMATION TECHNOLOGY AT COMPLETION OF PRELIMINARY INVESTIGATION

Abstract. The article attempts to comprehend the possibilities of using the latest information technologies by participants in criminal proceedings at the stage of completing the preliminary investigation of a criminal case. Purpose of the study: to develop proposals for optimizing the procedure for familiarizing participants in criminal proceedings with

the materials of the criminal case and notifying interested parties about the completion of the preliminary investigation. During the study, historical, legal, statistical methods, methods of analysis and synthesis were used. Proposals are made to improve criminal procedural legislation in this area. The article has high scientific value, since it contains specific proposals for improving criminal procedural legislation in order to optimize the procedures for notifying participants in the process about the completion of the preliminary investigation and familiarizing them with the materials of the criminal case, including the use of digital technologies.

Keywords: preliminary investigation, digital technologies, familiarization with case materials, participant in criminal proceedings, electronic document management

Под окончанием предварительного расследования традиционно понимается «заключительный (часть) этап стадии предварительного расследования, берущий начало с момента выполнения следователем всех процессуальных действий по всестороннему, полному и объективному исследованию обстоятельств, подлежащих доказыванию по уголовному делу, включающий комплекс процессуальных действий, проводимых следователем, начальником следственного подразделения, прокурором с участием других субъектов уголовно-процессуальных отношений и завершающийся принятием решения о дальнейшем движении уголовного дела» [3. С. 409].

Важнейшими процессуальными действиями данного этапа расследования являются: а) уведомление участников уголовного процесса об окончании предварительного следствия и б) ознакомление их с материалами уголовного дела, в том числе с вещественными доказательствами, приобщенными к делу. После реформирования суда и судебной системы Российской империи в 60-х годах позапрошлого века ознакомление потерпевшего, гражданского истца, а также обвиняемого и его защитника с материалами дела стало традиционным процессуальным действием для отечественного уголовного процесса. Так, в ст. 476 Устава уголовного судопроизводства Российской империи (далее – УУС) было закреплено положение, согласно которому судебный следователь по окончанию предварительного следствия, предъявив обвиняемому следственное производство, если от того поступило соответствующее ходатайство, обязан был выяснить, не желает ли ознакомленный представить еще что-либо в свое оправдание. Данная норма почти без изменений «перекочевала» в ст. 211 УПК РСФСР, принятого постановлением ВЦИК РСФСР от 25.05.1922, а ст. 252 УПК РСФСР, утвержденного постановлением ВЦИК РСФСР от 15.02.1923, предоставляла право ознакомления с материалами дела как подсудимому, так и его защитнику после передачи уголовного дела в суд. Эта норма на практике иногда игнорировалась правоприменителями.

В 1960 г. советский законодатель вернул обвиняемому и его защитнику право на ознакомление с материалами дела с момента окончания предварительного следствия, т. е. ввел нормы, подобные УУС 1864 г. (см. тексты УПК БССР и УПК РСФСР 1960 г.).

Ныне как в УПК Республики Беларусь (ст. 257, 258), так и в УПК РФ (ст. 215, 217) предусмотрено право обвиняемого и его защитника на ознакомление со всеми

материалами уголовного дела при окончании предварительного расследования. Эти участники процесса не могут быть ограничены во времени, необходимом для ознакомления с делом, что соответствует требованиям, предъявляемым международным сообществом к государствам, ратифицировавшим Конвенцию о защите прав человека и его основных свобод, согласно которой каждому обвиняемому орган уголовного преследования либо суд должен предоставить достаточное время и возможности для подготовки своей защиты (подпункт (b) пункта 3 ст. 6 Конвенции о защите прав человека и основных свобод).

По оценкам российских ученых О. И. Андреевой и О. В. Желевой, на современном этапе ознакомление с материалами уголовного дела примерно по 37,01 % дел длилось более месяца, причем увеличение сроков ознакомления (а зачастую – фактически углубленного изучения материалов) было связано с объемом дел. Так, свыше месяца проходило ознакомление: при наличии в деле от 7 до 15 томов – по 35,29 % дел; при наличии в деле от 15 до 20 томов – по 43,24 %; при наличии в деле более 20 томов – по 66,67 % уголовных дел [1. С. 181–183].

Проблема нарушения процессуальных сроков предварительного расследования и вопросов сокращения времени ознакомления лиц, явно затягивающих данное процессуальное действие, неоднократно отражались в юридической литературе. Имеется и обширная правоприменительная практика. Дискуссии представителей адвокатского корпуса, с одной стороны, и следователей и прокуроров, с другой, ведутся, как правило, вокруг таких вопросов, как: что представляет собой «явное затягивание срока» стороной и как этот факт доказать; кто должен отвечать за нарушение процессуальных сроков в процессе длительного ознакомления; каков алгоритм действий следователя при затягивании времени ознакомления [1. С. 176–199; 6. С. 22–23; 7. С. 19].

Для осмысления возможностей использования новейших информационных технологий участниками уголовного процесса на этапе окончания предварительного расследования уголовного дела необходимо прежде всего уяснить смысл словосочетания «информационные технологии». Легальное определение информационных технологий дано в Федеральном законе № 149-ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Так, информационные технологии – это процессы, использующие совокупность средств и методов сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта, а также распространения информации и способы осуществления таких процессов и методов [8].

Внедрение информационных технологий в деятельность следственных подразделений стран постсоветского пространства началось примерно с середины 90-х годов XX века, когда в кабинетах следователей и прокуроров появились первые персональные компьютеры, посредством которых началось составление уголовно-процессуальных документов в электронной форме. Ныне «сквозными» технологическими процессами для всех видов производств становятся автоматизация, роботизация и интеллектуализация [13. p. 42].

Как справедливо указывают О. А. Зайцев и П. С. Пастухов, «если проводить параллели между цифровизацией общества и действующей технологией уголов-

но-процессуальной деятельности, то становится понятно, что невозможно осуществить цифровую трансформацию в условиях бесконечного потока бумажных документов, в отдельных кабинетах, создавая дублирующие друг друга информационные системы, которые будут ограничены “стенами” ведомств. Должна меняться организация получения криминалистически значимой информации в электронном виде для принятия промежуточных решений» [4. С. 758].

С. В. Зуев утверждает, что необходимо соответствующее информационное обеспечение уголовного процесса, выдвинул идею информационного превосходства правоохранительных органов над преступностью [5. С. 4]. Несомненно, данная идея весьма важна для построения принципиально новой модели предварительного следствия, сочетающей в себе как быстрое накопление криминалистически значимой информации, фиксирование ее в электронных источниках, так и оперативную коммуникацию всех государственных органов и должностных лиц, производящих расследование и надзирающих за соблюдением законности при производстве оперативно-розыскных мероприятий и следственных действий.

Что касается конкретных предложений с указанием наименования информационных технологий, то, например, П. Е. Короткова и С. С. Юрьев для повышения достоверности добытых сведений и оптимизации предварительного расследования предлагают использовать так называемые «технологии распределенного реестра» (в частности, блокчейна) [12. С. 44].

Особенностями блокчейна как технологии, по мнению Т. Чепковой и Е. Лиходей, является «группировка и организация всех данных в цепочку блоков с криптографической защитой», причем «в такие последовательные цепочки можно только добавлять новые блоки данных, но нельзя исправлять или удалять уже записанные данные»; т. е. у правоприменителя и иных заинтересованных лиц имеется возможность отслеживания всей истории записей (транзакций), при этом систему практически невозможно взломать, а сохраненные данные – изменить или подделать [11].

Применительно к составлению и оформлению уголовно-процессуальных документов на стадиях возбуждения уголовного дела и в ходе предварительного расследования, полагаем, целесообразно использовать систему «публичного блокчейна закрытого типа», в которой доступ к проверке идентичности помещенных в электронный вариант уголовного дела копиям, направляемым участникам процесса, ограничен и контролируется специально уполномоченными на это должностными лицами (начальником следственного подразделения, прокурором, а по окончании предварительного расследования – и стороной защиты) [3. С. 88–94].

При этом процессуальные документы составляются в ходе производства следственного (процессуального) действия и немедленно помещаются в единую базу данных после окончания данного действия. Уголовное дело данные процессуалисты предлагают формировать в электронном виде автоматически по определенным параметрам. Для внедрения подобной системы требуется разработка специального программного обеспечения и, безусловно, внесение существенных изменений в УПК. Предлагается также апробация функционирования системы в отдельном регионе страны. Реализация данной инициативы поможет, на наш взгляд, не только сократить сроки, но повысить качество предварительного расследования.

Что касается уведомления физических лиц о необходимости прибытия в орган уголовного преследования для участия в процессуальных действиях, а также уведомления об окончании предварительного следствия и возможности ознакомления с материалами уголовного дела, приобщенными к делу вещественными доказательствами, то давно назрела необходимость внедрения электронного информирования всех заинтересованных лиц – потенциальных участников процессуальных действий. Наиболее детально предложения по введению электронного информирования участников уголовного процесса в досудебном производстве сформулировал Д. А. Воронов в 2020 г. [2. С. 301–302]. Заметим, что подобный порядок уведомления (информирования лиц) уже используется при осуществлении гражданского и хозяйственного процессов в Республике Беларусь.

Таким образом, в целях оптимизации процедуры окончания предварительного расследования и ознакомления участников уголовного процесса с материалами дела предлагаем внести в УПК Республики Беларусь [9] следующие дополнения:

1. Дополнить главу 22 УПК Республики Беларусь статьей 1951 «Электронное информирование участников процессуальных действий», состоящей из двух частей, закрепив в них порядок вызова лица для производства процессуальных действий и использование электронных документов при производстве предварительного расследования:

«Часть 1. Участнику уголовного процесса может быть предложено дать согласие на получение уведомлений о принятых процессуальных решениях, повесток, копий иных процессуальных документов в электронной форме (СМС-сообщения, электронная почта, иные способы и средства передачи электронных данных)».

«Часть 2. Согласие лица на электронное информирование подтверждается документом, в котором указываются данные об этом лице и его согласии на электронное информирование, а также способы связи (номер телефона, адрес электронной почты, иные), посредством которых должны осуществляться вызовы, уведомления, вручение копий процессуальных документов» [14].

2. Дополнить ст. 255 УПК Республики Беларусь частями 4^1 и 4^2 следующего содержания:

«Часть 4^1. Предоставление по окончании предварительного расследования потерпевшему, гражданскому истцу, гражданскому ответчику, обвиняемому и его защитнику, давших согласие на получение копий документов в электронной форме, материалов уголовного дела обеспечивается путем одновременного предоставления (направления) им копий материалов дела на электронных носителях. Лицо, содержащееся под стражей, знакомится с электронными документами при помощи технических средств, предоставляемых администрацией мест содержания под стражей либо органом предварительного расследования. Умышленное повреждение этих технических средств приравнивается к отказу в реализации права на ознакомление с материалами уголовного дела».

«Часть 4^2. Способ предоставления участнику уголовного процесса электронных копий материалов уголовного дела (передача технического средства, обеспечивающего возможность ознакомления с электронными документами, или электронного носителя, копирование на электронный носитель участника уголовного процесса,

отправление на электронную почту либо иной способ) определяется следователем в зависимости от технической возможности и объемов дела» [14].

В недалекой перспективе, полагаем, в уголовном судопроизводстве Союзного государства России и Беларуси произойдет полная замена бумажного документооборота электронным, будет внедрено электронное информирование участников уголовного процесса на всех стадиях.

Список литературы

1. Андреева О. И, Желева О. В. Злоупотребление обвиняемым субъективными правами и его преодоление в ходе предварительного расследования. Томск: Издательский Дом Томского государственного университета, 2019. 240 с.

2. Воронов Д. А. Электронное информирование участников процесса в досудебном производстве // Уголовный процесс. 2020. № 4 (184). С. 88–94.

3. Досудебное производство в уголовном процессе: учеб. пособие / И. В. Данько и др.; под ред. И. В. Данько. Минск: РИВШ, 2022. 460 с.

4. Зайцев О. А., Пастухов П. С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. Юридические науки. 2019. Вып. 46. С. 752–777.

5. Зуев С. В. Информационное обеспечение уголовного процесса: дис. … канд. юрид. наук. Омск: 2002. 207 с.

6. Матвеев А. В. Ознакомление с материалами уголовного дела в уголовном судопроизводстве России: автореф. дис. … канд. юрид. наук. М., 2009. 25 с.

7. Рагулин А. В. Право адвоката-защитника на ознакомление с материалами уголовного дела после завершения предварительного расследования: проблемные вопросы регламентации и практической реализации // Адвокат. 2012. № 4. С. 19–20.

8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: http:///www.consultant.ru/document/cons_doc_LAW_61798

9. Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 г. № 295-З [принят Палатой представителей 24 июня 1999 г.: одобрен Советом Республики 30 июня 1999 г.] // Национальный правовой Интернет-портал Республики Беларусь, 26.07.2022, 2/2919. URL: https://etalonline.by/document/?regnum=hk9900295

10. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой; МГЮА им. О. Е. Кутафина. М.: Проспект, 2021. 640 с.

11. Чепкова Т., Лиходей Е. Что такое технология распределенного реестра [Электронный ресурс]. СПС «КонсультантПлюс». URL: https:// beincrypto.ru/learn/chto-takoe-tehnologiyaraspredelennogoreestra

12. Юрьев С. С., Короткова П. Е. Институциональные аспекты обеспечения права на ознакомление с материалами уголовного дела // Евразийская адвокатура. 2021. № 3 (51). С. 41–46.

13. Technology and Development in the Third Industrial Revolution; ed. by R. Kaplinsky and Ch. Cooper. London: Frank Cass. 2005. 109 p. (In Eng.).

14. Воронов Д. А. Электронное информирование участников процесса в досудебном производстве // Уголовный процесс. 2020. № 4 (184). С. 88–94.

Р. Р. Мусина,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова
Я. О. Шишиморова,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

СБЫТ ЦИФРОВОЙ ИНФОРМАЦИИ, ДОБЫТОЙ ПРЕСТУПНЫМ ПУТЕМ, ДЛЯ СОВЕРШЕНИЯ ДЕЙСТВИЙ ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА

Аннотация. В статье рассмотрена проблема сбыта цифровой информации, добытой преступным путем, в целях совершения актов терроризма. Приведены статистические данные о получении цифровой информации, которая была добыта преступным путем, а также обозначены некоторые проблемы, существующие в уголовном законодательстве России, и пути их решения.

Ключевые слова: право, цифровые технологии, информация, терроризм, акт терроризма, государственная тайна, экстремизм

SALES OF DIGITAL INFORMATION OBTAINED BY CRIME TO PERFORM TERRORISM ACTIONS

Abstract. The article deals with the problem of marketing digital information, obtained by criminal means, for the commission of actions for the commission of acts of terrorism. Brief statistics related to obtaining digital information that was obtained by criminal means are given, as well as the problems existing in the criminal legislation of the Russian Federation and ways to solve them.

Keywords: law, digital technologies, information, terrorism, act of terrorism, state secret, extremism

В цифровые технологии, в том числе и информацию, погружено современное общество практически всегда: обмен данными по сети Интернет, во время работы за носителями такой информации, при использовании путей передачи данных с использованием беспроводных каналов связи и т. д. Век цифровых технологий нельзя представить без постоянного обмена цифровой информацией по всем возможным видам связи в силу того, что в настоящий момент ее хранение, распространение и передача затрагивают большинство сфер жизни общества.

Стоит отметить, что часть такой информации является объектом государственной и политической деятельности, исходя из чего она автоматически становится объектом преступных посягательств, привлекая злоумышленников в качестве рычага давления на нынешний политический строй, а также на представителей государственного управления и представителей политических структур. Мотив подобных преступных действий можно объяснить следующими причинами: путем шантажа, выведения общества из привычного строя, введение в заблуждение определенных более уязвимых слоев населения Российской Федерации,

злоумышленники вполне добиваются своей цели. В РФ такая деятельность является уголовно-наказуемой и именуется такими терминами, как «экстремизм» и «терроризм» в зависимости от квалифицирующих факторов.

В 2018 г. зарегистрировано 2263 случая утечек конфиденциальной информации из организаций, 22,8 % которых составляли утечки из государственных организаций. От общего числа всех зафиксированных случаев 5,4 % являются данными, охраняемыми государственной тайной. Стоит уточнить, что данная статистика касается всего мирового сообщества. Обратимся к статистике, предоставленной аналитическим центром InfoWatch за 2022 г., которая рассматривает случаи, связанные только с территорией нашей страны. Согласно ей, количество утечек, произошедших на территории Российской Федерации, составило 710 случаев, что в два раза превысило статистику 2021 г. Касаемо утечек, непосредственно связанных с государственными и силовыми структурами, стоит уточнить что от общего количества их процент составил 10,5, процент утечек из муниципальных учреждений – 3,6. [2]. Большинство вышеупомянутых утечек объединяет понятие «государственная тайна».

Рассмотрим понятие «государственная тайна» и разберемся, в чем заключается опасность ее утечки. Верховный Суд Российской Федерации дает следующее понятие: «Государственная тайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». Ключевыми словами, взятыми из вышеуказанного термина, являются «распространение которых может нанести ущерб безопасности Российской Федерации». Это означает, что утечка такой информации может повлечь за собой нарушение целостности территории России, массовые беспорядки, может встать вопрос о правомерности действий органов власти и силовых структур под призмой навязанного мнения со стороны, нарушение экономики страны и т. д.

Все вышеперечисленное подпадает под цели совершения действий террористического характера, в том числе связанных со сферой информационных технологий. Информационный терроризм как социально политическое явление является серьезной угрозой безопасности общества и государства в целом. Такой вид терроризма способен провоцировать кризис стран с высоким информационным развитием. На данный момент для преступников не составляет сложности найти уязвимое место в абсолютно любом средстве обработки, хранения и передачи той или иной информации. При соответствующих навыках и знаниях злоумышленник может проникать в любые электронные носители данных [1].

Терроризм (информационный терроризм) является видом экстремистской деятельности. Из вышенаписанного можно сделать вывод о том, что мы рассматриваем следующий вид терроризма. Политический терроризм включает в себя крайние взгляды на политические вопросы, часто вплоть до пропаганды насилия или других незаконных средств для достижения этих взглядов. Примеры включают крайне правые и крайне левые группы, такие как неонацисты и анархисты. Согласно ст. 280.3 УК РФ от 14 июля 2022 г., к числу актов экстремизма причислили

дискредитацию действий Вооруженных Сил РФ [4]. В дополнение хочется уточнить, что к традиционным методам совершения актов политического терроризма добавились еще и методы информационного давления на общество внутри страны, благодаря которым эффект совершения преступного деяния только усиливается.

В «цифровом обществе» реальную опасность могут представлять не только хорошо организованные и сплоченные террористические организации, но и прежде никому не известные малочисленные группы маргиналов или даже террористов-одиночек («индивидуальный терроризм»), которые появляются внезапно непосредственно перед нанесением удара и стремительно исчезают после него [3].

Главной проблемой информационного политического терроризма является тот факт, что не всегда есть возможность отследить лицо или группу лиц, которое либо сбывает информацию, заведомо полученную для совершения действий террористического характера, либо то лицо или группу лиц, которое совершает акт терроризма.

Проблемой же уголовного законодательства России в данной сфере является тот факт, что сфера информационных и компьютерных технологий крайне поверхностно урегулирована. В уголовном кодексе отсутствуют понятия «цифровые технологии», «компьютерные средства», в том числе акты терроризма с использованием цифровых технологий, в принципе, не урегулированы. Ни в тексте 205 статьи УК РФ, которая напрямую регулирует акты терроризма в стране, ни в примечании к ней нет упоминания о вышесказанном деянии с использованием средств, техник, методов и знаний, непосредственно связанных с информационной сферой. В УК РФ в принципе отсутствуют статьи, регулирующие кражу информации путем хакерского взлома носителей цифровой информации для дальнейшего ее использования в преступных умыслах. Этот факт и прогресс в сфере цифровых технологий требуют усовершенствования уголовного законодательства России в целом.

Также с учетом факта, что в настоящий момент происходит утечка данных, которые являются государственной тайной, свидетельствует о том, что система безопасности, которая призвана защищать от этих «утечек», требует усовершенствования.

Если урегулировать эти два вышеуказанных факта, статистика 2022 г. которая была изложена выше, с большей вероятностью способна сократиться в разы в последующие годы. Классические виды актов терроризма каждый год пополняются, преступление идет в ногу со временем, прогрессом и обществом. Вопрос, касающийся информационного терроризма, затрагивает не только Российскую Федерацию, но и весь мир в целом. Вопрос урегулирования информационной среды требует своевременного вмешательства. При четком вмешательстве большую часть таких преступлений можно предупредить.

Список литературы

1. Бегишев И. Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем // Актуальные проблемы экономики и права. 2010. № 1. С. 123–126. EDN KZBXMD.

2. INFOWATCH Утечки информации ограниченного доступа в России за 2022 год. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god

3. Большаков А. Г. Феномен политического терроризма в эпоху информационно-цифровой революции в современном обществе // Научный журнал Политическая наука. 2018. № 4. С. 102.

4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: consultant.ru/document/cons-doc-LAW-10699

Р. Р. Мусина,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова
Р. Э. Гильманов,
магистрант,
Казанский инновационный университет имени В. Г. Тимирясова
А. А. Собровина,
студент,
Казанский инновационный университет имени В. Г. Тимирясова

ЖЕСТОКОЕ ОБРАЩЕНИЕ С ЖИВОТНЫМИ И ЕГО ОСОБЕННОСТИ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИНТЕРНЕТА В ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ СТРАН И РОССИИ

Аннотация. Факты жестокого обращения с животными всегда вызывают широкий общественный резонанс. В последнее время такая ситуация стала еще более вопиющей, так как виновные в данном преступлении зачастую не только издеваются над беззащитными животными, но и снимают это на телефон, а позже выкладывают в Интернет, либо сразу ведут прямой эфир (стрим), когда причиняют мучения животным за определенное вознаграждение (донацию или донаты). Исследование посвящено анализу квалифицирующего признака состава преступления – жестокого обращения с животными, совершенное с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет») – и его соотношения с положениями зарубежного законодательства.

Ключевые слова: жестокое обращение с животными, интернет-технологии, защита домашних животных, домашнее животное

CRUELTY TO ANIMALS AND ITS FEATURES IN CONNECTION WITH THE USE OF THE INTERNET IN THE LEGISLATION OF FOREIGN COUNTRIES AND RUSSIA

Abstract. The facts of cruelty to animals always cause a wide public response. Recently, this situation has become even more egregious, since the perpetrators of this crime often not only mock a defenseless animal, but also shoot it on the phone, and later post it on the Internet, or immediately conduct a live broadcast (stream) when they inflict torment on an animal for a certain reward (donation or donations).

In 2017, a new qualifying feature was fixed in the Criminal Code of the Russian Federation – cruelty to animals committed … with a public demonstration, including in the mass media or information and telecommunications networks (including the Internet) (paragraph «d» of Part 2 of Article 245 of the Criminal Code). Our research is devoted to the analysis of this qualifying feature and its correlation with the provisions of foreign legislation.

Keywords: animal cruelty, Internet technologies, protection of pets, pet

Введение. В разных странах мира существуют законы, регулирующие отношения между людьми и домашними животными. Они защищают животных от жестокого обращения со стороны людей, определяют ответственность за нарушение правил содержания и ухода за животными, а также устанавливают санкции за преступления, связанные с домашними животными. Вопросы взаимоотношения человека и животного в современных реалиях уже перестали быть просто рассуждениями о нравственных началах деятельности человечества. В настоящее время противодействие жестокости по отношению к животным стало серьезным фактором общественной, политической и экономической жизни многих стран. Анализ ряда нормативных актов зарубежных стран свидетельствует о том, что противодействие ненадлежащему обращению с животными является весьма важной проблемой современного общества [1].

Некоторые преступления, связанные с домашними животными, могут быть квалифицированы как преступления против собственности [2]. Например, кража домашнего животного может быть рассмотрена как кража личной собственности, а порча имущества животного – как порча имущества владельца. При этом при причинении вреда животному или при жестоком с ним обращении могут использоваться информационно-телекоммуникационные технологии (сеть «Интернет») с целью продемонстрировать мучения животному либо получить за демонстрацию причинения животному мучений и страданий денежное вознаграждение.

Основная часть. Животные в Великобритании защищаются законодательством, которое распространяется на любое животное, будь то домашние животные, дикие или скот. Однако это не всегда было так. Согласно Европейской Конвенции по защите домашних животных, «под домашним животным» подразумевается любое животное, которое содержит или собирается завести человек, в частности, в его домашнее хозяйство, для собственного удовольствия и дружеского общения» [3]. А вот дикими животными являются уже животные, не выступающие для человека объектом каких-либо правоотношений. Но, несмотря на данное различие, все животные, вне зависимости от их статуса, защищаются законодательством. В прошлом животные в Великобритании были рассматриваемы как собственность, и кража или убийство животного рассматривалась исключительно как преступление против его владельца.

Однако в настоящее время животные имеют свойственные им личностные черты и их права защищены. Так, например, в 2006 г. Великобритания приняла Закон о защите животных, которое запрещает жестокое обращение с животными, включая убийство, мучение и жестокое обращение, а также заставление животного участвовать в забавных соревнованиях или при выступлениях. Хотя нужно отметить, что в социальных сетях видеозарисовки со смешными видео животных собирают огромное количество «лайков» и комментариев.

Значительным шагом вперед мы считаем то, что Закон Великобритании о защите животных (2006) [4] признал, что звери могут чувствовать боль и страдания. Кроме того, в настоящее время в Великобритании существуют и другие законы, охраняющие животных. Например, кража животных может быть наказана в соответствии с Законом о краже 1968 г. Сохранение диких животных, находящихся под защитой, регулируется Законом о диких животных и сельском хозяйстве 1981 г.

Южная Корея имеет довольно продвинутое законодательство, которое регулирует обращение с животными. В 2018 г. был принят закон об укреплении защиты прав животных, который запрещает жестокое обращение с животными, а также содержание животных для производства шерсти, кожи и мяса без должных условий по их уходу и защите их прав.

Действующий закон Южной Кореи о защите животных гласит, что любой, кто жестоко обращается с животными, может быть приговорен максимум к трем годам тюремного заключения или штрафу в размере около 25 тысяч долларов. Однако до настоящего момента животные приравнивались к вещам, которые принадлежат их хозяевам. Другие ключевые положения этого закона включают запрет на продажу и использование собак, выращенных для производства мяса, запрет на охоту на диких животных, защиту домашних животных и защиту животных в экспериментах на животных. Основанием для изменения законодательства о защите животных стала статистика, которая свидетельствует, что число случаев жестокого обращения с животными в Южной Корее увеличилось с 69 в 2010 г. до 914 в 2019 г.

Закон о защите животных также обязывает владельцев заботиться об их домашних животных и предоставлять им необходимую еду, воду, медицинскую помощь и укрытие. Владельцы не имеют права оставлять животных без присмотра на длительное время.

Южная Корея известна своей традицией употребления собак в качестве пищевого продукта, что приводит к несправедливому и жестокому обращению с животными. Кроме того, в Южной Корее существует культурное убеждение, что собаки, над которыми поиздевались, имеют лучший вкус, что оправдывает жестокое обращение с ними. На улицах Южной Кореи, как часто сообщают СМИ, можно увидеть продажу животных, включая собак и кошек, которые выращены нелегально, для корыстных целей. Многие из них находятся в плохих условиях содержания, а некоторые даже находятся в тяжелом состоянии здоровья. Достаточно популярным видом развлечений в Южной Корее являются собачьи бои, где животные в ходе ожесточенной битвы могут быть жестоко изуродованы. Правительство Южной Кореи принимает меры для борьбы с этой проблемой, но в целом ситуация все еще остается неудовлетворительной.

Законодательство Японии в данной области можно считать одним из самых перспективных, так как Япония является одной из успешно развивающихся стран. В Японии действует национальный закон защите животных с 1973 г. «О благосостоянии и содержании животных», который предусматривает наказание за убийство, ранение и жесткое обращение с ними без уважительной на то причины, также данный закон возлагает обязанность на владельцев защищать их и воспитывать.

Закон берет под защиту таких животных, как крупный рогатый скот, кроликов, кур, лошадей, свиней, голубей, собак, кошек, других животных, которые являются

млекопитающими. В данной стране, так же как и у нас, спорен вопрос на тот счет, являются ли земноводные, рыбы, змеи, черепахи, животными, которых должен охранять закон. Наказание за убийство или причинение вреда здоровью животных перечисленной категории – это штраф или тюремное заключение на срок, зависящий от тяжести преступного деяния.

Жестокость по отношению к животным в Японии является серьезной проблемой, однако правительство Японии принимает меры для защиты животных и преследования жестоких деяний. Закон обязывает владельцев животных, обеспечивать им достойные условия жизни, а также при обнаружении факта жестокого обращения с животными, со стороны других лиц, обязывает их сообщить о преступлении правозащитным органам [5]. Все же существует определенный ряд проблем в законодательстве данной страны в отношении животных. Будущее защиты животных в Японии выглядит недостаточно определенным, но все же в последнее время наблюдается повышенный интерес к этой проблеме со стороны общества и СМИ в Японии.

Ситуация с жестоким обращением с животными в США сложна и разнообразна. В США умышленное уничтожение домашнего животного обычно квалифицируется как жестокое обращение с животными или бессмысленное убийство животных. Каждый штат имеет свой закон об этом, но во многих штатах наказание за жестокое обращение с животными может включать штрафы и тюремное заключение. В случае если животное принадлежит кому-то другому, убийство этого животного может также привести к гражданским искам за вред, причиненный владельцу.

В целом, ситуация в США может носить разнообразный характер, но в последние годы наблюдается улучшение осведомленности общественности и принятие мер для борьбы с жестоким обращением с животными.

Также хотелось бы рассмотреть законодательство Австралии, регулирующее данную проблему, так в стране существует закон «Prevention of cruelty to animals act» 1962 г., который переводится, как закон о предотвращении жестокого обращения с животными. Данный закон устанавливает минимальные стандарты по уходу и содержанию животных, а также предоставляет властям возможность привлечения к ответственности лиц, которые нарушают эти стандарты. И он распространяется на всех животных.

В Австралии кража животного также может быть квалифицирована как кража личной собственности и наказываться как уголовное преступление. Жестокое обращение с животными является проблемой в Австралии, как и во многих других странах.

Изучение зарубежного законодательства в области жестокого обращения с животными дает нам возможность констатировать отсутствие квалифицирующего признака «жестокое обращение с животными, совершенное … с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет») (п. «г» ч. 2 ст. 245 УК РФ). Можно прийти к выводу, что российское уголовное законодательство идет в ногу со временем, так как фиксируется постоянный рост количества распространения видеозаписей с фактами жестокого обращения с животными в социальных сетях.

Приведем пример: в 2020 г. в Карелии зафиксирована вспышка жестокого обращения с животными [6, 7], некоторые случаи даже стали нарицательными – на-

пример, так называемые «хабаровские живодерки» [8], мучавшие животных в 2016 г. (что во многом и инициировало редактирование ст. 245 УК РФ). Нужно отметить и положительную роль СМИ, именно опубликование в социальных сетях историй об искалеченных животных, которым требуется ветеринарная помощь, зачастую помогает собрать необходимые денежные средства для их лечения. Полагаем, что публичная демонстрация через СМИ или социальные сети в Интернете жестокого обращения с животными негативно влияет на морально-нравственное состояние общества [9, 10, 11], особенно малолетних и несовершеннолетних, и может способствовать формированию жестокости в поведении лиц, просматривающих данный контент на постоянной основе.

Выводы и предложения. Таким образом, в различных странах мира существуют разные законы, которые регулируют отношения между людьми и домашними животными и устанавливают санкции за нарушение этих правил. Преступления, связанные с домашними животными, могут быть квалифицированы либо как преступления против собственности, либо как преступления против животных, в зависимости от конкретных обстоятельств дела и закона, действующего в данной стране. Несомненным плюсом российского уголовного закона является выделение пункта «жестокое обращение с животными, совершенное … с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет») (п. «г» ч. 2 ст. 245 УК РФ). Полагаем, что положительный опыт применения данного законодательного уточнения уголовной ответственности может быть применен и в зарубежном уголовном праве.

Считаем, что эффективным средством противодействия данным преступлениям будет мониторинг социальных сетей, а равно создание бота, которому можно пожаловаться на жестокий контент конкретной социальной сети или страницы в сети Интернет.

Список литературы

1. Мирошниченко В. С. Жестокое обращение с животными: уголовно-правовые и криминологические аспекты: автореф. дис. … канд. юрид. наук: 12.00.08 / Мирошниченко В. С. М., 2013. 29 с.

2. Латыпова Э. Ю. О способах мошенничества, совершенного в отношении домашних животных // Образование, воспитание и право в контексте глобальных вызовов: сб. материалов Междунар. науч.-практ. конф., Чебоксары, 21–22 апреля 2023 г. / Чуваш. гос. ун-т им. И. Н. Ульянова. Чебоксары, 2023. С. 439–444.

3. Европейская Конвенция по защите домашних животных. Редакци. ноябрь 19. № 125 Серии Европейских Договоров. Преамбула.

4. Animal Welfare Act 2006. 08.11.2006.

5. Лебедева П. Почему вам не стоит покупать домашнее животное в Японии 05.07.2019. URL: https://konnichiwa.ru/3249

6. Как мы издевались над животными в 2020 году (пока полиция Карелии игнорирует дел о жестоком обращении). URL: https://gubdaily.ru/article/respublika/kak-my-izdevalis-nad-zhivotnymi-v-2020-godu-poka-policiya-karelii-ignoriruet-dela-o-zhestokom-obrashhenii

7. Хуже зверей. 10 историй о живодерах и их жертвах. URL: https://staryiy.livejournal.com/874187.html

8. Хабаровские живодерки: что стало с двумя девушками, которые истязали щенков на «заброшке» и снимали на видео // Комсомольская правда. URL: https://www.hab.kp.ru/daily/27476.5/4683031

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

10. Латыпова Э. Ю. Принцип равенства и принцип гуманизма и их особенности в уголовном праве // Конституция Российской Федерации и развитие правовой системы государства: общетеоретические и отраслевые аспекты: материалы Международной научно-практической конференции. Казань: Отечество, 2019. С. 341–346.

11. Латыпова Э. Ю., Нечаева Е. В. Спорные вопросы содержания принципа гуманизма в уголовном праве // Вестник Казанского юридического института МВД России. 2019. № 3(37). С. 355–360.

Е. Д. Намысов,
заместитель начальника,
Карагандинская академия Министерства внутренних дел
Республики Казахстан имени Баримбека Бейсенова

МОШЕННИЧЕСТВО В ЦИФРОВОМ МИРЕ: АДАПТАЦИЯ К СОЦИАЛЬНЫМ ИЗМЕНЕНИЯМ

Аннотация. В статье описаны отдельные положения цифровых трансформационных преобразований, которые повлияли на рост мошенничества в Интернете. Согласно статистическим сведениям, в Республике Казахстан совершается большое количество преступлений в рассматриваемой сфере. Затрагиваемые аспекты являются частью общей системы, направленной на предотвращение и пресечение незаконного преступного поведения мошенников, использующих информационно-коммуникационные технологии. При совершении интернет-мошенничества, от которого чаще всего страдают простые люди, преступники используют различные тактики: фишинговые схемы, мошенничество с банковскими картами, поддельные сайты, вредоносное программное обеспечение, вирусы и многое другое.

Ключевые слова: противодействие, цифровизация, интернет-мошенничество, правоохранительная деятельность, информационно-телекоммуникационные технологии

FRAUD IN THE DIGITAL WORLD: ADAPTATION TO SOCIAL CHANGES

Abstract. This article describes some provisions of digital transformation transformations taking place in society now, which, among other things, influenced

the growth of fraud on the Internet. According to statistical data, a large number of crimes are committed in the Republic of Kazakhstan in this area. The aspects we have touched upon are part of a general system aimed at preventing and suppressing the illegal criminal behavior of fraudsters using information and communication technologies. When committing Internet fraud, which ordinary people most often suffer from, criminals use various tactics: phishing schemes, bank card fraud, fake websites, malicious software, viruses and much more.

Keywords: counteraction, digitalization, Internet fraud, law enforcement, information and telecommunication technologies

Введение. Под воздействием цифровых технологий, которые являются частью технологической сферы общества, создается новая экономическая и социальная реальность, но трудности, с которыми сталкивается новейшая индустриальная цивилизация, сложно переоценить. Мы говорим о смене глобального социотехнического порядка, который приведет к полному переформатированию привычных нам систем и выработке новых социально-экономических стратегий.

Как следствие, в последние годы вместе с развитием интернет-технологий растет и число случаев мошенничества в Интернете. Развитие цифровых коммуникаций дало мошенникам новые способы достижения своих коварных целей. Фишинг, онлайновые рынки, мошенничество в социальных сетях – вот лишь некоторые из многочисленных видов мошенничества в Интернете. Очень важно разработать эффективные стратегии борьбы с интернет-мошенничеством. Из-за мошеннических схем предприятия, население и государственные организации подвергаются серьезному риску нарушения безопасности и финансовых потерь. Мошенничество в Интернете может также привести к утечке данных, нарушению конфиденциальности и даже оказать влияние на политическую ситуацию в стране.

Основная часть. Республика Казахстан в течение последних нескольких лет активно развивает цифровые технологии. Государственные органы и коммерческие компании совместно работают над созданием благоприятной среды для развития передовых технологий, цифровой инфраструктуры и инновационных проектов. В стране создаются специализированные технопарки и инновационные центры, которые помогают молодым предпринимателям и исследователям в области инноваций и стартапов. Это стимулирует создание новых технологий и привлекает капитал в высокотехнологичный сектор, что, в конечном итоге, приводит к цифровой общественной трансформации.

Определение готовности общества к происходящей цифровой трансформации и ее основных целей является жизненно важным, поскольку динамичные процессы цифровой трансформации требуют эффективного реагирования на новые проблемы и обстоятельства адаптивного цифрового развития. В связи с этим на государственные организации возлагаются следующие обязанности: анализ текущего состояния цифрового поведения пользователей; определение готовности общества к дальнейшей цифровой трансформации; поддержка приоритетов нового цифрового развития; выявление причин, ограничений, барьеров и опасностей, препятствующих ускорению цифровой трансформации. Под влиянием цифровизации меняются все экономические процессы: от массового производства и массового потребления

до новых производств по созданию товаров со специфическими характеристиками для каждого потребителя, в том числе пользователей через сети Интернет.

Новые модели поведения пользователей формируются одновременно с изменением технической парадигмы, моделей управления, общественных устоев, значительными демографическими сдвигами и другими событиями, моделирующими поведение экономических игроков на рынке предоставления услуг.

Интеграция современных технологий и цифровых решений приобретает все большее значение для успеха и конкурентоспособности современных организаций и государств, что способствует экономическому росту. Экономическое развитие и современные технологии, по мнению А. Б. Воронкевича, тесно взаимосвязаны. Современное состояние экономики благоприятствует инвестициям в технологии: развитые страны ищут инновационные методы снижения затрат и стимулирования инноваций, а развивающиеся экономики увеличивают спрос на технологии для стимулирования роста [1. С. 15]. В свою очередь О. И. Попова добавляет, поскольку цифровые технологии повышают потребительский спрос, это создает благоприятные условия для социально-экономического расширения экономики [2. С. 123]. Т. Ф. Кузнецова отмечает, что третья волна капитализма была вызвана Интернетом и меняет многие стороны глобального рынка, от поведения потребителей до новых моделей компаний. Этот скачок, происходящий как в развитых, так и в развивающихся странах, обусловлен мобильностью, облачными вычислениями, бизнес-аналитикой и социальными сетями [3. С. 98]. В центре всей этой цепочки находится пользователь – человек. Развивающиеся платформы находятся в центре стратегии роста компаний в связи с быстрым экономическим, демографическим и доходным ростом.

Несмотря на все преимущества, которые дает обществу цифровая трансформация, важно помнить, что она несет в себе и новые опасности, связанные с ростом мошенничества в Интернете. Доступность интернет-сервисов и цифровых технологий делает людей и предприятия более восприимчивыми к кибератакам. Финансовые потери, связанные с мошенничеством, влияют на потребительские расходы, инвестиции и репутацию. Для обеспечения безопасности, доверия и устойчивости цифровой экономики развитие кибербезопасности становится все более важным компонентом цифровой трансформации.

Согласно статистическим сведениям по итогам 2020 г., в Республике Казахстан количество зарегистрированных мошенничеств составило 33 759, из них 14 220 интернет-мошенничеств. За 12 месяцев 2021 г. количество зарегистрированных мошенничеств составило 41 083, из них 21 405 интернет-мошенничества. За аналогичный период 2022 г. в Республике Казахстан количество зарегистрированных мошенничеств составило 43 499, из них 20 569 интернет-мошенничеств. За 6 месяцев 2023 г. количество зарегистрированных мошенничеств в стране составило 20 518, из них 9 545 интернет-мошенничества [4] (рис. 1).

По данным статистики, в период с 2020 г. по первое полугодие 2023 г. в Республике Казахстан наблюдался рост числа зарегистрированных уголовных дел о мошенничествах. Значительная часть зарегистрированных преступлений связана с мошенничеством в Интернете. Полученные данные свидетельствуют о необходимости усиления мер кибербезопасности и защиты пользователей от интернет-мошенничества для обеспечения устойчивого роста цифровой экономики и защиты интересов физических и юридических лиц.

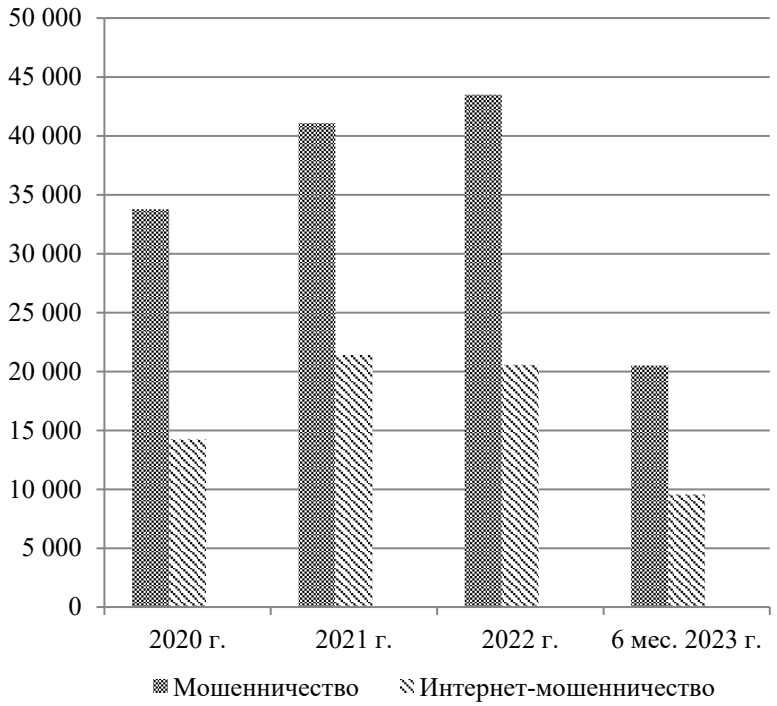


Рис. 1. Сведения о зарегистрированных мошенничествах и интернет-мошенничествах с 2020 г. по 6 месяцев 2023 г.

Следовательно, можно прийти к выводу о том, что число совершаемых интернет-мошеничеств растет пропорционально развитию информационно-телекоммуникационных технологий в стране. В результате наблюдаются высокая степень и постоянный рост цифровизации. По уровню развития электронного правительства Республика Казахстан в этом году заняла 28-е место из 193 стран, по сравнению с 29-м местом в 2020 г. Индекс развития (E-Government Development Index, EGDI) в целом по стране составил 0,86 п. [5].

С течением времени технологии развиваются, что в том числе позволяет совершенствоваться преступным процессам, связанным с использованием Интернета. Но не только развитие компьютерных технологий является причиной этого. С криминологической точки зрения это можно объяснить ростом профессионализма самого преступника. Создав определенный профиль своего противоправного поведения в Интернете, преступник фактически усиливает его. Социальные сети, форумы, чаты и другие формы сетевого общения не только позволяют систематически совершать тот или иной вид преступлений, но и способствуют изменению профиля преступной деятельности и усложнению механизмов ее осуществления.

Первое правило технологии М. Кратцберга, которое гласит, что «Технология сама по себе не является ни хорошей, ни плохой, но и нейтральной ее назвать нельзя» [6], было сформулировано исследователем в результате изучения эволюции технологий и их взаимодействия с социокультурными процессами. Действительно, результаты использования новых технологий зависят от того, какую цель преследует данная тема. Однако развитие образа жизни, морали, институтов и других

аспектов современного общества все больше подвергается влиянию технологий. Таким образом, киберпространство из простого технического средства передачи информации превратилось в значимое социальное явление, связанное с коммуникативным аспектом интернет-технологий.

Средства коммуникации в информационном пространстве, включая электронную почту, skype, чаты, форумы, вебинары, видеоконференции и социальные сети, используются для установления связей с большими группами населения, влияния на них или взаимодействия с ними, а также для распространения информации. Доступ пользователей к информационному пространству может осуществляться одним из двух способов:

– онлайн, что позволяет использовать сеть в режиме реального времени;

– офлайн, когда задачи готовятся для сети заранее, а подключение требуется только для передачи или приема подготовленных данных.

Участники коммуникации в информационном пространстве взаимодействуют друг с другом по разным причинам:

– деловым (получение или предоставление услуг, ведение бизнеса);

– коммуникационным (общение с единомышленниками);

– познавательным (получение образования);

– развлекательным (интерактивные игры, просмотр телепередач) и т. д.

Информационное пространство выступает в роли заменителя реального, физического мира. Пользователи сетей являются также участниками социальных контактов, которые широко распространены в современном информационном обществе и привели к появлению социальных групп с заранее заданными характеристиками [7. С. 21].

Киберпространство становится все более сложным и разнообразным в связи с ростом числа пользователей Интернета и быстрым развитием информационных технологий. В современном информационном обществе люди активно участвуют в онлайн-коммуникациях, общаются в социальных сетях, используют онлайн-платформы, электронную коммерцию, финансовые операции и многое другое. Вместе с этим растет и число случаев мошенничества в Интернете.

Преступники, использующие Интернет, постоянно пытаются воспользоваться новыми возможностями, которые он предоставляет, в своих корыстных целях. Они постоянно выявляют недостатки и пробелы в системах онлайновых платежей, протоколах безопасности, поведении пользователей и их доверии. Злоумышленники становятся все умнее и изобретательнее по мере развития Интернета и информационных технологий.

В настоящее время преступники имеют доступ к специальным инструментам для мошенничества и обмана в Интернете. Они создают фальшивые сайты, выдают себя за надежные компании, рассылают фишинговые письма и сообщения, размещают вредоносные программы и многое другое. Они обманывают своих жертв, умело маскируясь и используя современные технологии. Многие пользователи Интернета попадаются на удочку мошенников, особенно те, кто не обладает достаточными навыками и знаниями в области кибербезопасности. Преступники могут обмануть человека, выдавая его за друга, родственника или представителя законной организации,

и вымогать деньги или частную информацию. Иногда жертвы мошенничества не понимают, что их обманули, до тех пор, пока не наступают неприятные последствия.

Также существует риск утечки персональных данных, преступники имеют возможность получить доступ к конфиденциальным данным, включая пароли, номера кредитных карт, личную информацию и финансовые данные, что может привести к финансовым потерям и нарушению безопасности.

Киберпреступность распространяется по всему миру благодаря широкому распространению Интернета, что затрудняет борьбу с ней правоохранительных органов. Хотя существует несколько способов борьбы с мошенничеством в Интернете, включая повышение уровня кибербезопасности, обучение пользователей и сотрудничество правоохранительных органов, каждый пользователь также несет ответственность за защиту себя и своих данных в Интернете. Чтобы не стать жертвой киберпреступников, необходимо проявлять осторожность, быть бдительными и знать о потенциальных опасностях.

Заключение. Таким образом, благодаря информационному веку и Интернету у нас появилось множество возможностей для общения, учебы, работы, развлечений и расширения кругозора. Однако эти преимущества сопровождаются растущим числом мошенничеств в Интернете. Осознание того, что каждый из нас, пользователей Интернета, сам отвечает за свою кибербезопасность, имеет огромное значение. Очень важно быть внимательным и осторожным при работе в Интернете, не доверять сомнительным или ненадежным источникам, следить за защитой своих финансовых средств и личной информации.

Разумеется, общество и правоохранительные органы должны активно участвовать в борьбе с интернет-мошенничеством, усиливая меры кибербезопасности и сотрудничая по всему миру. В условиях информационного общества использование Интернета и других цифровых технологий должно быть более продуманным. Мы можем воспользоваться преимуществами информационного века и снизить опасность киберпреступлений, выбрав правильную стратегию дальнейшего развития. Мы можем сделать Интернет безопасной и полезной средой для всех, только работая вместе, сотрудничая и будучи ответственными пользователями.

Список литературы

1. Воронкевич, А. Б. Изменение особенностей потребительского поведения на рынке товаров массового потребления под влиянием цифровизации в России // Практический маркетинг. 2020. № 7 (281). С. 10–18.

2. Попова, О. И. Влияние цифровизации на потребительское поведение и развитие СМИ // Знак: проблемное поле медиаобразования. 2020. № 3 (37). С. 121–126.

3. Кузнецова, Т. Ф. Цифровизация и цифровая культура // Горизонты гуманитарного знания. 2019. № 2. С. 96–102.

4. Основные показатели органов уголовного преследования: аналитический обзор // Официальный сайт Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Информационный сервис. URL: https://www.qamqor.gov.kz

5. Какое место занимает Казахстан в международном рейтинге по развитию электронного правительства. URL: https://elorda.info/ru/ekonomika/23550–1666159896

6. James R. Hansen Technology and the History of Aeronautics: An Essay. URL: http://www.centennialofflight.net/essay/ Evolution_of_Technology/Tech-OV1.htm
7. Самойленко О. А. Основные методики расследования преступлений, совершенных в киберпространстве: монография. Одесса: ТЭС, 2020. 372 с.

И. Э. Никитина,
доктор юридических наук, профессор,
Российский университет транспорта (МИИТ),
главный научный сотрудник,
Российский федеральный центр судебной экспертизы
при Министерстве юстиции Российской Федерации

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ПРЕИМУЩЕСТВО ИЛИ ВЫЗОВ?

Аннотация. В статье рассмотрены проблемы, связанные с использованием современных информационно-коммуникационных технологий в уголовном судопроизводстве. В качестве преимущества внедрения указанных технологий в уголовное судопроизводство часто упоминается оптимизация процесса раскрытия и расследования преступлений за счет повышения эффективности работы с информацией (ее поиском, сбором, хранением, обработкой, предоставлением и использованием). С другой стороны, обеспокоенность вызывает уровень достоверности, проверяемости и обоснованности результатов, полученных с использованием технологии искусственного интеллекта. Все чаще на повестку дня выносится обоснованное предложение о «приостановке» внедрения искусственного интеллекта в наиболее уязвимые области жизнедеятельности человечества, для осмысления и прогнозирования возможных вызовов в будущем.

Ключевые слова: информационно-коммуникационные технологии, искусственный интеллект и право, искусственный интеллект, права человека, алгоритмы, программный код, машинное обучение

THE USE OF ICT IN CRIMINAL JUSTICE: AN ADVANTAGE OR A CHALLENGE?

Abstract. The paper considers the advantages and disadvantages of using modern ICT in criminal proceedings. Information and communication technologies make it possible to optimize the process of detecting and investigating crimes by increasing the efficiency of working with information (its search, collection, storage, processing, provision and use). Questions are raised by the level of reliability, verifiability and validity of the results obtained using AI systems.

Keywords: Information and communication technologies, artificial intelligence and law, artificial intelligence; human rights; algorithms; program code; machine learning

Введение. Без современных информационно-коммуникационных технологий (далее – ИКТ) сегодня уже трудно представить многие сферы жизнедеятельности общества и государства. ИКТ позволяют оптимизировать процесс раскрытия и расследования преступлений за счет повышения эффективности работы с информацией (ее поиском, сбором, хранением, обработкой, предоставлением и использованием) [1].

Возможно, в ближайшем будущем роботы смогут выполнять базовые правоохранительные функции. Искусственный интеллект (далее – ИИ) в состоянии обеспечить мониторинг потоков видеоданных с уличных камер видеонаблюдений и вовремя предупредить соответствующие службы о подозрительной активности на подконтрольной им территории. И это далеко неполная интеграция современных сетей видеонаблюдения. Возможен их синтез с программами поиска изображений, параллельной проверкой информации о подозрительных лицах в доступных базах данных и оперативно-справочных картотеках. Экспертами разработано их ранжирование по заранее заданным показателям. Сегодня правоохранительные органы используют роботов для проведений обысков и спасательных операций [2], для обезвреживания взрывных устройств [3] и даже для ликвидации вооруженных преступников [4].

Преимущества от внедрения ИКТ в управленческие процессы обеспечения общественной безопасности и осуществления уголовного преследования в большей части подтверждаются отечественной и зарубежной правоприменительной практикой [1].

Так, мониторинг, проводимый Национальным институтом правосудия США (National Institutes of Justice, NIJ) дал оптимистическую оценку потенциала применения ИКТ в уголовном судопроизводстве:

– для идентификации лиц, совершающих противоправные деяния в видеороликах;

– для выявления склонности лица, находящегося под надзором правоохранительных органов, к рецидиву преступлений;

– проведения ДНК экспертиз и исследований;

– анализа аудиофайлов стрельбы со смартфонов и смарт-устройств и т. п. [5].

Отечественные ученые выделяют следующие направления возможного использования ИКТ в уголовном судопроизводстве: 1) автоматизированные системы обработки данных; 2) автоматизированные информационно-поисковые системы; 3) автоматизированные информационно-справочные системы; 4) автоматизированные рабочие места; 5) автоматизированные системы управления; 6) экспертные (информационно-аналитические и рекомендующие) системы [1].

И. Н. Яковенко называет шесть направлений использования компьютерных технологий в расследовании и раскрытии преступлений: 1) автоматизированные системы управления и автоматизированные рабочие места; 2) информационно-справочные системы; 3) экспертно-консультирующие системы; 4) расчетно-аналитические системы; 5) информационные обучающие системы; 6) программы обработки изображений [1].

Тем не менее в ходе уголовного судопроизводства наиболее ощутимо ограничиваются основные права и свободы граждан. Поэтому, в первую очередь, обеспокоенность вызывает уровень достоверности, проверяемости и обоснованности

результатов, полученных с использованием технологии ИИ. Все чаще на повестку дня выносится обоснованное предложение о «приостановке» внедрения ИИ в наиболее уязвимые области жизнедеятельности человечества, для осмысления и прогнозирования возможных вызовов в будущем.

Основная часть. Одной из задач, представленной в рамках исследования, проанализировать, в каких направлениях деятельности правоохранительных органов применение ИКТ сможет оказывать серьезную поддержку в раскрытии и расследовании преступлений, а в каких, возможно, приведет к нарушению справедливости уголовного судопроизводства.

Таким образом, можно ли современные ИКТ, в частности искусственный интеллект, считать частью экосистемы уголовного правосудия?

Искусственный интеллект – это быстро развивающаяся область ИКТ. В середине 1950-х годов Джон Маккарти (John McCarthy), считающийся основателем указанной технологии, определил его как «науку и технику создания интеллектуальных машин».

Поскольку ИИ способен анализировать огромное количество данных, его можно использовать в расследовании преступлений и их предотвращении. Например, в противодействии торговле людьми, в частности с рекламой секс-услуг в Интернете. Каждое сообщение оставляет цифровой след. Безусловно, не во всех случаях его возможно отследить, но это больше связано с деятельностью на уровне спецслужб. Деятельность же непрофессионалов – криминальных элементов, эксперты могут отслеживать с помощью специальных алгоритмов. ИИ, обрабатывая входные данные, анализирует даже такие незначительные на первый взгляд детали, как рост арестов за мелкие кражи в районе, где рекламируются секс-услуги. Поскольку если кто-то стал жертвой торговли людьми и привезен из другого региона, его часто лишают доступа к базовым продуктам для нормальной жизни. ИИ способен отследить рост краж даже гигиенических средств, как зубная паста или мыло, сопоставив информацию с рекламируемыми секс-услугами.

Кроме того, использование ИИ применимо к обработке информации, касающейся снятия гостиничных номеров, оплаченных наличными в тех районах, где предоставляются или рекламируются сексуальные услуги во время крупных массовых мероприятий.

Анализируя подозрительные сообщения, правоохранительные органы применяют ИИ для установления связей между рекламой и ее авторами, обращая внимание на такие нюансы, как схожие стили написания текстов, определенные настройки, используемые более чем в одном объявлении, на веб-сайтах. Технологии машинного обучения для ИИ могут применяться не только для раскрытия преступлений против личности, но и других видов преступлений [6].

Кристофер Ригано (Christopher Rigano) определяет ИИ «как способность машины воспринимать окружающую среду и реагировать на нее независимо, выполняя задачи, которые обычно требуют человеческого интеллекта и процессов принятия решений, но без прямого вмешательства человека. Одной из граней человеческого интеллекта является способность учиться на собственном опыте. Машинное обучение – это приложение ИИ, которое имитирует эту способность и позволяет машинам и их программному обеспечению учиться на собственном опыте.

Он приходит к выводу о том, что ИИ может стать постоянной частью экосистемы уголовного правосудия, оказывая помощь в расследовании и позволяя специалистам в области уголовного правосудия обеспечивать общественный порядок и безопасность» [7].

Гарри Серден (Harry Surden) высказывает противоположную точку зрения на рациональность использования ИИ в уголовном судопроизводстве, поскольку, как показывает практика, «ИИ, не понимает смысл и значение шаблонов (тенденций, структурных особенностей и т. д.), как это понимают люди. Используя их, ИИ может формировать полезные и схожие с человеческими решения (результаты) по итогам обработки даже сложных задач. Но качество результатов деятельности ИИ напрямую зависит от массива обрабатываемых им данных» [7].

ИИ не понимает смысла понятий «справедливости или равенства всех перед законом», для него правильными будут любые решения, которые он принимает на основе полученной и обрабатываемой информации (с учетом того, как он запрограммирован). Следовательно, если в ходе обработки массива информации ИИ придет к выводу о том, что часть населения с определенными признаками (цвет кожи, расовая принадлежность, наличие правонарушений в прошлом и т. д.) подвергались задержаниям чаще других лиц, то и «машинный интеллект» будет считать, что именно такие лица более опасны для общества и рекомендовать органам полиции активнее патрулировать районы, где такие лица проживают или часто бывают. Соответственно, это приведет еще к большим задержаниям определенных слоев населения. Возникнет замкнутый круг [7].

Вопросы вызывает уровень достоверности, проверяемости и обоснованности результатов, полученных с применением систем ИИ.

Ж. Р. Темирбеков объясняет это тем, что программный код некоторых современных систем ИИ либо закрыт, либо крайне объемный и комплексный, либо предусматривает самоизменение и самомодернизацию, либо имеет место все вышеупомянутое вместе взятое. Это приводит к тому, что даже для экспертов в сфере ИИ сложно объяснить, каким именно образом и почему алгоритм системы ИИ выдал конкретный результат [7].

Так, в Нью-Йорке команда адвокатов подготовила исковое заявление в суд на авиакомпанию в интересах доверителя, которому были нанесены телесные повреждения. В приложенных к иску документах адвокаты привели прецеденты. Суд направил документы авиакомпании, а ответчики заявили, что некоторых дел не существует. «Шесть из представленных дел, похоже являются фиктивными судебными решениями с фиктивными цитатами и фиктивными внутренними ссылками», - написал судья в постановлении.

Выяснилось, что юрист с более чем 30-летним опытом работы использовал ChatGPT, чтобы найти судебную практику. Чат дважды подтвердил, что дела существуют. В Твиттере (заблокированна на территории Российской Федерации) появилась запись разговора между чат-ботом и адвокатом:

– да, Varghese v. China Southern Airlines Co LTD, 925 F.3d 1339 (11 th Cir. 2019) – это реальное дело, – ответил ChatGPT.

На вопрос юриста, каков источник, чат-бот отреагировал: «:Дело может быть найдено в справочных базах данных, таких как LexisNexis и WestLaw» [8].

С другой стороны, компания «Гарант» акцентирует внимание на решениях low-code и no-code, помогающих юристам использовать нейронные сети для анализа правовой информации и представляет разработанную аналитическую систему «Сутяжник».

Заключение. Так или иначе, ИИ оказывает и будет далее оказывать заметное воздействие на существующую правовую реальность. Хотя современный уровень «машинного интеллекта» значительно уступает возможностями человека, но давать прогнозы на будущее, сегодня довольно затруднительно.

Список литературы

1. Фролов В. В. Использование информационных технологий в расследовании: направления, проблемы и перспективы // Полицейская и следственная деятельность. 2023. № 2. С. 1–13. DOI: 10.25136/2409–7810.2023.2.40032 EDN: AOLZL. URL: https://nbpublish.com/library_read_article.php?id=40032

2. Dulles A. The Craft of Intelligence, 1963, Lyons Press; Reprint edition, May 1, 2016.

3. Goodman Marc. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016.

4. URL: www.cs.cmu.edu/afs/cs.cmu.edu/project/learn43/lib/photoz/.g/web/glossary/bayesnet.html

5. Erik Brynjolfsson and Andrew McAfee, “The Business of Artificial Intelligence: What It Ca. and Canno. Do for Your Organization,” Harvard Business Review (August 2017); and Giosué Lo Bosco and Mattia Antonino Di Gangi, “Deep Learning Architectures for DNA Sequence Classification,” Fuzzy Logic and Soft Computing Application. 2017: Revised Selected Papers From the 11th International Workshop, WILF 2016, Naples, Italy, December 19–21, 2016, eds. Alfredo Petrosino, Vincenzo Loia, and Witold Pedrycz (London: Springer Nature, 2018), 162–171, doi:10.1007/978–3–319–52962–2.

6. Radulov, Artificial intelligence and security. Security 4.0. URL: https://stumejournals.com/journals/confsec/2019/1/3.full.pdf

7. Темирбеков Ж. Р. Искусственный интеллект и право: краткий обзор // Право и государство. 2021. № 3(92). С. 142–156. DOI: 10.51634/2307–5201_2021_3_142.

8. ЕСПЧ навигатор. URL: https://echrnavigator.ru/

А. А. Нуждин,
кандидат юридических наук, доцент,
Академия Федеральной службы исполнения наказаний
Российской Федерации

ПРЕДУПРЕДИТЕЛЬНОЕ ЗНАЧЕНИЕ НАУЧНО-ТЕХНИЧЕСКОГО РАЗВИТИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Аннотация. Статья посвящена анализу научно-технического развития уголовно-исполнительной системы. Показано предупредительное значение цифровой трансформации учреждений и органов Федеральной службы исполнения наказаний. Приведены примеры использования современных информационно-коммуникацион-

ных технологий, искусственного интеллекта для предупреждения, прогнозирования пенитенциарных преступлений. Проанализированы нормативные документы стратегического планирования в области научно-технического развития уголовно-исполнительной системы. Сделан вывод о важности и необходимости проводимой политики в области цифровой трансформации.

Ключевые слова: научно-техническое развитие, цифровая трансформация, искусственный интеллект, предупреждение, преступление, расследование, уголовно-исполнительная система

PREVENTIVE VALUE OF SCIENTIFIC AND TECHNICAL DEVELOPMENT OF THE PENAL SYSTEM

Abstract. The article is devoted to the analysis of scientific and technical development of the penal system. The author tried to show the preventive value of the digital transformation of institutions and bodies of the Federal Penitentiary Service. Examples of the use of modern information and communication technologies, artificial intelligence for the prevention and prediction of penitentiary crimes are given. The normative documents of strategic planning in the field of scientific and technical development of the penal system are analyzed. The conclusion is made about the importance and necessity of the policy in the field of digital transformation.

Keywords: scientific and technical development, digital transformation, artificial intelligence, prevention, crime, investigation, penal enforcement system

Целями уголовно-исполнительного законодательства являются исправление осужденных и предупреждение совершения новых преступлений (как осужденными, так и иными лицами) [6]. Для реализации поставленных целей уже многие годы идет поиск тех сил и средств, которые позволят если не реализовать их, то приблизиться к их достижению. И если исправление осужденных является достаточно спорной категорией [3], то предупредить совершения новых преступлений вполне возможно.

В современном мире должны применяться и современные методы предупреждения преступности, в том числе в местах лишения свободы. В первую очередь речь идет об использовании цифровых технологий, искусственного интеллекта, научно-технического прогресса. В настоящее время в России ведется активная политика, направленная на цифровую трансформацию уголовно-исполнительной системы, цифровизацию всего общества.

На федеральном уровне принято много законов в сфере цифровой трансформации, утвержден ряд концепций и программ, избрано стратегическое направление в области цифровой трансформации государственного управления. Федеральная служба исполнения наказаний как федеральный орган исполнительной власти быстро отреагировало на изменения государственной политики в данной сфере, активно включилась в цифровизацию и научно-техническое развитие своей деятельности. Так, в конце 2020 г. был издан приказ Федеральной службы исполнения наказаний «Об утверждении ведомственной программы цифровой трансформации Федеральной

службы исполнения наказаний на 2021 г. и плановый период 2022 и 2023 гг.» (с изменениями на основании приказа ФСИН России от 22.10.2021 № 943) [4].

Основные результаты, которые должны быть достигнуты, по итогам реализации концепции действительно впечатляют. Их внедрение выведет деятельность уголовно-исполнительной системы на качественно новый уровень. По итогам программы должна быть создана единая информационная система ФСИН России; значительно сокращены временные затраты на получение и обработку юридически значимой информации от учреждений и органов уголовно-исполнительной системы для подготовки управленческих решений; сокращены временные затраты на получение и предоставление информации в рамках межведомственного информационного взаимодействия, в том числе с судебным департаментом при Верховном Суде Российской Федерации; 100 % исправительных колоний должны быть обеспечены возможностью проведения «мгновенного цифрового аудита» со стороны территориальных органов ФСИН России и центрального аппарата ФСИН России. С одной стороны, может показаться, что указанные выше изменения носят лишь организационный характер и напрямую не связаны с достижением цели предупреждения совершения новых преступлений в местах лишения свободы. Однако именно организация предупредительной деятельности играет решающую роль. Как будет осуществляться указанная деятельность, какой круг должностных лиц и органов будет в нее вовлечен, каков объем предоставляемых им полномочий, как данные должностные лица и органы взаимодействуют между собой – от этого будет зависеть конечный результат.

Документом стратегического планирования можно признать Концепцию развития уголовно-исполнительной системы на период до 2030 г. (далее – Концепция) [5]. Один из разделов указанной Концепции посвящен научно-техническому развитию уголовно-исполнительной системы. Реализация отдельных положений Концепции позволит:

1) создать и внедрить в деятельность уголовно-исполнительной системы единую информационную систему, обеспечивающую сквозную автоматизацию рабочих процессов. Реализация данного пункта Концепции будет способствовать повышению оперативности обмена информацией, принятия управленческих решений, выведет на новый уровень работу по внутриведомственному и межведомственному взаимодействию;

2) создать единое защищенное управляемое информационное пространство для обеспечения внедрения и эксплуатации информационных систем и информационных ресурсов;

3) развить научный потенциал уголовно-исполнительной системы, способствующий получению научных и научно-технических результатов высокого качества (в том числе с использованием новых технологий);

4) развить систему сбора и обработки данных и принятия решений на основе результатов применения искусственного интеллекта в части обеспечения безопасности. Технологии на основе искусственного интеллекта проникают во все сферы общественной жизни: здравоохранение, культуру, сельское хозяйство [2]. А почему бы не использовать их в предупреждении преступлений, в том числе совершаемых

в местах лишения свободы? Так, искусственный интеллект может быть полезен и в противодействии пенитенциарной преступности (аналитические средства для правоохранительных органов, автоматическая обработка потокового видео, поступающих со всех камер исправительного учреждения, система распознавания по различным фрагментам, платформа контекстного интеллекта), и в ее прогнозировании (прогноз психометрики преступного сообщества, система прогнозирования пенитенциарных преступлений, система сканирования данных, автоматическая система фиксации нарушений) [1].

Действительно, искусственный интеллект имеет большой потенциал в процессе расследования и предупреждения пенитенциарных преступлений. Он может помочь должностным лицам в следующих областях:

– анализ больших объемов данных (искусственный интеллект способен обрабатывать и анализировать огромные объемы информации, включая сообщения о преступлениях (регистрационные карточки), информацию об осужденных, уголовные дела прошлых лет с целью выявления скрытых корреляционных связей, возможных закономерностей;

– прогноз пенитенциарной преступности: на основе имеющихся данных искусственный интеллект может выявлять тенденции и «предсказывать» вероятность совершения того или иного преступления тем или иным осужденным;

– искусственный интеллект способен сопоставлять фотографии, имеющиеся в различных базах данных. Подобная информация может быть использована, к примеру, для отслеживания всей цепочки незаконного оборота наркотиков: от изготовителя до потребителя;

– анализ видеоархивов: искусственный интеллект способен распознавать различные объекты на видеозаписях, сопоставлять их. По заранее заданному алгоритму возможно осуществлять поиск тех или иных следов преступной деятельности;

– поведенческий анализ: искусственный интеллект может анализировать цифровые следы осужденных, их поведение на территории исправительного учреждения. Это позволит выявить подозрительную, нетипичную активность для предотвращения подготавливаемого или пресечения совершаемого преступления.

Научно-техническое развитие уголовно-исполнительной системы в сухом остатке должно привести к упрощению сбора и анализа информации. Ведь именно информация лежит в основе любой деятельности.

Конечным итогом научно-технического развития уголовно-исполнительной системы в области предупреждения пенитенциарных преступлений должно стать: информирование субъектов предупреждения данными об объекте воздействия в той мере, которая необходима и достаточна для решения стоящих задач, характере, интенсивности, продолжительности, необходимых силах и средствах, а также выбора других параметров предупредительного воздействия; прогнозирование развития криминогенных и антикриминогенных факторов, способствующих появлению возможных преступников-осужденных; ориентация субъектов предупреждения пенитенциарной преступности в сложившейся криминологической обстановке, ознакомление и понимание ими основных задач, методов, способов и результатов предупредительного процесса; воздействие на поведение осужденных,

на их внутренние убеждения и мотивации с целью выработки уважения к режиму исправительного учреждения; организация взаимодействия отделов и служб исправительного учреждения; накопление и переработка информации для принятия долгосрочных и краткосрочных административных решений.

Можно сделать вывод, что научно-техническое развитие уголовно-исполнительной системы, использование современных технологичных и научных достижений может быть использовано с целью предупреждения пенитенциарных преступлений.

Применение научно-технических достижений в уголовно-исполнительной системе может включать и иные аспекты, которые будут способствовать реализации цели предупреждения совершения новых преступлений:

1) использование информационных технологий для автоматизации процессов учета и контроля осужденных (создание разветвленных баз данных осужденных);

2) внедрение инновационных методов реабилитации и ресоциализации осужденных, использование психологических и педагогических программ (вопросы пробации);

3) развитие биометрических систем и технологий для более надежной идентификации осужденных, а также контроля доступа в исправительное учреждение иных лиц;

4) проведение научных исследований в уголовно-исполнительной системе в области экспертно-криминалистического предупреждения, разработка новых методов раскрытия и предупреждения преступлений, использование современных лабораторных технологий для анализа доказательств и проведения судебных экспертиз.

Список литературы

1. Sukhodolov A. P., Bychkova A. M. Artificial intelligence in crime counteraction, prediction, prevention and evolution // Russian Journal of Criminology. 2018. Т. 12, № 6. С. 753–766.

2. Барометр отрасли: цифровая трансформация экономики // СберПро: [сайт]. 25.07.2023. URL: https://clck.ru/36owsD

3. Зубкова В. И. Исправление осужденных: реальность и перспективы // Человек: преступление и наказание. 2013. № 3(82). С. 44–48.

4. Об утверждении ведомственной программы цифровой трансформации Федеральной службы исполнения наказаний на 2021 г. и плановый период 2022 и 2023 гг.: Приказ Федеральной службы исполнения наказаний от 30.12.2020 № 984 // Документ опубликован не был.

5. Об утверждении Концепции развития уголовно-исполнительной системы на период до 2030 г.: Распоряжение Правительства Российской Федерации от 29.04.2021 № 1138-р // Собрание законодательства Российской Федерации. № 20. 17.05.2021. Ст. 3397.

6. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ // Собрание законодательства Российской Федерации. № 2. 13.01.1997. Ст. 198.

А. А. Петрикина,
кандидат юридических наук, доцент,
Северо-Кавказский филиал
Российского государственного университета правосудия

ПРАВОСУДНОСТЬ СУДЕБНЫХ РЕШЕНИЙ ПО УГОЛОВНЫМ ДЕЛАМ И ВНЕДРЕНИЕ НОВЫХ ТЕХНОЛОГИЙ

Аннотация. Стремительное и активное внедрение новых технологий в уголовный процесс требует глубокого научного анализа и своевременного правового регулирования. Актуальным является выделение и правовое определение новых форм работы эксперта и специалиста в уголовном судопроизводстве в целях повышения эффективности обнаружения, расследования преступлений, вынесения законных и справедливых судебных решений. Цель исследования заключается в разработке подходов к разработке новых форм участия лиц, обладающих специальными знаниями, в уголовном процессе, формулировании основных направлений их развития, выявлении их влияния на качество отправления правосудия по уголовным делам. Активное внедрение электронных средств слежения в уголовном процессе, изучение возможностей транспортировки вещественных доказательств свидетельствуют о необходимости ревизии форм участия специалиста и эксперта в целях постановления законных, обоснованных, мотивированных и справедливых судебных решений. Поэтому были выделены новые виды участия лиц, обладающих специальными знаниями, в уголовном процессе, обозначено их влияние на правосудность приговоров.

Ключевые слова: судебное решение, цифровые технологии, эксперт, специальные знания, приговор, справедливость, законность, обоснованность

THE JUSTICE OF JUDICIAL DECISIONS IN CRIMINAL CASES AND THE INTRODUCTION OF NEW TECHNOLOGIES

Abstract. The rapid and active introduction of new technologies into the criminal process requires in-depth scientific analysis and timely legal regulation. It is relevant to identify and legally define new forms of work of an expert and a specialist in criminal proceedings in order to increase the effectiveness of detection, investigation of crimes, making lawful and fair judicial decisions. The purpose of the work: to develop approaches to the study of new forms of participation of persons with special knowledge in the criminal process, to formulate the main directions of their development, to identify their impact on the quality of the administration of justice in criminal cases. The active introduction of electronic means of tracking in criminal proceedings, the study of the possibilities of transporting material evidence indicate the need to revise the forms of participation of a specialist and an expert in order to make legitimate, justified, motivated and fair court decisions. Therefore, new types of participation of persons with special knowledge in the criminal process were identified, their influence on the justice of sentences was indicated.

Keywords: judicial decision, digital technologies, expert, special knowledge, sentence, justice, legality, validity.

Обоснованное и мотивированное судебное решение по уголовному делу не может обойтись без использования судом специальных знаний [5. С. 432]. В Российской Федерации в Уголовно-процессуальном кодексе отражены лишь некоторые формы их применения:

– участие специалиста в надлежащем производстве процессуальных и следственных действий, когда требуются специальные знания;

– помощь в формулировании вопросов эксперту;

– заключение и показания специалиста;

– заключения и показания экспертов.

Существуют также доктринальные формы использования специальных знаний в уголовном процессе. Это предоставление информации и консультаций [1].

Перманентное развитие научно-технического прогресса приводит к серьезной трансформации уголовного судопроизводства и отдельных его форм. Чтобы эффективно и успешно противостоять преступности, судья, прокурор, следователь должны иметь возможность обращаться к лицам, обладающим специальными знаниями, быстро, оперативно и своевременно.

В настоящий момент мало изученной является помощь специалистов [3] при транспортировке некоторых видов вещественных доказательств, которая связана с рисками:

– сохранения доказательств;

– безопасности транспорта для окружающих;

– вещественные доказательства могут стать предметом или орудием другого преступления.

Законность, обоснованность и мотивированность приговоров зависит от оценки судом всех доказательств по уголовному делу [2. С. 117]. Важно создать законодательство, позволяющее учитывать специфику перевозки соответствующих предметов с возможностью привлечения к этому специалистов.

Стремительное внедрение цифровизации в уголовное судопроизводство привело к появлению дистанционных форм, а также трансформации уже имеющихся с учетом новых технологий.

Появление возможности осуществлять посредством видеоконференцсвязи допрос, очную ставку и опознание требует внимательного отношения следователя. Поскольку без надлежащего технического сопровождения с участием специалиста полученное в результате такого следственного действия доказательство уязвимо. Проверка его достоверности в суде может сопровождаться сложностями. Судье проще исключить его из процесса доказывания, чем допустить вынесение порочного судебного решения. Поэтому в УПК следует внести изменения, касающиеся обязательного участия специалиста при производстве следственных действий удаленным способом.

Законы отдельных зарубежных стран подробно регламентируют использование электронных средств слежения в ходе уголовного преследования [6, 7]. Их анализ показывает наличие перечня аудиовизуальных, электронных и иных технических средств слежения (электронный браслет вместе со стационарным устройством контроля, ретранслятор и аудиовизуальное устройство контроля). Нормы закона

лишь закрепляют возможность использования этих технических средств в уголовном процессе России. Но ряд сложных проблем остается без должного правового регулирования: реестр этих средств, безопасность их использования, регулярный осмотр и техническая эксплуатация [4. С. 120].

Уголовное преследование лиц, связанное с аудиовизуальным наблюдением за ними, должно осуществляться с соблюдением требований научности, законности, этики и безопасности с наблюдением за этим процессом лицами, обладающими специальными знаниями, назрела необходимость создания единого центра использования этих средств; имеют право на отдельное существование нормы уголовно-процессуального права о транспортировке, хранении и использовании определенных видов доказательств, ведь именно в результате их правильного собирания, проверки и оценки можно постановить правосудный приговор; выделенные новые формы специальных знаний должны получить более тщательное правовое закрепление в подзаконных нормативных актах.

Значимость получения и передачи информации в уголовном судопроизводстве дистанционно и в цифровом формате очень велика, однако отсутствие должного правового регулирования не дает высоких результатов в борьбе с преступностью.

Тенденция законодателя к передаче информации по уголовным делам через портал «Государственные услуги» видится не совсем правильной, поскольку не учитывает совместную работу ученых в области уголовно-процессуального права, граждан, следователей, дознавателей, прокуроров, адвокатов, судей и специалистов в области высоких технологий; оставляет без внимания специфику конкретной уголовно-процессуальной формы и не влияет на ликвидацию законодательных пробелов.

На правосудность судебных решений в современных условиях влияет очень большое количество факторов. Поскольку уголовно-процессуальная деятельность суда в наибольшей степени может отразиться на правах и свободах личности нельзя допускать отрицательные качественные изменения приговоров. Поэтому применение новых технологий должно сопровождаться правовой определенностью и грамотным профессиональным сопровождением специалистов соответствующей отрасли знаний.

Список литературы

1. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2// Утвержден Президиумом Верховного Суда Российской Федерации 30 апреля 2020 года. URL: https:// http://www.vsrf.ru/files/28881

2. Лебедев В. М. Судебное производство в уголовном процессе Российской Федерации. Научно-практическое пособие по применению Уголовно-процессуального кодекса РФ / под общ. ред. В. М. Лебедева. 2-е изд., перераб. и доп. М.: Юрайт, 2011.

3. Статистический анализ экспертных компаний в Российской Федерации. Статистика приведена по состоянию на 23.03.2020. Центр экспертиз для суда при

Институте экспертизы для суда и криминалистики. URL: https://ceur.ru/library/articles/jekspertiza/item361229

4. Кириллова Н. П. Основные сценарии современной уголовно- процессуальной политики// Российский криминологический журнал. 2018. № 12(1). С. 116–127.

5. Тарасов А. А., Шарипова А. Р. «Правовые заключения» экспертов и специалистов в российском судопроизводстве // Вестник СПБ: Право. 2017. № 8(4). С. 430–442.

6. Chen, S., Zhao, C., Huang, L., Yuan, J., & Liu, M. Study and implementation on the application of block-chain in electronic evidence generation. Forensic Science International: Digital Investigation. 2020. December. URL: https://www.sciencedirect.com/science/article/abs/pii/S 2666281720300573?via%3Dihub#preview-section-cited-by

7. Guo, Z. Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. Computer Law & Amp. 2023. April. URL: https://www.sciencedirect.com/science/article/abs/pii/S 0267364922001170?via%3Dihub

О. А. Попова,
соискатель,
Университет прокуратуры Российской Федерации

ФЕЙКОВЫЕ НОВОСТИ – ОРУЖИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ В ЦЕЛЯХ НАНЕСЕНИЯ УЩЕРБА НАЦИОНАЛЬНЫМ ИНТЕРЕСАМ СТРАНЫ

Аннотация. В статье раскрывается понятие и сущность современного феномена медиа-пространства – фейковых новостей, источники их распространения, уровень доверия населения к новостным сообщениям, влияние дезинформации (фейков) на криминальное поведение личности в условиях информационного общества, а также наступление негативных социально-экономических последствий. Анализируется социальная обусловленность введения уголовной и административной ответственности за распространение фейковой информации, способы борьбы с дезинформацией.

Ключевые слова: право, информационные технологии, информационное общество, информационная безопасность, кибербезопасность, фейковые новости, дезинформация, криминальное поведение личности, противодействие преступности, медиаграмотность

FAKE NEWS – WEARPONS OF INFORMATION WARFARE IN ORDER TO DAMAGE THE NATIONAL INTERESTS OF THE COUNTRY

Abstract. The article describes the concept and essence of the modern phenomenon of the media space – fake news, examines the sources of their dissemination, the level of public confidence in news reports, the influence of disinformation (fakes) on criminal behavior of the individual in the information society, as well as the onset of negative

socio–economic consequences, analyzes the social conditionality of the introduction of criminal and administrative responsibility for the dissemination fake information, ways to combat disinformation.

Keywords: law, information technology, information society, information security, cybersecurity, fake news, disinformation, criminal behavior of the individual, crime prevention, media literacy

В настоящее время использование ложной общественно значимой информации стало доминирующим приемом при осуществлении многочисленных попыток нанесения ущерба национальным интересам Российской Федерации.

Зачастую местом ее распространения является информационное пространство, где информационные технологии ускоряют и масштабируют объемы распространяемой информации, упрощая доступ к ней большего количества людей. Интернет-сайты, форумы, социальные сети, мессенджеры являются мощным информационным ресурсом, используемым с целью активизировать проявление деструктивных процессов в российском обществе.

Средством выражения недостоверной информации служит современный феномен медийного пространства – фейковые новости (от англ. Fake – «подделка, что-либо ложное, сфальсифицированное, выдаваемое за действительное») [1].

У этого понятия много синонимов: дезинформация, киберпропаганда, когнитивный взлом и информационная война – это всего лишь один аспект более серьезной проблемы: манипулирования общественным мнением с целью воздействия на реальный мир [2].

Проблема фейковых новостей стала широко обсуждаться в последние годы, но сама их концепция существования насчитывает тысячелетия.

В 2019 г. ВЦИОМ проведено в Российской Федерации масштабное исследование, которым установлено, что треть россиян сталкивались с недостоверными новостями в сети Интернет, 20 % респондентов встречали их на телевидении, 7 % – в газетах, 5 % – на радио. Большая часть опрошенных (62 %) сразу поняли, что столкнулись с ложной информацией в СМИ и Интернете, однако треть из них (31 %) сначала поверили недостоверным данным, и лишь впоследствии узнали об их несоответствии действительности [3].

В данной связи высокую актуальность приобрел вопрос изучения такого социального явления, как «фейкинг» – деятельность по созданию и распространению недостоверной информации, а также фейковизации – особого процесса информационно-психологического воздействия на общество в среде масс-медиа.

Исходя из теоретических аспектов данного явления, исследователи А. П. Суходолов и А. М. Бычкова дают следующее определение: «Фейковые новости – это сообщение, стилистически созданное как настоящая новость, но ложное полностью или частично по своему содержанию» [4]. «Феномен новостных фейков – это современная концепция существования социума в условиях, когда в формировании общественного мнения преобладают, а поэтому и массово используются эмоции, вместо объективности. Отсутствие критической составляющей новостной повестки делает возможным превалирование фейков над фактами и реальностью.

При стремительном развитии соответствующих технологий и неконтролируемого распространения не соответствующих действительности новостей – ситуация может приобрести характер «информационных терактов», сила разрушений которых крайне негативно отразится на функционировании общества в целом» [11].

Согласно мнению профессора Е. И. Галяшиной, чтобы говорить о фейковом сообщении, как о разновидности заведомой лжи, необходимо соблюдение трех условий: 1) сообщение должно быть ложным в объективном смысле – не соответствующим реальным фактам и обстоятельствам, имевшим место в действительности; 2) осознание вещающим, что это сообщение ложно; 3) намерение, стремление придать заведомо ложному сообщению видимость истинности с целью ввести аудиторию в заблуждение [5].

Анализ информационного поля показал, что фейк – это целенаправленное использование специально сфабрикованных новостей, главной целью которых является дискредитация, подрыв репутации какого-либо института, организации или персоны с целью получения от этого выгоды: политической или финансовой.

Проблема активного распространения заведомо ложной информации имеет следующую социальную обусловленность.

Дезинформация признается одним из ведущих инструментов информационной войны, в целях которой применяется информационное оружие, а именно соответствующие информационные технологии, средства и методы ее ведения. При ее ведении преследуются цели нанесения ущерба национальным интересам страны.

Содержание понятий «национальные интересы Российской Федерации и стратегические национальные приоритеты» отражены в Указе Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», в числе прочих к ним относятся: защита конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации, укрепление обороны страны; поддержание гражданского мира и согласия в стране, укрепление законности, укрепление мира и безопасности, правовых основ международных отношений. Данным нормативным правовым актом также признается актуальность развития безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия и укрепление традиционных российских духовно-нравственных ценностей [6].

Так, в условиях массовой русофобии и информационной войны именно фейкинг как проводник лжи и обмана выступает как главное оружие, нацеленное на правду как одну из важных традиционных духовных ценностей русского народа [5].

Использование информационного оружия против Российской Федерации стало наиболее выражено в период проведения СВО на Украине. Применение информационных технологий в наступательных целях и создание США и их союзниками «IT-армии Украины» для атак на российскую инфраструктуру было подтверждено информагентству «РИА Новости» 03.08.2022 замглавы МИД России О. Сыромолотовым [7].

По обнародованным Роскомнадзором данным конца февраля 2022 г., по состоянию на 09.06.2023 было выявлено и удалено свыше 206 тыс. страниц сайтов

с недостоверными материалами о сути конфликта СВО, действиях и потерях вооруженных сил, 38 тыс. призывов к протестам, с суммарной аудиторией свыше 202 млн пользователей. Также Роскомнадзор ограничил доступ к почти 3500 копий сайтов «антироссийских информационных ресурсов». Речь идет о сайтах иностранных СМИ и иноагентов [8].

По сведениям, приведенным в интервью Генерального прокурора Российской Федерации в 2022 г., после начала СВО было заявлено и удовлетворено более 340 требований прокуроров о блокировании недостоверной общественно значимой информации о СВО, удалено или заблокировано порядка 138 тыс. интернет-ресурсов [9].

Так, например, в июле 2023 г. Генеральной прокуратурой Российской Федерации принято решение о признании нежелательными на территории страны деятельности иностранных организаций SIA TV Rain (Латвия) и TVR Studios B. V. (Нидерланды) [10]. Данные организации регулярно публиковали информационные материалы экстремистских организаций («ФБК», «штабы Навального»), террористических организаций («Хизб ут-Тахрир»), иностранных агентов («Медуза», «Радио Свобода»), размещали большое количество видеоматериалов, к которым ранее Роскомнадзором принималось решение об ограничении к ним доступа в связи с нарушениями российского законодательства. Руководство названными ресурсами осуществляла иностранная журналистка Н. Синдеева, признанная иностранным агентом, после принятия надзорным ведомством и Роскомнадзором мер по ограничению доступа к сайту, телеканалу и страницам в социальных сетях в отношении ООО «Телеканал Дождь» (признан иноагентом в России) за систематические нарушения законов о СМИ и об информации.

В то же время для эффективного противодействия проявлениям, направленным против российских духовно-нравственных ценностей, исторической памяти, а также гражданского мира и согласия в российском обществе, не следует полагаться лишь на правоохранительные и контрольно-надзорные меры.

«Особое внимание в свете обозначенной проблемы должно быть уделено научно обоснованной системе мониторинга протестной активности населения, выявлению и устранению причин и условий, способствующих ее росту, противодействию угрозам возникновения очагов социальной, межнациональной и межконфессиональной напряженности в современных общественно-политических и социально-экономических условиях» [12].

Реализуя цель защиты национальных интересов страны в сфере информационной безопасности следует более широко использовать средства массовой информации, а также новые информационно-коммуникационные технологии, включая Интернет, поощрять работу в этом направлении институтов гражданского общества, работать над повышением уровня медиаграмотности населения.

В свою очередь, на законодательном уровне уже приняты меры по недопущению роста противоправных деяний в анализируемой сфере. Введена не только административная, но и уголовная ответственность за совершение преступлений с использованием заведомо ложной информации, которая может повлечь нанесение ущерба национальным интересам Российской Федерации. В настоящее время это

следующие составы преступлений: статьи 207, 207^1, 207^2, 207^3, 280^3, 284^1, 284^2, 330^1, 354^1 УК РФ.

Решая вопрос о необходимости криминализации данных преступных деяний, законодатель справедливо признал их общественно опасными и требующими введения на них уголовно-правового запрета.

Вопрос недопущения избыточного ограничения уровня свободы слова и личности, безусловно, является важным. Правоприменители обязаны в каждом конкретном случае устанавливать все фактические обстоятельства подлежащего правовой оценке деяния, а также степень его общественной опасности.

В свою очередь, от научного сообщества требуется проведение новых криминологических исследований распространения заведомо-ложной информации для выработки научно обоснованных мер борьбы с новой, стремительно изменяющейся формой преступности, использующей в своем арсенале информационные технологии.

Только комплексный сбалансированный подход способен обеспечить эффективную защиту информационной безопасности Российской Федерации.

Список литературы

1. Википеди. свободная общедоступная универсальная интернет-энциклопедия Wikipedia. URL: https://ru.wikipedia.org/wiki.

2. Gu L., Kropotov V., Yarochkin F. The fake news machine: how propagandists abuse the internet and manipulate the public. URL: https://www.trendmicro.com

3. ВЦИО. Всероссийский центр изучения общественного мнения: официальный сайт. М., 2019. URL: https://wciom.ru

4. Суходолов А. П., Бычкова А. М. «Фейковые новости» как феномен современного медиапространства: понятие, виды, назначение, меры противодействия // Вопросы теории и практики журналистики. 2017. Т. 6, № 2. С. 143–169.

5. Галяшина Е. И., Богатырев К. М., Никишин В. Д. Фейковизация как средство информационной войны в интернет-медиа. М.: Проспект, 2023. С. 18–19.

6. «О Стратегии национальной безопасности Российской Федерации»: Указ Президента Российской Федерации от 02.07.2021 № 400. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/49e275533c7512b66bfcaa9bd9eef6d046da8060/?ysclid=lmkf7h68no70973741

7. Информационное агентство «Рианновости»: официальный сайт. М., 2022. URL: https://ria.ru/20220803/ssha-1806822731

8. Информационное агентство «Рианновости»: официальный сайт. М., 2023. URL: https://ria.ru/20230609/roskomnadzor-1877118432.html

9. Генеральная прокуратура Российской Федерации: официальный сайт. М., 2022. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=75896540

10. Генеральная прокуратура Российской Федерации: официальный сайт. М., 2023. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=89207602

11. Попова О. А. К вопросу о социальной обусловленности норм об ответственности за распространение заведомо ложной информации (ст. 207.1, 207.2, 207.3 УК РФ) // Сборник материалов II Всероссийской научно-практической конференции «Новые, появляющиеся и видоизменяющиеся формы преступности: научные основы противодействия (Долговские чтения)». 2022. С. 188–194.

12. Меркурьев В. В. Деятельность Прокуратуры по предупреждению преступлений против основ конституционного строя и безопасности государства в условиях роста протестной активности населения // Вестник университета Прокуратуры Российской Федерации. 2022. С. 88–100.

Е. А. Проскура,
адвокат,
член Адвокатской палаты Челябинской области

НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ ПРАВА НА ЧАСТНУЮ ЖИЗНЬ В СЕТИ «ИНТЕРНЕТ»

Аннотация. На сегодняшний день в информационном обществе одним из самых ценных ресурсов является информация. Получить ее в большинстве случаев не составляет труда. Сеть «Интернет» облегчает эту задачу, именно поэтому вопрос об угрозе нарушения личных границ человека становится актуальным как никогда, поскольку именно эти незримые границы являются наиболее уязвимыми. Для получения информации о человеке злоумышленнику не нужно взламывать двери, ему достаточно войти в Сеть при помощи компьютера или другого устройства. Право на неприкосновенность частной жизни имеет решающее значение для соблюдения и осуществления прав человека в сети «Интернет» и вне ее, играя ключевую роль в осуществлении всего спектра прав человека. Именно поэтому право на неприкосновенность частной жизни закреплено как в международных документах, так и во внутреннем законодательстве государств.

Ключевые слова: частная жизнь, личная тайна, семейная тайна, распространение сведений, публичность, Интернет, неприкосновенность, информация

A FEW ASPECTS OF CRIMINAL DEFENSE PRIVACY RIGHT IN THE INTERNET

Abstract. There is no denying that we currently live in the information-oriented society. In today's world information is considered to be the most valuable resource. It is admittedly easy to get any information. Using the Internet considerably simplifies the way we get necessary data. That is why the issue of the private information safety is getting urgent like never before. It is the invisible boundaries that have become the most vulnerable. To get some information about any person a delinquent no longer bothers to break into the person's place. The intruder goes on-line and clicks a few buttons. The human right of privacy is crucial for the respect and observance of human rights on-line and off-line, playing an essential part of in realization of human rights in general. That is the reason why privacy right is formalized by not only the international legal instruments but also domestic legislation.

Keywords: privacy, personal data, family privacy, defamation, data dissemination, publicity, the Internet, immunity, information

Жизнь человека в информационном обществе, существующем в эпоху развитых цифровых технологий очень удобна. Находясь около компьютера, можно наслаждаться шедеврами живописи, знакомиться с научными трудами ученых всего мира, даже путешествовать по другим странам, получать самую разную информацию, в том числе и информацию, которая не должна была стать известна широкому кругу пользователей. Действительно, с сети «Интернет» очень много информации, которая относится к тому или иному человеку и является сферой частной его жизни. Информация передается очень быстро и за весьма короткий промежуток времени может стать достоянием общественности. Это становится проблемой, когда некая приватная информация распространяется без воли лица, к которому она относится. Довольно часто пользователи Сети сами выкладывают свою личную информацию, в том числе и ту, которая по содержанию своему должна носить приватный характер. Много информации появляется в Сети вне зависимости от желания индивида.

Сеть «Интернет» ежеминутно пополняется большим объемом данных, в том числе и силами тех лиц, которые вообще о противоправности своих действий не задумываются. Именно поэтому сегодня не приходится говорить о должной степени осознания злоумышленником противоправной сути действий по сбору и распространению информации, а также о должной степени осознания пользователями сети последствий размещения личной информации.

Государству необходимо не только упорядочивать правовое регулирование уголовно-правовой охраны частной жизни, элементами которой является личная и семейная жизнь, но и параллельно работать над повышением уровня правовой грамотности и осведомленности лиц о наличии защищаемого уголовным законом права на неприкосновенность частной жизни как для потенциальных потерпевших, так и для потенциальных нарушителей. Необходимо создавать культуру пользования Интернетом, предполагающую наличие границ, которые нельзя нарушать.

В России право на неприкосновенность частной жизни провозглашается Конституцией РФ и защищается Уголовным кодексом РФ. Важным элементом права на частную жизнь является конституционный запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Думается, что закрепление данного права в Основном законе в качестве основополагающих прав гражданина является отражением того, что государство признает право на охрану частной жизни гражданина, о которой ранее не имелось четких упоминаний на законодательном уровне, поскольку оно не только существует объективной действительности, но и является основополагающим для любого демократического государства. В соответствии с ч. 1 ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Одной из гарантий неприкосновенности частной жизни является ее уголовно-правовая защита, которая предусмотрена в том числе ст. 137 УК РФ. Содержание указанной статьи на настоящий момент порождает достаточно много вопросов. В ч. 1 ст. 137 УК РФ, устанавливающей ответственность за следующие действия, посягающие на неприкосновенность частной жизни:

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия.

2. Распространение сведений о частной жизни лица, составляющих его личную или семейную тайну в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Информация, относящаяся к личной или семейной тайне, может попасть к злоумышленнику как противозаконным способом, так и быть передана ему самим потерпевшим по той или иной причине (семейные, дружественные связи и проч.). Информация о частной жизни может быть передана или получена в силу исполнения договорных обязательств на вполне законных условиях (к примеру, приватные фотографии могут быть сделаны фотографом по просьбе заказчика), однако их размещение на странице фотографа в социальных сетях без согласия лица, фигурирующего на фотографиях, образует состав преступления, предусмотренного ч. 1 ст. 137 УК РФ.

Данная норма так же, как и ряд других является воплощением функции защиты личной информации со стороны государства. Нельзя отрицать, что вопрос регулирования уголовной ответственности за сбор и распространение личных конфиденциальных данных у законодателя всегда вызывал некоторые трудности. До 1996 г. уголовный закон конкретной статьи, посвященной ответственности за нарушения неприкосновенности личной жизни не содержал. Более того, понятие частной жизни однозначного законодательного закрепления не имело. Лишь появление в 2013 г. в Гражданском кодексе РФ ст. 152.2 «Охрана частной жизни гражданина» наметило тенденции более четкого законодательного регулирования данного вида нематериальных благ.

На настоящий момент вопросов относительно реализации ст. 137 УК РФ все еще остается достаточно много. С развитием информационного общества и распространением сети «Интернет» эти вопросы становятся все более явными, но решать их приходится правоприменителю. Полагаем, что имеющегося подхода к уголовно-правовой охране частной жизни недостаточно. Ряд проблем, обозначившихся в применении ст. 137 УК РФ требует своевременного решения путем внесения изменений в Уголовный кодекс РФ. Отмечу, что с момента появления указанного состава в УК РФ его содержание менялось несколько раз, в том числе и путем исключения из диспозиции части первой ст. 137 УК РФ субъективного признака в виде корыстной или иной личной заинтересованности, а также объективного признака в виде вредных последствий. Однако вопрос о необходимости изменений является дискуссионным. Дело в том, что распространенная частная информация может быть самой разной. Если появление какой-то информации, являющейся личной тайной, не причинит большого вреда, то распространение другой (скажем, более приватной) информации может положить конец карьере или семейной жизни человека, привести его к глубокой моральной травме или даже к самоубийству. Однако о последствиях подобного преступного деяния говорится только в ч. 3 ст. 137 УК РФ, касающейся несовершеннолетних потерпевших.

Нужно отдать должное судам, рассматривающим дела по указанной статье, которые со ссылкой на правовые позиции Конституционного суда РФ учитывают последствия, причиненные распространением охраняемой личной информации при назначении наказания [3]. Заслуживает в данном контексте внимания позиция Конституционного суда РФ о том, что отсутствие указания на последствия

в рассматриваемой нами статье не означает, что при назначении наказания данные последствия судами не должны учитываться.

При рассмотрении ситуации с получением и/или разглашением информации о частной жизни лица неминуемо встает вопрос о том, где заканчивается гражданско-правовой деликт или административное правонарушение и наступает уголовная ответственность за совершенное преступление. Для решения данного вопроса необходимо анализировать каждую конкретную ситуацию. Трудности вызывает отсутствие четкой дефиниции частной жизни лица, составляющей его личную или семейную тайну, за разглашение информации о которой можно понести уголовную ответственность: будет ли, к примеру, считаться личной тайной размещенная лицом фотография на своей странице в социальных сетях, доступ к которой открыт для нескольких друзей, является ли личной тайной сведения о задолженности по коммунальным услугам или по кредитному договору и др. Суды отвечают на эти вопросы исходя из производных каждого рассматриваемого дела. В любом случае должен решаться вопрос о том, являются ли сбор и распространение охраняемой личной тайны умышленным, а также о том, какова цель собирания или распространения личной и семейной тайны.

Суды указывают, что диспозиция ч. 1 ст. 137 УК РФ является отсылочной, для уяснения содержания признака предмета инкриминируемого преступления необходимо обращаться к действующему правовому регулированию в сфере конституционного статуса личности.

При анализе статей 23 (часть 1) и 24 (часть 1) Конституции Российской Федерации можно увидеть, что конфиденциальным характером обладает любая информация о частной жизни лица, а потому она во всяком случае, относится к сведениям ограниченного доступа. Право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера. При анализе судебной практики можно увидеть, какими характеристиками должна обладать «частная жизнь» в контексте статьи 137 УК РФ [1]. Во-первых, это область жизнедеятельности человека. Во-вторых, указанная область жизнедеятельности касается отдельного лица. В-третьих, данная область жизнедеятельности не должна контролироваться ни обществом, ни государством. В-четвертых, она не является противоправной. Не дает законодатель определения понятию «семейная тайна», которое также наравне с термином «личная тайна» включено в диспозицию ч. 1 ст. 137 УК РФ. Отсутствует однозначный ответ на данный вопрос и в правовой доктрине. Отметим, что ст. 150 Гражданского кодекса РФ «нематериальные блага» отграничивает понятие «неприкосновенность частной жизни» от понятия «личная и семейная тайна». К понятию же термина «тайна» мы можем обратиться только изучая словари.

Верховный Суд РФ, пытаясь устранить данные пробелы, указывает, что не может повлечь уголовную ответственность собирание или распространение сведений о частной жизни в государственных, общественных или иных публичных интересах, а также в случаях, если сведения о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле.

Как указывалось, при помощи сети «Интернет» лицо может как получить, так и распространить личную тайную информацию. Однако будет ли распространение такой информации посредством сети «Интернет» уголовно-наказуемым деянием, предусмотренным ст. 137 УК РФ, если данный способ в ней не указан? Либо понятия сеть «Интернет» и «СМИ» являются идентичными?

Стоит отметить, что понятия «информационно-телекоммуникационные сети», «сеть «Интернет» появились в Уголовном кодексе РФ относительно недавно. Их появление служит своеобразным маркером, показывающим, что законодатель реагирует на стремительные изменения в информационной среде общества и предпринимает попытки предотвратить использование различных элементов цифровой среды в противоправных целях. Вышеуказанные понятия: «информационно-телекоммуникационные сети», «сеть «Интернет», также как понятие «электронные сети», продолжают появляться в различных составах Уголовного кодекса РФ (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.1 и других).

Несмотря на это, до сих пор законодателем не дается исчерпывающих и понятных определений вышеуказанных терминов. Определение понятию «информационно-телекоммуникационные сети» дается в п. 4 ст. 2 Федерального закона от 27 июня 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Понятию «сеть «Интернет» на настоящее время законодатель определения не дал. Учитывая, что в ряде вышеуказанных статей Уголовного кодекса РФ используется понятие «информационно-телекоммуникационные сети (включая сеть «Интернет»)», можно сделать вывод о том, что сеть «Интернет» является разновидностью информационно-телекоммуникационных сетей. Поэтому существует мнение о том, что необходимо исключить из текста Особенной части УК РФ указание на сеть «Интернет», [2. С. 93–96].

Как мы видим, понятие «Интернет» прямо ни в одной части статьи 137 УК РФ не упомянуто, поскольку указано только на «распространение сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации».

Если рассмотреть, к примеру, диспозицию квалифицированного состава п. «д» ч. 1 ст. 110 УК РФ, также касающегося распространения информации, то можно увидеть, что в указанной статье предусмотрено деяние по склонению к совершению самоубийства «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)». Отличие от ч. 1 ст. 137 УК РФ достаточно явное. Логичного объяснения данному отличию нет. В данной статье нет указания на противоправность распространения охраняемой информации в «информационно-телекоммуникационных сетях (включая сеть «Интернет»)». Думается, что такая ситуация является недоработкой законодателя, которую приходится устранять путем судебного правотворчества, поскольку из практики видно, что распространение информации о частной и семейной жизни лица посредством

информационно-телекоммуникационных сетей, включая сеть «Интернет», является уголовно наказуемым.

Значимую роль играют выводы Постановления Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)», где предусматривается, что распространение сведений о частной жизни лица заключается в сообщении (разглашении) их одному или нескольким лицам в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет») [5]. Такое толкование представляется логичным.

Судить о масштабах проблемы преступного сбора и распространения личной информации достаточно сложно, поскольку дела по ст. 137 УК РФ относятся к делам частно-публичного обвинения (относительно ч. 1 ст. 137 УК РФ) и предполагают наличие обращения потерпевшего. При этом, если собранные тайно от потерпевших видео- или фотоматериалы выкладываются в Интернет, потерпевшие, не осведомленные о нарушении своих прав, не имеют возможности подать заявление о привлечении нарушителей к уголовной ответственности. На этот счет существует способ решения проблемы, при котором руководитель следственного органа, следователь, а также дознаватель с согласия прокурора могут возбуждать уголовное дело о любом преступлении, указанном в ч. 2 и 3 ст. 20 УПК РФ, и при отсутствии заявления потерпевшего или его законного представителя, если данное преступление совершено в отношении лица, которое в силу зависимого или беспомощного состояния либо по иным причинам не может защищать свои права и законные интересы [4. С. 51–58].

Более того, многие факты неправомерного (преступного) распространения личной тайны не влекут за собой справедливого и адекватного уголовно-правового воздействия со стороны государства. Часто преступления остаются безнаказанными, так как значительная доля потерпевших не хочет дальнейшей огласки личной информации, которая так или иначе будет иметь место в ходе расследования уголовного дела. Как показывает анализ приговоров по ст. 137 УК РФ, чаще всего подсудимыми становятся лица, которые с потерпевшими ранее имели семейные и другие личные связи (к примеру, бывшие мужья или жены), данное обстоятельство также становится фактором, влияющим на желание потерпевшей стороны инициировать возбуждение уголовного дела. Часть потерпевших вообще не знают, что за описанные в ст. 137 УК РФ действия предусмотрена уголовная ответственность, что свидетельствует о низкой правовой грамотности современного общества. В данном контексте задачей государства является не только регулирование вопросов привлечения к уголовной ответственности за нарушение неприкосновенности частной жизни, но и создание условий для правильного и адекватного понимания человеком своих личных границ и возможности их адекватной защиты.

Более остро стоит вопрос о распространении информации о личной жизни несовершеннолетних потерпевших, которые не могут самостоятельно опреде-

лить для себя свои личные границы, поскольку сегодня такие границы становятся все более размытыми, в том числе благодаря стараниям популярных блогеров. В данном случае сеть «Интернет» представляет собой существенную угрозу для несовершеннолетнего. Современное общество столкнулось с масштабной проблемой отсутствия нравственных ориентиров для молодежи. Чаще всего подростки ориентируются на сверстников или на более взрослых молодых людей, которых видят в том же Интернете. Направляя свои приватные фото и видео третьим лицам, дети воспринимают происходящее с ними как игру ровно до тех пор, пока злоумышленники не начинают ими манипулировать. Полагаем, что культуру общения в сети «Интернет» нужно прививать как можно раньше. К сожалению, существующие методы уголовно-правового воздействия за рассматриваемые выше преступные деяния, злоумышленников не останавливают. Отметим, что практика по ч. 3 ст. 137 УК РФ очень немногочисленна, однако отрицать фактическое наличие преступлений, предусмотренных нормой, нельзя.

Кроме того, справедливым можно назвать замечание о том, что указание в диспозиции ч. 1 ст. 137 УК РФ на отсутствие согласия потерпевшего на настоящий момент лишено смысла [6. С. 41–48]. Необходимо отметить, что если сведения о человеке составляют тайну, то при их незаконном распространении в Интернете будет абсолютно неважно, зарегистрирован ли сайт как СМИ.

К сожалению, указанные противоречия все еще находятся вне поля зрения законодателя, который достаточно неохотно вносит изменения в диспозицию ст. 137 УК РФ.

Необходимо обратить внимание еще на одно изменение в рассматриваемую ст. 137 УК РФ, которое внесено в Уголовный кодекс РФ Законом от 28 декабря 2013 г., когда указанная статья дополнена новой, третьей частью, направленной на усиленную уголовно-правовую охрану конфиденциальной информации, касающейся несовершеннолетнего. В данной части под распространением понимается распространение определенной законом информации о несовершеннолетнем «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях». Как видим, понятие «Интернет» здесь также не упомянуто, несмотря на использование понятия «информационно-телекоммуникационные сети», которого нет в части первой этой же статьи.

Исходя из вышеизложенного толкования, сделанного Верховным Судом РФ, а также из употребления в отдельных составах УК РФ понятия «информационно-телекоммуникационные сети (включая сеть «Интернет»)», следует сделать вывод о том, что распространение предусмотренной ч. 3 ст. 137 УК РФ информации, касающейся несовершеннолетнего, через сеть «Интернет» является уголовно-наказуемым, так же как и ее распространение, предусмотренное частью первой данной статьи.

Считаем, что сегодня недостаточно одного указания в части 1 статьи 137 УК РФ на совершение распространения в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Возможность и необходимость разграничения понятий «СМИ» и «Интернет» должна более детально изучаться законодателем. Полагаем, что ранее, когда Интернет не был так распространен, данный вопрос не имел такой актуальности.

На сегодняшний день в целях более четкого и планомерного регулирования защиты лица от посягательств на его частную жизнь вопрос уголовного преследования за собирание и распространение сведений посредством сети «Интернет» должен быть введен в ст. 137 УК РФ (как в первую, так и в третью части) четко и однозначно. Поскольку на настоящий момент нет такого цельного представления о том, что есть сеть «Интернет», говорить о целесообразности устранения данного понятия из составов Уголовного кодекса РФ и оставления только понятия «информационно-телекоммуникационные сети» не представляется возможным.

Абсолютно точно нельзя воспринимать сеть «Интернет» только как один из видов СМИ, хотя законодательно предусмотрено, что в ряде случаев возможна регистрация сайта в сети «Интернет» в качестве СМИ. «Сеть «Интернет» – понятие более широкое, поскольку не все сайты, социальные сети и др. являются средствами массовой информации. На настоящий момент очень быстро и очень легко практически любой пользователь, имеющий доступ в Интернет, может получить и разместить личную информацию, принадлежащую другому лицу.

Однако если, согласно ст. 49 Закона РФ от 27 декабря 1991 г. № 2124–1 «О средствах массовой информации», у журналиста имеется обязанность получать согласие на распространение в средствах массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей, за исключением случаев, когда это необходимо для защиты общественных интересов, то у всех остальных вообще нет на это права.

Вместе с тем на настоящий момент, как следует из судебной практики, основными незаконными «распространителями» личной конфиденциальной информации являются лица без статуса журналиста. Как уже указывалось, на сегодняшний момент это может быть любой человек, обладающий устройством с выходом в Интернет. Использование Интернета для распространения личной тайны значительно облегчает задачу злоумышленнику, потому что он может реализовать свой умысел очень быстро и легко. При этом информация может распространиться за считанные секунды среди огромного количества людей, что делает последствия от совершения преступления, предусмотренного ч. 1 ст. 137 УК РФ, при помощи Интернета более тяжелыми для потерпевшего, и, следовательно, такое преступление должно повлечь более серьезную ответственность. На настоящий момент деяния, предусмотренные ч. 1 ст. 137 УК РФ, относятся к преступлениям небольшой тяжести. Для законодателя степень общественной опасности таких преступлений невелика. Как уже указывалось, для преступления, предусмотренного данной статьей, но совершенного с использованием сети «Интернет», такое положение дел не является справедливым, поскольку Интернет увеличивает степень общественной опасности указанного преступления многократно.

Таким образом, анализируя степень распространенности преступлений, предусмотренных ст. 137 УК РФ, именно посредством использования сети «Интернет», полагаем, что в дальнейшем необходимо дополнение ч. 1 ст. 137 УК РФ квалифицирующим признаком «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)». Это позволит сделать законодательное регулирование в области охраны частной жизни более качественным и адаптированным

под современные реалии. Более того, это будет способствовать достижению единообразия в регулировании вопроса о привлечении к ответственности за преступления, совершенные с использованием информационно-телекоммуникационных сетей. Говоря о единообразии, хотелось бы отметить, что ряд статей наравне со способом совершения преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») называет не только распространение информации в СМИ, но и ее распространение посредством электронных сетей. Однако включение в ч. 2 ст. 137 УК РФ такого способа распространения информации, как распространение через электронные сети будет лишним, поскольку электронные сети можно отнести к разновидности информационно-телекоммуникационным сетей, поскольку законодатель не называет каких-либо особенностей электронных сетей, наличие которых позволило бы утверждать об обратном.

Список литературы

1. Апелляционное постановление Ставропольского краевого суда от 15 ноября 2018 г. по делу № 22–6353/2018.
2. Литвяк Л. Г., Пирогова Е. Н. К вопросу о понятии электронных информационно-телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. С. 93–96.
3. Определение Конституционного Суда Российской Федерации от 9 июня 2005 года № 248-О // СПС «Гарант».
4. Пикуров Н. И. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 51–58.
5. Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «Гарант».
6. Сабитов Т. Р. Об использовании терминов «средства массовой информации» и «Интернет» при формулировании признаков составов преступлений // Российское право: образование, практика, наука: журнал.2020. № 6. С. 41–48.

А. К. Расулев,
доктор юридических наук, профессор,
Институт законодательства и правовой политики
при Президенте Республики Узбекистан

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РАМКАХ ИНИЦИАТИВЫ «ОДИН ПОЯС И ОДИН ПУТЬ»

Аннотация. В статье поднимается проблема киберпреступности в контексте международной инициативы «Один пояс и один путь». Освещаются такие ключевые аспекты, как необходимость создания универсального международного акта, эффективное сотрудничество между государственными органами, подготовка кадров,

технологическое сотрудничество и повышение правовой культуры. Предложены конкретные меры для совместных усилий в борьбе с киберпреступностью, включая создание «Киберполиции» и Академии кибербезопасности.

Ключевые слова: киберпреступность, «один пояс и один путь», международное сотрудничество, универсальный международный акт, кибербезопасность, правовая культура, Узбекистан

COUNTERING CYBERCRIME WITHIN THE FRAMEWORK OF THE «ONE BELT, ONE ROAD» INITIATIVE

Abstract. The article explores the pressing issue of cybercrime in the context of the international «One Belt, One Road» initiative. Key aspects such as the need for a universal international act, effective collaboration between state agencies, workforce training, technological cooperation, and legal culture enhancement are covered. Specific measures for joint efforts in combating cybercrime are proposed, including the establishment of a «Cyber Police» and a Cybersecurity Academy.

Keywords: cybercrime, «one Belt, One Road», international cooperation, universal international act, cybersecurity, legal culture, Uzbekistan

Актуальность. Сегодня современные информационно-коммуникационные технологии стали настолько незаменимыми, что практически невозможно представить нашу жизнь без Интернета и иных гаджетов. Все больше сфер виртуализируются. Пандемия коронавируса «сподвигнула» многие сферы и отрасли цифровизироваться. Вследствие чего появился так называемый виртуальный мир со своими удобствами и возможностями, так и проблемами. Одним из таких проблем является киберпреступность. Преступность не выбирает место или границы, поэтому ни для кого не является странным, что в виртуальном мире появились новые виды и формы преступлений. Эти преступления получили названия киберпреступлений.

Согласно статистическим данным информационно-аналитической компании ASTRA, в 2022 г. киберпреступность нанесла ущерб на сумму 6 триллионов долларов США, по прогнозам к 2025 г. эта цифра достигнет 10,5 триллионов долларов США. По подсчетам, сегодня за день совершаются 2328 правонарушений в киберпространстве, ежечасно их жертвами становятся 97 человек [7].

Специалисты компании Cybersecurity Ventures отмечают, что к 2031 г. программы-вымогатели будут обходиться своим жертвам примерно в 265 миллиардов долларов США ежегодно, лишь для преодоления последствий криптопреступности с 2025 г. ежегодно потребуется 30 миллиардов долларов США [8]. Эти цифры наглядно показывают почему важна эффективная и своевременная стратегия по противодействию киберпреступности в целом. Не зная границ и пределов, киберпреступления требуют совместных усилий всего мирового сообщества. Ведь не зря 16-я цель в области устойчивого развития ООН посвящена содействию построению миролюбивого и открытого общества в интересах устойчивого развития, обеспечение доступа к правосудию для всех и создание эффективных, подотчетных и основанных на широком участии учреждений на всех уровнях [10].

Насколько важно решение рассматриваемой проблемы в рамках инициативы «Один пояс и один путь»? На наш взгляд, есть две самые большие причины, обуславливающие важность решения проблемы.

Во-первых, масштаб инициативы. По данным одного из самых престижных и старейших вузов в Китае – Университета Фудань, инициатива включает 149 государств мира, в том числе Китай [2]. Еще 8 стран изъявили желание включиться в инициативу. Географически страны представляют практически всю Африку, существенную часть Евразии, а также большинство стран Латинской Америки. В них проживает больше 62 % населения Земли. Значит, киберпреступность представляет угрозу населению и государствам на трех материках нашей Земли. Отсутствие совместных усилий повышает риск совершения киберпреступлений.

Во-вторых, высокий уровень вреда киберпреступлений. В качестве примера можно привести Китай. Согласно современным научным исследованиям, Китай занимает первое место по уровню киберпреступности [3]. Также Китай входит в тройку стран, которая больше всех подвергается кибератакам. В частности, эти атаки направлены на оборонную промышленность, средства связи и технологии. В целом из 10 топ-стран по уровню киберпреступности шесть стран относятся к участникам инициативы «Один пояс и один путь». Поэтому для стран этой инициативы решение проблемы киберпреступности является востребованным.

Основные направления международного сотрудничества. В рамках инициативы «Один пояс и один путь» нам представляется целесообразным выделить следующие направления:

Первое – разработка универсального международного акта в области противодействия киберпреступности. Поддержка инициативы около 150 странами мира свидетельствует о широких возможностях, а также о различиях в правовом аспекте. Законодательство стран различается, что выражается в признании или непризнании каких-либо кибератак преступлением, возложением расследования преступлений на определенный государственный орган. Сложности возникают, когда киберпреступление совершается гражданином одного государства со своей территории, а последствие наступают на территории другого государства. В большинстве случаев киберпреступления носят транснациональный характер. Поэтому Управление ООН по наркотикам и преступности относит киберпреступления к категории транснациональных преступлений.

К сожалению, в мире отсутствует единый универсальный документ в области противодействия киберпреступности. Существуют ряд региональных актов, самым известным из которых является Будапештская конвенция по компьютерным преступлениям. Однако этот документ не стал поистине универсальным и международным. Среди стран вызывают споры некоторые его положения, в особенности пункт «b» статьи 32. По этой статье сторона может без согласия другой Стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему [6]. Этот пункт вызывает озабоченность правоохранительных органов

многих органов, так как повышается риск кибербезопасности важных информационных ресурсов государств.

С учетом важности компромисса и гармонизации законодательств стран мира представляется важной разработка универсального международного акта в области киберпреступности, который будет включать как вопросы материального (какие нарушения следует признавать киберпреступлением), так и процессуального права (порядок и условия взаимоотношений между судами, правоохранительными и иными уполномоченными органами государств). Именно страны инициативы «Один пояс и один путь», на наш взгляд, должны стать инициаторами разработки и принятия этого документа в рамках ООН.

Второе – налаживание эффективного сотрудничества между уполномоченными государственными органами. Эффективность противодействия международного сотрудничества, как правило, оценивается уровнем раскрываемости преступлений и эффективностью профилактических мер. В этой части государствам следует разработать программу сотрудничества, а также порядок и особенности расследования киберпреступлений, нанесших вред нескольким странам.

Представляется целесообразным трансформация и улучшение деятельности Управления по борьбе с киберпреступностью Интерпола. В частности, необходимо создать отдельную платформу и механизм сотрудничества между сотрудниками соответствующих органов. Такая платформа может быть в форме «Киберполиции», которая будет вести мониторинг и учет различных инцидентов путем анализа открытых данных или информационных ресурсов стран (с согласия государств). При обнаружении определенного киберинцидента государства посредством «Киберполиции» смогут создать оперативно-следственные группы или вести первичные меры для обнаружения и закрепления следов правонарушения.

Успех совместных операций по противодействию киберпреступлениям уже имеет место. Так, в рамках совместной операции Интерпола, полиции Нигерии и компания Group-IB (специализируется на расследовании международных киберпреступлений, Сингапур) «Falcon» в 2020 г. была пресечена деятельность киберпреступников из Нигерии. Эта преступная группировка с 2017 г. скомпрометировала не менее 500 тысяч государственных и частных компаний в более чем 150 странах [9].

Третье – совместная работа по подготовке (переподготовке) и повышению квалификации кадров. Любой успех зависит, в первую очередь, от человеческих ресурсов. К сожалению, не все сотрудники правоохранительных органов стран мира обладают необходимыми знаниями или навыками по расследованию киберпреступлений. На это есть объективные причины, ведь правовая оценка киберпреступлений требует не только сугубо юридических, но и специальных познаний в области информационно-коммуникационных технологий. Поэтому государствам следует обмениваться опытом в рамках образовательных процессов. Учитывая опыт стран, а также имеющиеся научно-исследовательские ресурсы следует обсудить вопрос о создании Академии кибербезопасности и его филиалов в регионах мира, которая будет координироваться усилиями ООН и объединять в себе как образовательные, так и научно-исследовательские составляющие. В этой

Академии представляется целесообразным осуществлять работу по подготовке (переподготовке) и повышению квалификации кадров.

Четвертое – организационно-техническое сотрудничество. Раскрытие киберпреступлений или обнаружение следов кибератак требует современного оснащения и технологий. К сожалению, не все страны обладают такими технологиями. Иногда попросту нет технологий определения следов по каким-либо методам или способам совершения киберпреступлений. Это влияет на степень противодействия киберпреступности. Ошибочно предполагать, что нераскрытие киберпреступности в какой-то стране влияет только на эту страну. Чувствуя безнаказанность, злоумышленники могут продолжать свою преступную деятельность. Поэтому важна технологическая составляющая процессов противодействия киберпреступлений.

В этой связи странам, в частности государствам в рамках инициативы «Один пояс и один путь», следует объединить усилия по улучшению технологического обеспечения уполномоченных государственных органов, обмениваться современными достижениями. Кроме того, странам следует проводить совместные научно-практические исследования для разработки новых технологий для противодействия киберпреступности.

Пятое – меры по повышению правовой культуры. В рамках международного сотрудничества недостаточно лишь сотрудничество между странами и правоохранительными структурами. Важны и профилактические меры. На наш взгляд, среди мировой общественности, в частности детей, необходимо формировать чувство цифровой гигиены. Необходимо создание единой платформы «Безопасная онлайн среда», которая будет как информационно-разъяснительной платформой, так и ресурсом для получения определенных заявлений или предложений.

Такой опыт применяется в некоторых зарубежных странах. В Австралии систематически проводится онлайн-кампания «Оставайся умным» (Stay Smart Online), которая предоставляет частным лицам и малому бизнесу информацию о том, как защитить себя от угроз кибербезопасности и снизить риск их возникновения. Более того, веб-сайт Австралийского офиса Комиссии по кибербезопасности способствует обеспечению безопасности в Интернете, предоставляя образовательные ресурсы для детей, родителей и других лиц, информируя их о различных формах киберпреступлений и способах, которыми они могут защитить себя в Интернете, а также предоставляя пользователям возможность сообщать об определенных киберпреступлениях через веб-сайт [1].

В Канаде платформа Правительства Get Cyber Safe предоставляет частным лицам и предприятиям информацию о рисках кибербезопасности и способах, с помощью которых частные лица и предприятия могут защитить себя от угроз кибербезопасности [4].

Схожая программа имеется в Великобритании – GetSafeOnline. Это инициатива по повышению осведомленности о кибербезопасности, которая предоставляет людям информацию о методах обеспечения безопасности дома и на рабочем месте [5].

В США действует инициатива Национального альянса по кибербезопасности StaySafeOnline [6], которая предлагает людям информацию о безопасных методах работы в Интернете, киберпреступлениях, защите ключевых онлайн-аккаунтов и цифровых устройств, а также управлении конфиденциальностью. Каждый октябрь в США Национальным альянсом по кибербезопасности и Министерством внутренней безопасности отмечается национальный месяц осведомленности о кибербезопасности (NCSAM).

Заключение. В заключение следует отметить, что инициатива «Один пояс и один путь» имеет глубокие исторические корни. В древности Великий шелковый путь был не только торговым путем, но пересечением различных культур, местом для обмена опытом и знаниями. Сегодня инициатива «Один пояс и один путь» также имеет все шансы стать таким. Совместные и слаженные усилия по всем вопросам глобального характера, включая противодействие киберпреступности, позволит странам добиться благосостояния и безопасности. Как гласит знаменитая китайская пословица, «дружная семья и землю превратит в золото».

Список литературы

1. Australian Cyber Security Centre. URL: https://www.staysmartonline.gov.au/about-us

2. Countries of the Belt and Road Initiative (BRI). URL: https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri

3. D. Howard Kass. Cybercrime Top 10 Rankings: China is No. 1 While U. S. Records Highest Rate of Security Breaches. URL: https://www.msspalert.com/news/cybercrime-top-10-rankings-china-is-no-1-while-u-s-records-highest-rate-of-security-breaches

4. Get Cyber Safe. URL: https://www.getcybersafe.gc.ca/en

5. Get Safe Onine. URL: https://www.getsafeonline.org

6. National CyberSecurity Alliance. URL: https://staysafeonline.org

7. Nivedita James. 90+ Cyber Crime Statistics 2023: Cost, Industries & Trends. URL: https://www.getastra.com/blog/security-audit/cyber-crime-statistics

8. Steve Morgan. CISO Show: Ransomware Is Relentless. Sponsored by KnowBe4. URL: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

9. Операция «Falcon»: Group-IB помогла Интерполу выявить преступников из Нигерии, атаковавших компании по всему миру. URL: https://www.facct.ru/media-center/press-releases/gib-interpol-bec

10. Цели в области устойчивого развития. URL: https://www.un.org/sustainabledevelopment/ru/peace-justice

В. В. Ровнейко,
кандидат юридических наук, доцент,
Удмуртский государственный университет

УГОЛОВНО-ПРАВОВАЯ ОХРАНА И АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ РАСПРОСТРАНЕНИЯ ЗАПРЕЩЕННОЙ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ

Аннотация. Статья посвящена анализу некоторых аспектов уголовно-правовой охраны и административно-правового регулирования отношений в сфере передачи и распространения запрещенной законодательством РФ информации с использованием социальных сетей и мессенджеров. Проведенный анализ действующего законодательства, практики его применения и иной информации об уголовно-правовых и административно-правовых способах противодействия использованию социальных сетей и мессенджеров позволил выявить определенные тенденции и сформулировать некоторые выводы. Социальные сети и мессенджеры, являясь видами сетевых информационных пространств и имея некоторые общие черты, должны рассматриваться в качестве самостоятельных правовых понятий. Правовые нормы, регулирующие эту сферу деятельности и особенности уголовной ответственности в этой сфере, только формируются. Различные интернет-ресурсы в связи с различными техническими особенностями и возможностями имеют различное правовое регулирование. Конкретизация регулятивных норм по отношению к социальным сетям и мессенджерам позволит постепенно сформировать необходимые и достаточные уголовно-правовые нормы, а также единообразный подход к определению понятий, используемых в уголовном, административном и информационном праве.

Ключевые слова: уголовное право, административное право, социальные сети, мессенджеры, преступления, совершенные с использованием информационно-телекоммуникационных сетей, распространение запрещенной информации, понятие «публичность»

Финансирование: Исследование проведено при финансовой поддержке ФГБОУ ВО «Удмуртский государственный университет» («Научный потенциал-2023») в соответствии с приказом ректора от 14.04.2023 № 476/01–01–04 «О проведении в 2023 году конкурса междисциплинарных научно-исследовательских работ (грантов) молодых ученых, преподавателей и сотрудников УдГУ».

CRIMINAL LAW PROTECTION AND ADMINISTRATIVE REGULATION OF RELATIONS IN THE SPHERE OF DISTRIBUTION INFORMATION PROHIBITED BY RUSSIAN FEDERATION LEGISLATION IN SOCIAL NETWORKS AND MESSENGERS

Abstract. The article is devoted to the analysis of some aspects of criminal law protection and administrative legal regulation of relations in the field of transmission and

dissemination of information prohibited by the legislation of the Russian Federation using social networks and messengers. The analysis of the current legislation, the practice of its application and other information on criminal and administrative legal methods of countering the use of social networks and messengers allowed us to identify certain trends and formulate some conclusions. Social networks and messengers, being types of network information spaces and having some common features, should be considered as independent legal concepts. The legal norms regulating this sphere of activity and the specifics of criminal liability in this area are only being formed. Various Internet resources due to various technical features and capabilities have different legal regulation. The specification of regulatory norms in relation to social networks and messengers will gradually form the necessary and sufficient criminal law norms, as well as a uniform approach to the definition of concepts used in criminal, administrative and information law.

Keywords: criminal law, administrative law, social networks, messengers, crimes committed using information and telecommunication networks, dissemination of prohibited information, publicity

Введение. Отношения по созданию и использованию социальных сетей и мессенджеров регулируются Федеральным законом от 27.07.2006 № 149-ФЗ (ред. от 31.07.2023) «Об информации, информационных технологиях и о защите информации» (далее – Закон). Социальные сети и мессенджеры являются широко используемыми средствами коммуникации и образуют сетевые информационные пространства [19]. Социальные сети часто объединяют в единую группу с мессенджерами, так как и те, и другие предоставляют средства для общения большому кругу лиц, но правовое регулирование их создания и использования имеет ряд различий.

Необходимо отметить, что значение социальных сетей и мессенджеров постоянно возрастает. Согласно опубликованным статистическим данным об Интернете и социальных сетях в мире за 2023 г., в России проникновение Интернета находится на уровне 88,2 %. Аудитория соцсетей продолжает расти. Популярными приложениями социальных сетей в мире в 2023 г. являются, например, YouTube, Facebook*, WhatsApp, Instagram*, Messenger, TikTok, Telegram, Twitter**. Необходимо обратить внимание на то, что «платформы, которые мы сегодня называем «социальными», будут продолжать расширять свое влияние на нашу жизнь, перестраивая наши источники информации, наши привычки потребления развлечений и ориентиры, формирующие наше мировоззрение» [2].

В Информационном письме Банка России обращено внимание на повышенную опасность использования социальных сетей и мессенджеров для финансирования терроризма [10].

В связи с этим является оправданным особое внимание, уделяемое социальным сетям и мессенджерам.

Основная часть. За нарушение установленных законодательством Российской Федерации ограничений и запретов на распространение информации предусмотрена административная и уголовная ответственность [14]. Это положение позволяет сделать вывод о том, что обладатели информации, владельцы соответствующих

сайтов и других информационных ресурсов могут быть субъектами не только административной, но и уголовной ответственности. Действие указанной статьи распространяется и на владельцев социальных сетей и мессенджеров.

Сфера применения норм, устанавливающих административную ответственность для владельцев социальных сетей, постоянно расширяется, а сама ответственность ужесточается. Так, в июле 2023 г. была установлена административная ответственность за правонарушения для владельцев именно социальных сетей [5]. Закон вступил в действие с 1 сентября 2023 г.

Часть 1 ст. 10.6 Закона устанавливает для владельцев социальных сетей обязанность соблюдать требования законодательства Российской Федерации, в частности не допускать использование социальной сети в целях совершения уголовно наказуемых деяний и распространения запрещенной информации, и обязанность осуществлять мониторинг социальной сети в целях выявления материалов, содержащих информацию, запрещенную законодательством Российской Федерации, а также уведомлять пользователя социальной сети о принятых мерах по ограничению доступа к его информации, а также об основаниях такого ограничения [14], т. е. не допускать распространение запрещенной информации, проводить мониторинг социальных сетей и блокировать или удалять запрещенную информацию. Достаточно большое количество стоп-контента удаляется, благодаря усилиям волонтеров и в результате действий государственных органов, но, к сожалению, не весь стоп-контент может быть оперативно заблокирован и удален [4].

В отношении владельцев мессенджеров, а также пользователей социальных сетей и мессенджеров специальных обязанностей Законом не предусмотрено. Что вполне объяснимо организационно-техническими причинами. Отсутствие закрепленной в Законе обязанности не нарушать Уголовный закон Российской Федерации и соблюдать другие законы Российской Федерации от обязанности не допускать распространения запрещенной информации не освобождает. Следует обратить внимание на то, что в отношении владельцев социальных сетей и мессенджеров применяются административные меры, такие как ограничение доступа и административные штрафы. Но административные меры, применяемые к владельцам социальных сетей и владельцам мессенджеров, а также к самим сетевым пространствам, различны.

Необходимо отметить, что понятие «социальная сеть» может рассматривать как нормативное. А понятие «мессенджер» – таковым не является.

Статью 10.6 Закона, которая была включена в декабре 2020 г. [14] и вступила в силу с 1 февраля 2021 г., назвали «Законом о социальных сетях». Под это понятие попали популярные социальные сети. К ним также могут быть отнесены сайты с объявлениями типа Avito и Юла, YouTube и TikTok, и даже некоторые мессенджеры, например Telegram, так как там можно создавать свои каналы (страницы) [20].

Согласно ст. 10.6. Закона «социальная сеть» определена как интернет-ресурс, который 1) предназначен и (или) используется для предоставления и (или) распространения посредством созданных персональных страниц информации; 2) на которых может распространяться реклама; 3) доступ к которым в течение суток составляет более пятисот тысяч пользователей сети «Интернет», находящихся на

территории Российской Федерации». Реестр социальных сетей содержит исчерпывающий перечень социальных сетей.

Для включения в Реестр к иностранным компаниям предъявлены три требования: разместить на информационном ресурсе электронную форму; создать филиал, открыть представительство или учредить российское юридическое лицо; зарегистрировать личный кабинет на официальном сайте Роскомнадзора. Это требования предусмотрены Федеральным законом 2021 г., который получил название закона о «приземлении» [9].

Понятие «мессенджер» в законе не используется, но Федеральным законом, принятым в декабре 2022 г. и вступившим в силу с 1 марта 2023 г., в ст. 10 Закона были введены части 8–10, которые позволяют определить мессенджеры как информационные ресурсы, которые 1) предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ, 2) при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения и 3) не предусматривается размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет»» [8].

Был установлен запрет на использование иностранных мессенджеров государственными учреждениями и кредитными организациями Российской Федерации. За незаконное использование иностранных мессенджеров государственными учреждениями и кредитными организациями введена административная ответственность [6]. В перечень запрещенных к использованию вошли девять мессенджеров [18].

В отношении мессенджеров блокировка (ограничение доступа) не применяется. На владельцев мессенджеров не возлагается обязанность по недопущению распространения стоп-контента, мониторингу, блокировке доступа и удалению запрещенного контента.

Блокировка социальных сетей (ограничение доступа к Интернет-ресурсам, содержащим информацию, распространение которой в Российской Федерации запрещено) в соответствии со ст. 15.1 Закона может осуществляться как в судебном, так и во внесудебном порядке. Как отмечают исследователи, суды активно участвуют в блокировке интернет-ресурсов [15]. Создана и постоянно пополняется ЕАИС «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

Такая административная мера как блокировка контента применяется только в отношении социальных сетей. В отношении мессенджеров используется запрет на их использование. Отношение и законодателя, и правоприменителя к этим интернет-ресурсам дифференцировано. Например, деятельность Instagram* и Facebook* в России признана экстремистской и запрещена, но пользоваться ими по-прежнему возможно, хотя и с рядом ограничений. При этом решение о запрете Instagram и Facebook*, не коснулось мессенджера WhatsApp ввиду отсутствия у него функций по публичному распространению информации [16]. Обязанность по выявлению и удалению запрещенного контента входит в обязательные требования для деятельности социальных сетей. За неисполнение этой обязанности в марте 2022 г. и были заблокированы Facebook*, Instagram*, Twitter** [17].

Ограничение доступа социальным сетям и размещенной в них информации с территории Российской Федерации может быть обойден путем использования анонимайзеров и VPN-сервисов. Федеральный закон, вступивший в силу еще с 1 ноября 2017 г., запретил использование анонимайзеров и VPN-сервисов для посещения запрещенных Роскомнадзором сайтов. За неисполнение соответствующего требования Роскомнадзора будет устанавливаться ограничение доступа к информационным ресурсам, предоставляющим доступ к сетям, системам и программам, используемым для обхода блокировок; на операторов поисковых систем возложена обязанность прекращать выдачу ссылок на заблокированные информационные ресурсы (статья 15.8 Закона).

В СМИ отмечалось, что «принят закон против всех анонимайзеров, VPN-сервисов, браузеров Tor и Opera» [1]. Но до настоящего времени эти требования не исполнялись. В связи с этим Минцифры вышло с предложением предоставить Роскомнадзору полномочия по блокировке сайтов, которые содержат информацию о методах и способах обхода блокировок в стране. Соответствующий проект опубликован 1 сентября 2023 года на государственном портале нормативных правовых актов. На текущий момент он находится на этапе обсуждения, который должен закончиться 15 сентября [3].

Все вышеуказанные меры являются административными и применяемыми только к владельцам социальных сетей и информационным ресурсам. В отношении мессенджеров позиция законодателя более лояльна, т. к. у мессенджеров «отсутствуют функций по публичному распространению информации».

Здесь подходы к определению понятия «публичности» в административном праве и в уголовном принципиально различаются. Например, при решении вопроса о публичности распространения информации путем направления сообщений в мессенджерах, – для применения уголовного закона такое распространение считается публичным. В двух постановлениях Пленума Верховного Суда РФ, содержатся идентичные разъяснения о признании публичными совершение подобных действий [13, 11].

Случаи использования социальных сетей и мессенджеров для совершения различных преступлений, в том числе преступлений экстремистского характера, нередки. В постановлении Пленума Верховного Суда содержатся разъяснения, что «для признания наличия в действиях подсудимого признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики» [12]. В указанном постановлении Пленума также содержится примерный перечень средств «доступа к электронным или информационно-телекоммуникационным сетям, в том числе сети «Интернет», который может осуществляться с различных компьютерных устройств, технологически предназначенных для этого, с использованием программ, имеющих разнообразные функции» [12]. К таким средствам могут относится и мессенджеры, и социальные сети. Позиция Верховного Суда РФ позволяет усматривать использование социальных сетей и мессенджеров как

использование информационно-телекоммуникационных сетей независимо от того, какое количество лиц к ним подключено и на какой круг лиц (определенный или неопределенный) они рассчитаны. Неопределенность круга лиц – является признаком публичности в уголовном праве. Массовые рассылки сообщений возможны не только через средства мобильной связи, но и через мессенджеры.

Заключение. Проведенный анализ действующего законодательства, практики его применения и иной информации об уголовно-правовых и административно-правовых способах противодействия использованию социальных сетей и мессенджеров позволяют сформулировать некоторые выводы.

Необходимо отметить, что социальные сети и мессенджеры, являясь видами сетевых информационных пространств и имея некоторые общие черты, все-таки должны рассматриваться в качестве самостоятельных правовых понятий, так как регулятивное законодательство определяет их признаки и статус по-разному, различаются и административно-правовые способы противодействия их незаконному использованию.

С учетом действующего уголовного законодательства сложно определить, какие именно нормы устанавливают уголовную ответственность владельцев социальных сетей и мессенджеров за неисполнение установленных Законом требований, связанных в первую очередь с недопущением распространения через социальные сети и мессенджеры запрещенной законодательством Российской Федерации информации, проведением мониторинга по выявлению такой информации, ограничению доступа и блокирования такой информации, а также непринятием мер по ограничению доступа к информационным ресурсам, используемым для обхода блокировок. Предусмотренные действующим законодательством Российской Федерации и применяемые к владельцам социальных сетей и их информационным ресурсам меры носят преимущественно административный характер.

Административные меры, предусмотренные действующим законодательством Российской Федерации и применяемые к владельцам мессенджеров и их информационным ресурсам меры, также носят административный характер, но они не налагают на последних тех обязанностей, которые установлены в отношении социальных сетей.

Закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, и устанавливает обязанности и запреты для профессиональных участников этих отношений. В настоящее время, несмотря на указание в Законе на возможность привлечения к уголовной ответственности профессиональных участников информационных отношений, в первую очередь владельцев социальных сетей и мессенджеров, такая возможность отсутствует. Их ответственность носит административный характер и применяются административные меры.

Обязанности пользователей социальных сетей и мессенджеров Законом не установлены. За использование социальных сетей и мессенджеров для совершения различных преступлений законодательством России предусмотрена уголовная ответственность. Действие существующих уголовно-правовых норм направлено на поведение пользователей социальных сетей и мессенджеров. Уголовная ответственность предусмотрена за использование социальных сетей и мессенджеров

для размещения запрещенной законодательством Российской Федерации информации и совершения иных противоправных действий.

Складывается впечатление, что говорить об уголовной ответственности владельцев социальных сетей и мессенджеров за неисполнение установленных законодательством России обязанностей по недопущению, мониторингу, блокировке и удалению запрещенной Законом информации в настоящее время не имеет смысла. Правовые нормы, регулирующие эту сферу деятельности и особенности уголовной ответственности в этой сфере, только формируются. Различные интернет-ресурсы в связи с техническими особенностями имеют различное правовое регулирование. Конкретизация регулятивных норм по отношению к социальным сетям и мессенджерам позволит постепенно сформировать необходимые и достаточные уголовно-правовые нормы, а также единообразный подход к определению понятий, используемых в уголовном, административном и информационном праве.

---

* Meta и принадлежащие ей Facebook и Instagram признаны экстремистскими, их деятельность запрещена на территории Российской Федерации.

** Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

Список литературы

1. В России запретили Tor и VPN. Что теперь делать. URL: https://habr.com/ru/companies/pochtoy/articles/405827

2. Интернет и соцсети в начале 2023 год. главные цифры Global Digital 2023. URL: https://vc.ru/marketing/596126-internet-i-socseti-v-nachale-2023-goda-glavnye-cifry-global-digital-2023

3. Капранов Олег. Роскомнадзор предложили наделить полномочиями по блокировке сайтов с информацией о VPN-сервисах. URL: https://rg.ru/2023/09/03/mincifry-predlozhilo-zapretit-informaciiu-o-vpn-servisah.html

4. Ключевская Наталья. Стоп, контент: новые обязанности владельцев соцсетей и права пользователей. URL: https://www.garant.ru/article/1444081

5. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 31.07.2023 № 401-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_453256/3d0cac60971a511280cbba229d9b6329c07731f7

6. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 24 июня 2023 г. № 277-ФЗ // СПС «КонсультантПлюс».

7. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 30.12.2020 № 530-ФЗ // СПС «КонсультантПлюс».

8. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации: Федеральный закон от 29.12.2022 № 584-ФЗ // СПС «КонсультантПлюс».

9. Закон «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» регулирует отношения, связанные с осуществлением деятельности иностранных лиц в сети «Интернет» на территории Российской Федерации: Федеральный закон от 01.07.2021 № 236-ФЗ // СПС «КонсультантПлюс».

10. О национальной оценке рисков ОД и ФТ: Информационное письмо Банка России от 18.01.2023 № ИН-08–12/6. URL: http://www.cbr.ru

11. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_125957

12. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // СПС «КонсультантПлюс».

13. О судебной практике по уголовным делам о преступлениях экстремистской направленности: Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_115712

14. Об информации, информационных технологиях и о защите информации: Федерального закона от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс».

15. Омелин В. Н., Горовой В. В. Анализ судебной практики по блокировке интернет-групп в мессенджерах и страниц в социальных сетях // Уголовно-исполнительная система: право, экономика, управление. 2019. № 1 // СПС «КонсультантПлюс».

16. Роскомнадзор исключил Instagram и Facebook из реестра соцсетей. URL: https://rg.ru/2022/03/29/roskomnadzor-iskliuchil-instagram-i-facebook-iz-reestra-socsetej.html

17. Роскомнадзор ограничил доступ к социальной сети Twitter. URL: https://iz.ru/1300900/2022–03–04/roskomnadzor-ogranichil-dostup-k-sotcialnoi-seti-twitter

18. Роскомнадзор сообщил, какие иностранные мессенджеры с 1 марта 2023 года не должны использоваться в работе ряда организаций. URL: https://www.garant.ru/news/1611089

19. Сетевое информационное пространство: основные понятия и термины. URL: https://www.finam.ru/publications/item/setevoe-informatsionnoe-prostranstvo-20230629–1037

20. Что соцсети должны пользователя. новый закон. URL: https://dzen.ru/a/X_6Z7WJb_HMtKC 0l

В. И. Романов,
кандидат юридических наук, доцент,
Казанский (Приволжский) федеральный университет

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ЦИФРОВЫХ СРЕДСТВ КРИМИНАЛИСТИКИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ УЧАСТНИКОВ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО УГОЛОВНОМУ ДЕЛУ

Аннотация. В условиях цифровизации и информатизации повышается роль и задачи средств криминалистики, используемых в сфере обеспечения безопасности участников уголовного судопроизводства на досудебной стадии по уголовному делу. Многие средства криминалистики, в том числе и цифровые, способны оказать помощь правоохранительным органам в борьбе с преступностью. В статье рассмотрены проблемные вопросы применения цифровых, специальных следообразующих средств, их виды, возможность применения в практической деятельности и, как следствие, формирование безопасного участия всех субъектов, участвующих в уголовном судопроизводстве.

Ключевые слова: криминалистика, научно-технические средства, криминалистические следообразующие средства, безопасность участников уголовного судопроизводства

FEATURES OF THE USE OF DIGITAL AND TECHNICAL AND FORENSIC MEANS TO ENSURE THE SAFETY OF PARTICIPANTS IN PROCEEDINGS IN CRIMINAL CASE

Abstract. In the conditions of digitalization and informatization, the role and tasks of criminalistics tools used in the field of ensuring the security of participants in criminal proceedings at the pre-trial stage of a criminal case are increasing. Many forensic tools, including digital ones, are able to assist law enforcement agencies in the fight against crime. The article discusses the problematic issues of the use of digital, special trace-forming tools, their types, the possibility of application in practice and, as a result, the formations of safe participation of all subjects involved in criminal proceedings.

Keywords: criminalistics, scientific and technical means, forensic trace-forming means, security

Вопросы безопасности участников досудебного производства обеспечиваются при помощи комплекса мер, предусмотренных современным законодательством.

Обеспечение безопасности участвующих в уголовном деле лиц имеет уголовно-процессуальное и криминалистическое значение. Речь идет о цифровых, специальных следообразующих средствах. Криминалистические следообразующие средства в отечественной практике используются уже многие годы, но из-за грифа «для служебного использования», о них знают немногие. Об этом можно судить и по содержанию учебников по криминалистике, где о них не упоминается вообще или в лучшем случае только в качестве названия. В одних случаях их называют «химическими ловушками», в других – «маркерами» [1. С. 65].

Цифровые следы, в отличие от следообразующих, очень хорошо маскируются, их легко удалить или скрыть преступникам в попытке бегства, уничтожения следов своего присутствия и в связи с преступным поведением.

На сегодняшний день в криминалистике предлагается широкий спектр методов и средств для восстановления удаленных преступниками данных. Специалисты по работе с цифровыми следами используют новейшие достижения науки и техники, работают с дисками, с поврежденными файлами, неисправными носителями информациями, восстанавливают утраченные или удаленные файлы и получают доказательства.

В отличие от цифровых, криминалистические следообразующие средства подразделяются на красящие, люминесцирующие, запаховые, сигнальные, радиационные, комплексные.

В настоящее время имеется перечень серийных следообразующих средств, используемых в криминалистике. Они формируются на НПО «Спецтехника и связь» МВД России, а также иных предприятиях. Например, в городе Подольск выпускаются средства, позволяющие устанавливать различные следы, что способствует предотвращению краж, грабежей, разбойных нападений. Особенно часто встречаются денежные куклы «Кукла» и «Кукла-С» с красящим составом, слезоточивым составом, а также с составом для использования цветочного дыма. Для подачи сигнала тревоги и маркировки преступника может применяться кукла «Керн-МГД». При этом денежная кукла по внешнему виду ничем не привлекательна, представляет собой пачку денег, в которой из настоящих денег только две наружные купюры, а внутри спрятаны не настоящие денежные знаки, а напечатанные на обычном принтере. В большинстве случаев такие куклы используются для совершения мошеннических действий.

В результате совершенствования методики ведения борьбы с коррупцией в нашей стране активно применяются маркирующие средства. В криминалистике их именуют фломастерами «М» и «К». Их предназначение состоит в нанесении опознавательных меток, которые позволяют идентифицировать подлинные денежные средства, документы, изделия из кожи, траки и многие иные товары [2. С. 67].

Обнаружение проставленных обозначений при помощи маркеров можно осуществить при помощи ультрафиолетовых осветителей, которые при помощи голубого свечения позволяют установить неправомерные действия, к примеру, передачу денежных средств.

Современные реалии развития общества в условиях цифрового технического прогресса не могут не принимать во внимание анализ криминалистических положений дня сегодняшнего, и тем более при развитии направлений развития криминалистики будущего.

Цифровые технологии активно применяются и используются в криминалистике наряду с привычными способами и средствами обнаружения преступных действий злоумышленников. Изучение виртуальных следов, умных устройств, цифровых носителей, устройств с беспроводной связью, роботов-помощников, способствуют пересмотру привычных для нас средств и наборов криминалистики.

Технологии искусственного интеллекта активно внедряются во все отрасли и сферы государственной и общественной жизни. Для нас становятся привычными

такие действия, как восстановление утраченного пароля, восстановление удаленных данных, распознавание запороленных сайтов, фильтрация файлов, визуализация доказательств, сетевой анализ, и многое другое [3. С. 159–169].

Многие вопросы обеспечения безопасности участников досудебного производства в уголовном процессе решаются с учетом применения и использования новейших технологий, позволяющих не только защитить информацию, но и сведения об участвующих в деле лицах.

В современных условиях, анализируя меняющуюся следственную ситуацию, следователь должен переработать огромный массив информации, выделить из нее криминалистически значимую и не допустить при этом ошибок. При расследовании конкретного дела в компьютер в диалоговом режиме вводятся сведения о составе и способе преступления, предмете преступного посягательства, потерпевшем и т. д. После обработки на экран выдаются рекомендации, которые могут быть использованы в планировании расследования, позволяют выбрать данные по эпизодам, по их участникам, подсказывают как осуществить конкретное следственное действие, произвести поиск и сопоставление эпизодов, фамилий, дат и прочих материалов [4. С. 67].

В целях более активного внедрения цифровых и технико-криминалистических средств в практическую деятельность для раскрытия и расследования преступлений о них нужно говорить, писать, проводить семинары, одним словом поддерживать тесную взаимосвязь с руководителями ЭКУ, проводить анализ их деятельности с руководителями и практических оперативных аппаратов соответствующих подразделений.

Представляется, что применение таких средств в соответствии с их предназначением, скажется на обеспечении правовой гарантии безопасности личности, лиц, вовлеченных в орбиту уголовно-процессуального расследования и, как следствие, улучшит раскрываемость по делам о коррупции, кражах, хищениях и других преступлениях.

Список литературы

1. Криминалистические средства и методы собирания доказательств: учеб. пособие для бакалавров / под ред. Е. П. Ищенко. М.: Проспект, 2017.

2. Криминалистика. Конспект лекций. Учебное пособие / Лавров В. П., Шалимов А. Н., Романов В. И., Рахматуллин Р. Р. / под ред. Лаврова В. П. М: Изд-во «Проспект», 2020.

3. Романова Г. В. Информационные технологии в деятельности следователя // Вестник Волжского университета имени В. Н. Татищева. 2023. Т. 1, № 2. С. 159–169.

4. Романова Г. В., Романов В. И. Применение средств криминалистической техники в свете новых информационно-компьютерных технологий // Развитие научных идей профессора Р. С. Белкина в условиях современных вызовов (к 100-летию со дня рождения): сборник научных статей по материалам Международной научнопрактической конференции «63-и криминалистические чтения» (Москва, 20 мая 2022 г.): в 2 ч. / редкол.: Ю. В. Гаврилин, Б. Я. Гаврилов, С. Б. Россинский, Ю. В. Шпагина. М.: Академия управления МВД России, 2022. Ч. 2. С. 67–72.

Г. В. Романова,
кандидат юридических наук,
Казанский институт (филиал) Всероссийского государственного
университета юстиции (РПА Минюста России)

К ВОПРОСУ О СОБИРАНИИ ЦИФРОВОЙ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация. Проблематика цифровой информации очень часто связана с применением многочисленных электронных носителей. Общество зависит от цифрового ресурса, способного облегчить жизнь населения. Цифровые технологии с каждым новым днем увеличивают ценность информации, воспринимаемой людьми. В настоящей статье исследуются особенности и проблемы сбора цифровой информации в части доказывания по уголовному вопросу.

Ключевые слова: цифровая информация, доказательство, уголовное дело, следственные действия, цифровой носитель, информационный ресурс

ON THE ISSUE OF COLLECTING DIGITAL INFORMATION IN PROVING CRIMINAL CASES

Abstract. The problems of digital information are gradually finding a response in the theory of modern law with the development of electronic document management and the number of electronic media used to ensure it. This makes it necessary to study digital information in proving criminal cases, the specifics of their use in criminal proceedings. The article discusses the issues of collecting digital information in proving criminal cases.

Keywords: digital information, evidence, criminal case, investigative actions, digital media, information resource

Современный период развития информационных систем в обществе позволил расширить информационное пространство, активно использовать средства и ресурсы интернет-технологий. Цифровое информационное поле определяется преимущественно инфраструктурой, современными средствами коммуникации, позволяющими пользователям активно общаться между собой, а также собирать, анализировать и использовать полученные сведения. Оно формирует определенное пространство, в котором содержатся информация, сведения, технологии, направленные на получение информации.

Отсутствие цифрового информационного ресурса не позволяет окончательно сформировать и обеспечить все элементы уголовно-процессуального доказывания. Если доказательства получены сотрудниками правоохранительной системы с нарушением, то они не могут применяться в уголовном судопроизводстве.

Познавательная деятельность субъекта доказывания фактически начинается с собирания доказательственной информации, введения такой информации в уголовный процесс.

В теории уголовно-процессуального права собирание доказательств означает отдельный этап, направленный на поиск необходимой информации, объясняющей произошедшее преступное событие.

Сам по себе сбор цифровой информации – сложный процесс, включающий в свое содержание поиск, изучение и оформление полученного информационного ресурса как доказательства по уголовному делу. Собирание цифрового ресурса предусматривает широкий диапазон поиска, исследование материального носителя, изъятие сведений, их транспортировку, хранение. Причем, следует помнить, что не каждая цифровая информация может стать доказательством по уголовному делу, а только та, что относится к изучаемому преступному событию.

Цифровая информация собирается при помощи следственных и иных процессуальных действий. При этом федеральный законодатель не всегда учитывает изменения современного общества, его потребности. В этой связи проблематика прослеживается в используемой трактовке «электронный носитель», которая не совсем понятно отражает его правовую сущность, пренебрегая терминами «электронный» и «цифровой» носитель (пункт 5 части 5 статьи 82 УПК РФ) [1]. На наш взгляд, такие изменения необходимы, так как для доказывания по уголовному делу важна сама цифровая информация, а не сам ее носитель.

В качестве следующей проблемы обратим внимание, на чем сказывается отсутствие порядка получения электронной, цифровой информации. В процессе обыска, осмотра, выемки следователь может обнаружить и правильно оформить цифровой ресурс, способный стать доказательственной основой в уголовном деле.

В научной среде очень часто обсуждается вопрос о необходимости привлечения специалиста при изъятии цифрового ресурса как носителя важной информации по уголовному делу. Р. А. Белкин обращает внимание на то, что законодатель допускает возможность изъятия цифрового носителя в процессе производства обыска и выемки. Такое действие может потребовать значение технических устройств, а также владение специальными познаниями в области программного обеспечения [2. С. 59].

Как нам видится приглашение специалиста при изъятии устройства, содержащего цифровую информацию, позволяет обеспечить право владельца технического устройства на получение хорошей копии, которой в дальнейшем можно будет пользоваться.

Как представляется собирание цифрового информационного ресурса рассматривается в качестве перспективного направления, способного стать востребованным в силу развития современных информационных технологий. Цифровые ресурсы помогают скомпоновать доказательственную основу и стать незаменимым помощником в поиске компрометирующих сведений относительно лица, совершившего преступление.

Иная сторона проблематики содержит обоснованное требование того, что цифровое доказательственное назначение информации должно быть законным. Не должны нарушаться требования допустимости доказательств с учетом всех пожеланий федерального законодателя.

В процессе собирания цифровой информации следователь в ходе осмотра цифрового носителя вынужден использовать технические устройства, помогающие ему ознакомиться с такой информацией. В большинстве случаев ошибки происходят из-за невнимательности следователя при осмотре цифрового носителя, содержащего сведения необходимые в процессе расследования. Простое наблюдение цифрового

носителя не может стать полноценным его осмотром. Информация, содержащаяся на сложном техническом устройстве (компьютере, планшете, смартфоне), которая отображается на экране, не считается цифровой. Ее следует воспринимать и относить к разряду цифровых следов.

Осматривая техническое устройство, считывая информацию на мониторе, следователь изучает не саму цифровую информацию, а только ее проекцию. Это связано с техническими характеристиками, цифровыми кодами, работой компьютерных программ, способных распознавать различные сигналы, преобразуя их в определенное состояние.

Обработка цифровых носителей позволяет пользователю изучить текст, который появляется на экране. Любая допущенная программой ошибка может сделать информацию не читабельной, бессмысленной и не воспринимаемой окружающими.

Цифровую информацию отличают при помощи цифровых следов, способных предоставить сведения, интересующие следствие, при помощи специальных сигналов. В этой связи преобразование цифрового ресурса считается важным шагом в обработке информации, получения данных, сведений, способных нести в себе цифровой код и быть значимым в процессе расследования уголовного дела.

Судебная практика имеет большой накопленной опыт, согласно которому собирание цифрового информационного ресурса в процессе следственного действия (например, осмотре) может производиться без приглашения специалиста. Но речь идет только о простых случаях, не требующих специальных познаний с работой технических устройств и использования программного обеспечения [3–6].

В большинстве случаев суды настаивают на приглашении специалиста при сборе цифровой информации с электронного носителя, только если есть риск потери ее доказательственного свойства.

На наш взгляд, к привлечению специалиста нужно подходить индивидуально в каждом случае, с учетом требований уголовно-процессуального закона (ч. 1 ст. 168 УПК РФ), основываясь на собственном опыте и навыках работы с техническими устройствами. В случае появления риска потери цифровой информации с электронного носителя (диска, облачных серверов, удаленных носителей и т. д.), незамедлительно приглашать специалиста.

В заключение хотелось бы обратить внимание на огромную ценность цифровой информации в уголовном судопроизводстве, способной раскрыть цифровой код и рассекретить сведения цифрового носителя. Собирание цифровой информации связано с изучением работы сложных технических устройств, познанием этапов преступной деятельности человека в цифровой реальности. Любое доказательство может быть получено только путем проведения следственных и иных действий в рамках установленного законом порядка. Поскольку цифровая информация, по крайней мере при рассмотрении вопроса о признании ее доказательством по уголовному делу, не может существовать отдельно от материального носителя, а он признаваться способом выражения ее в материальном мире, то и порядок собирания такой информации будет происходить с учетом специфических свойств вещественных и документальных доказательств.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации. М.: Проспект, 2023.
2. Белкин А. Р. Теория доказывания в уголовном судопроизводстве. Ч. 2. М.: Юрайт, 2017. С. 59.
3. Апелляционное определение Свердловского областного суда от 8 августа 2016 г. по делу № 22–6494/2016.
4. Апелляционный приговор Свердловского областного суда от 15 июня 2016 г. по делу № 22–4973/2016.
5. Апелляционное постановление Приморского краевого суда от 4 августа 2015 г. по делу № 22–4519/2015.
6. Апелляционное постановление Московского городского суда от 7 октября 2013 г. по делу № 10–9861.

З. И. Сагитдинова,
кандидат юридических наук, доцент,
Уфимский университет науки и технологий

«ИННОВАЦИОННАЯ» ПРЕСТУПНОСТЬ: ПОСТАНОВКА ПРОБЛЕМЫ

Аннотация. Преступность была и остается частью современного общества, а потому в своем развитии проходит те же этапы, что и общество в целом. Цифровизация жизнедеятельности общества не могла не оказать своего влияния и на преступное поведение человека. В настоящей публикации рассмотрен вопрос о том, как меняются преступность в условиях перехода к инновационному типу развития общества и стоящие перед государством задачи.

Ключевые слова: уголовное право, цифровые технологии, преступность, цифровизация преступности, инновационная преступность, социальная инженерия, дистанционный способ совершения преступления

«INNOVATIVE» CRIME: STATEMENT OF THE PROBLEM

Abstract. Crime has been and remains a part of modern society, and therefore in its development it goes through the same stages as society as a whole. The digitalization of life could not but have an impact on human criminal behavior. In this publication, we will consider the question of how crime is changing in the context of the transition to an innovative type of development of society and what tasks the state faces in this regard.

Keywords: criminal law, digital technologies, crime, digitalization of crime, innovative crime, social engineering, remote way of committing a crime

Преступность как непреходящий и прирастающий продукт общества [2. С. 922], как социальное явление, которое входит в систему соответствующего общества и мирового сообщества в целом, социальна по происхождению, по причинам и условиям [1. С. 46–47], которые носят экономический, социальный, социально-психологический и т. п. характер [1. С. 75–77; 2. С. 488–594;].

Для начала определимся в базовых понятиях и, не прибегая к их общесмысловым значениям, обратимся к дефинициям нормативного уровня. Так, согласно Федеральному закону от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике», инновационная деятельность – это деятельность (включая научную, технологическую, организационную, финансовую и коммерческую деятельность), направленная на реализацию инновационных проектов, а также на создание инновационной инфраструктуры и обеспечение ее деятельности, в свою очередь, инновационный проект направлен на достижение экономического эффекта от мероприятий по осуществлению инноваций, под которыми понимается введенный в употребление новый или значительно улучшенный продукт (товар, услуга) или процесс, новый метод продаж или новый организационный метод в деловой практике, организации рабочих мест или во внешних связях. Подобный подход к пониманию инноваций и инновационной деятельности прослеживается и в подзаконных нормативных актах (см., например: Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утв. Указом Президента РФ от 9 мая 2017 г. № 203; Стратегия инновационного развития Российской Федерации на период до 2020 года, утв. Распоряжением Правительства РФ от 8 декабря 2011 г. № 2227-р; Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р; Основные направлениях политики Российской Федерации в области развития инновационной системы на период до 2010 года, утв. Правительством РФ 5 августа 2005 г. № 2473п-П7; Стратегия развития науки и инноваций в Российской Федерации на период до 2015 года, утв. Межведомственной комиссией по научно-инновационной политике 15 февраля 2006 г. и др.). Естественно, что не только Россия, но и другие государства мира ориентированы на инновационное развитие своих экономик и общества. Характерной чертой современного мирового развития является переход ведущих стран к новому этапу формирования инновационного общества – построению экономики, базирующейся преимущественно на генерации, распространении и использовании новых знаний, техники, технологий. И в этом процессе ключевым элементом является применение достижений науки, техники и технологий для реализации генеральной цели – получения социально-полезных результатов.

Однако в обществе всегда находятся люди, готовые и стремящиеся использовать продуцируемые другими людьми новые знания, технику, технологии в своих преступных целях. При этом в качестве причин таких «инновационных» преступлений, то есть совершаемых с использованием новых знаний, техники, технологий, выступают присущие таким людям антиобщественные свойства личности – детерминанты, благодаря которым происходит выбор в пользу общественно опасных способов для целей удовлетворения потребностей; эти причины носят криминогенный социально-психологический характер. Но не стоит, на наш взгляд, отрицать и существование такой детерминанты «инновационной» преступности, как ее условие – появление и распространение инноваций. Подчеркнем, мы не усматриваем прямой корреляции между возникновением «инновационной» преступности» и инновационным развитием общества, но само существование инноваций может стать криминогенным фактором, способствующим формированию преступной

мотивации у лиц с криминогенно-деформированной психологий, не отрицающих возможность и допустимость выбора общественно опасного типа поведения.

Например, такие известные во все времена и всем странам преступления, как кража и мошенничество сегодня совершаются не только традиционными способами и не только с изъятием традиционного имущества (вещей, наличных денег). Широкое распространение получили хищения безналичных денежных средств, совершаемых путем дистанционного воздействия на элементы банковской системы (например, банковский счет, электронный кошелек). Этому способствует появление электронных форм платежей, SMS-банкинга, АТМ-банкинга (использование банкомата и платежной карты). Нередко они совершаются с использованием специальной техники и специальных информационно-телекоммуникационных технологий (к примеру, банковских троянов). В 2017 г. Генеральным Прокурором Ю. Я. Чайкой в официальную статистику было введено обобщенное понятие «Преступления, совершенные с использованием современных (информационно-телекоммуникационных) технологий», или ИТП. По данным официальной статистики МВД России, при совершении каждого четвертого преступления в 2022 г. были использованы информационно-телекоммуникационные технологии, в том числе в 73 % случаев злоумышленники воспользовались сетью «Интернет» [6]. За последние десять лет почти в 50 раз выросло число ИТП, при этом реальное число таких преступлений в три раза больше регистрируемого.

Все достижения IT-сферы весьма эффективно используются в противоправных целях. Так, в России в 2011–2015 гг. получило достаточно широкое распространение преступление с условным названием «скимминг», для которого характерно использование специального технического устройства – скиммера (картридера), предназначенного для считывания информации с магнитной ленты держателя банковской карты, видеокамеры для фиксации вводимых ПИН-кодов, энкодера – устройства для чтения/записи информации на магнитную полосу пластиковых карт и компьютера, все это оборудование предназначено для изготовления дубликата банковской карты и хищения денежных средств из банкоматов [1, 5]. Величайшее изобретение человечества – сеть Интернет, без которой мы уже не мыслим свою жизнь, уже примерно два десятилетия используется преступниками как средство совершения преступлений, а развитие интернет-технологий ведет к тому, что уровень «сетевой» преступности постоянно повышается и «совершенствуется». Например, технология TOR (The Onion Router) – это программное обеспечение, которое позволяет использовать сеть «Интернет» абсолютно анонимно за счет прохождения информации через целый ряд слоев. Создаваемый «луковичным» маршрутизатором уровень анонимности дает колоссальные возможности совершать массу преступлений – торговлю наркотическими средствами и психотропными веществами, оружием, поддельными документами, распространение порнографических материалов и предметов, найм убийц и т. п., не попадая в поле зрения правоохранительных органов. С появлением одной из наиболее значимых инноваций современности – криптовалюты, приобретающей большую популярность в качестве объекта инвестиций и средства расчетов, появились и общественно опасные деяния, совершаемые с ней как с предметом и средством преступления.

Нейротехнологии – одна из групп сквозных технологий, которые предназначены для улучшения функций мозга путем воздействия на нервную систему человека, одновременно могут умышленно использоваться в целях, противоречащих интересам человека, а также их применение может причинить по неосторожности вред его здоровью или даже смерть. Развитие робототехники, появление на дорогах общего пользования беспилотных транспортных средств (оборудованных системой автоматического управления, передвигающихся без участия человека), с одной стороны, социально полезно, что связано с их экономичностью, комфортом, повышением технологичности процесса управления транспортом, минимизацией участия в нем человеческого фактора (поэтому и проводится сейчас эксперимент по использованию на дорогах общего пользования высокотехнологичных транспортных средств [4]), а с другой стороны, ставят их в ряд источников повышенной опасности, способных стать предметом совершения неосторожных дорожно-транспортных преступлений. Так, стоит упомянуть о смертельном ДТП, причиной которой стал неуправляемый электрокар «Тесла» [7], и вопрос, кто понесет ответственность (в том числе уголовную), остается на данный момент открытым.

Перечень примеров «инновационных» преступлений может быть продолжен, но и приведенных, как думается, достаточно для вывода о том, что в условиях инновационного развития общества появляется и модифицируется «инновационная» преступность, в связи с чем, на наш взгляд, перед государством стоят как минимум две задачи в сфере уголовного права. Во-первых, своевременная и беспробельная криминализация «инновационных» общественно опасных деяний, пока не могущих считаться преступлениями в силу отсутствия уголовно-правового запрета на их совершение (см. выше примеры с криптовалютой и электромобилями), но причиняющих либо способных причинить существенный вред личности, обществу, государству, и имеющих достаточную распространенность. Во-вторых, выработка единой национальной правоприменительной политики в части квалификации «инновационных» преступлений (см. выше примеры хищений с использованием IT-технологий), которые в силу их технической или технологической составляющей в настоящее время вызывают квалификационные проблемы.

В настоящее время преступность качественно модифицировалась, и уже на международном уровне признано, что «новые вызовы преступного мира, а также увеличивающаяся сложность определенных видов преступности обусловлены быстрым развитием новых технологий…» (Заключение Консультативного совета европейских прокуроров № 7(2012) от 11 декабря 2012 г., пункт 19). Таким образом, сопутствующим негативным явлением инновационного развития общества в современный период становятся «инновационные» преступления, которые, в отличие от преступлений, традиционно существующих во все времена и во всех странах, требуют новых подходов к уголовно-правовому реагированию на них на национальных уровнях. С учетом транснационального характера большинства преступлений, составляющих «инновационную» преступность, желательно задействовать в уголовно-правовой борьбе с ней и наднациональный уровень для унификации национальных подходов к установлению преступности и наказуемости таких «инновационных» общественно опасных деяний.

Список литературы

1. Кассационное определение Московского городского суда от 11 февраля 2023 г. № 22–552/2013 // СПС «КонсультантПлюс».
2. Криминология: учеб. пособие / Г. И. Богуш, О. Н. Ведерникова, М. Н. Голоднюк и др.; науч. ред. Н. Ф. Кузнецова. М.: Проспект, 2010. 496 с.
3. Лунеев В. В. Курс мировой и российской криминологии: учебник. В 2 т. Т. I. Общая часть. М.: Юрайт, 2011. 1003 с.
4. Постановление Правительства РФ от 26 ноября 2018 г. № 1415 «О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств» // СПС «КонсультантПлюс».
5. Приговор Советского районного суда г. Красноярска от 20 октября 2020 г. по делу № 1–972/2020 // База судебных актов, судебных решений и нормативных документов «Судебные и нормативные акты РФ». URL: http://sudact.ru/regular/doc/JaQ4gdOGV8ZA
6. Состояние преступности в России за январ. декабрь 2022 года. М., 2023. С. 30–31 // Официальный сайт МВД России. URL: file:///C:/Users/user/Downloads/Sbornik_22_12%20(1).pdf
7. Out of control Tesla speeds through Chinese streets, killing two people and injuring three others. URL: www.dailymail.co.uk/news/article-11423865/Out-control-Tesla-speeds-Chinese-streets-killing-two-people-injuring-three-others.html

В. Ф. Саетгараев,
преподаватель,
Казанский юридический институт
Министерства внутренних дел
Российской Федерации

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ КОРРУПЦИИ

Аннотация. В статье анализируются тенденции и возможности использования цифровых технологий в деятельности органов внутренних дел по противодействию коррупции, акцентируется внимание на взаимодействии с гражданским обществом посредством различных информационно-телекоммуникационных платформ. Особое внимание уделяется положениям нормативных правовых документов, регламентирующих вопросы цифровой трансформации.

Ключевые слова: противодействие коррупции, цифровые технологии, институты гражданского общества, органы внутренних дел

DIGITAL TECHNOLOGIES IN ANTI–CORRUPTION ACTIVITIES OF INTERNAL AFFAIRS BODIES

Abstract. The article analyzes the trends and possibilities of using digital technologies in the activities of internal affairs bodies to combat corruption, focusing on interaction with

civil society through various information and telecommunication platforms. The provisions of regulatory legal documents regulating issues of digital transformation are analyzed.

Keywords: anti-corruption, digital technologies, civil society institutions, internal affairs bodies

Введение. Цифровые технологии активно проникают во все сферы общественной жизни, включая и сферу противодействия коррупции. Интернет создал среду, которая решает не только информационные задачи, но также является базой для коммуникации и организации совместной антикоррупционной деятельности. Более того, Интернет стал одним из главных инструментов уличения чиновников в коррупционных действиях. Посредством Сети люди получают необходимую информацию, узнают о передовых технологиях, делятся опытом, обнародуют и популяризируют опыт уличения в коррупционной деятельности. С помощью Интернета можно остаться неузнанными, или же стать известными на весь мир [1].

Возможности использования интернет-технологий в сфере противодействия коррупции весьма разнообразны, среди которых выделяются два направления: «первое – это использование глобальной сети как инструмента для коррупционных разоблачений, второе – создание в Интернете всевозможных антикоррупционных объединений, союзов, сообществ и т. д.» [1].

Основная часть. Глобальная сеть позволяет бороться с незаконными действиями чиновников как в одиночку, так и объединяя вокруг себя сторонников такой борьбы. Поэтому все интернет-ресурсы, основная деятельность которых связана с разоблачительством, можно условно разделить на четыре группы:

1. Сайты, осуществляющие анонимные опросы для сбора информации о фактах коррупционной деятельности.

2. Интернет-платформы, созданные для экстренной связи с органами внутренних дел (далее – ОВД).

3. Сайты индивидуальных разоблачителей, которые на своей страничке или в блоге публикуют отдельные случаи взяточничества.

4. Горячие линии различных организаций, осуществляющие сбор информации о коррупционных проявлениях в коммерческих компаниях.

Следует отметить, что деятельность по противодействию коррупции в Интернете должна быть основана, прежде всего, на принципе законности [8]. Из этого следует, что, во-первых, все действия, совершаемые разоблачителями, должны соответствовать действующему законодательству и не выходить за его рамки, а во-вторых, быть законодательно урегулированы со стороны государства. Именно заинтересованность государства в нормативном правовом обеспечении мер противодействия коррупции посредством Интернета должна быть гарантом эффективности деятельности разоблачителей.

Федеральный закон «О противодействии коррупции» признает граждан и институты гражданского общества полноценными субъектами антикоррупционной деятельности [2]. Необходимость участия институтов гражданского общества в вопросах противодействия коррупции нашло свое отражение и в документах стратегического планирования РФ: Концепции общественной безопасности, Стратегиях:

национальной безопасности, экономической безопасности, противодействия коррупции, развития информационного общества, а также Национальных планах противодействия коррупции и других, закрепивших важную роль институтов гражданского общества в защите национальных интересов и реализации стратегических национальных приоритетов России.

К сожалению, действующим российским законодательством правовой статус институтов гражданского общества в полной мере не отражен. Среди главных причин, препятствующих данному процессу, выделяются две:

1. Отсутствие единого понимания сущности институтов гражданского общества с учетом широкого применения данного термина в законодательстве;

2. Как следствие из первой причины – сложность организации форм антикоррупционной деятельности.

Рассматривая сущность институтов гражданского общества, на наш взгляд, наиболее точно ее раскрыл Ю. А. Тихомиров, определяя, что это обусловленный конституционными принципами народовластия и приоритета прав и свобод человека и гражданина структурно-правовой способ легального самовыражения и социализации личности; способ непосредственного выражения мнений, предложений, позиций граждан по вопросам общественной жизни; способ прямого участия в принятии социально значимых решений [3]. Заслуживает внимания позиция Н. Н. Никитиной, раскрывающая сущность институтов гражданского общества как разнообразных способов организационно-правового участия в социально-политической жизни общества и, прежде всего, способ коммуникации общества с государством для реализации определенных целей [4]. Автор отмечает, что общество находится на пороге своего нового качественного изменения, связывая это с развитием современных цифровых технологий и средств коммуникации, цифровизацией социального пространства [5]. Тем самым можно констатировать, что институты гражданского общества уже представляются не в традиционном виде (общественных объединений, организаций и т. д.), а в форме сообществ, групп, форумов в социальных сетях, мессенджерах. Развитие информационных технологий дает широкие возможности для социальной активности граждан в общественной жизни посредством ресурсов виртуального пространства, где наблюдается широкое развитие сетевых сообществ. Как уже отмечалось выше, важным критерием институтов гражданского общества являются способы коммуникации, а сетевизация способствует развитию гражданского общества.

Научный мир заявляет, что на современном этапе в условиях глобализации появляется глобальное гражданское общество [5. С. 12], на формирование которого оказывает влияние развитие современных информационных технологий. Развивается виртуальное пространство, идет процесс цифровизации общественных отношений, все это порождает новые способы коммуникаций как между людьми, так и между институтами: государственными и общественными. Данные тенденции ведут к образованию так называемого электронного гражданского общества.

Изменения общественных отношений нашли свое отражение и в законодательстве, так Стратегия развития информационного общества среди основных задач применения информационных и коммуникационных технологий для развития

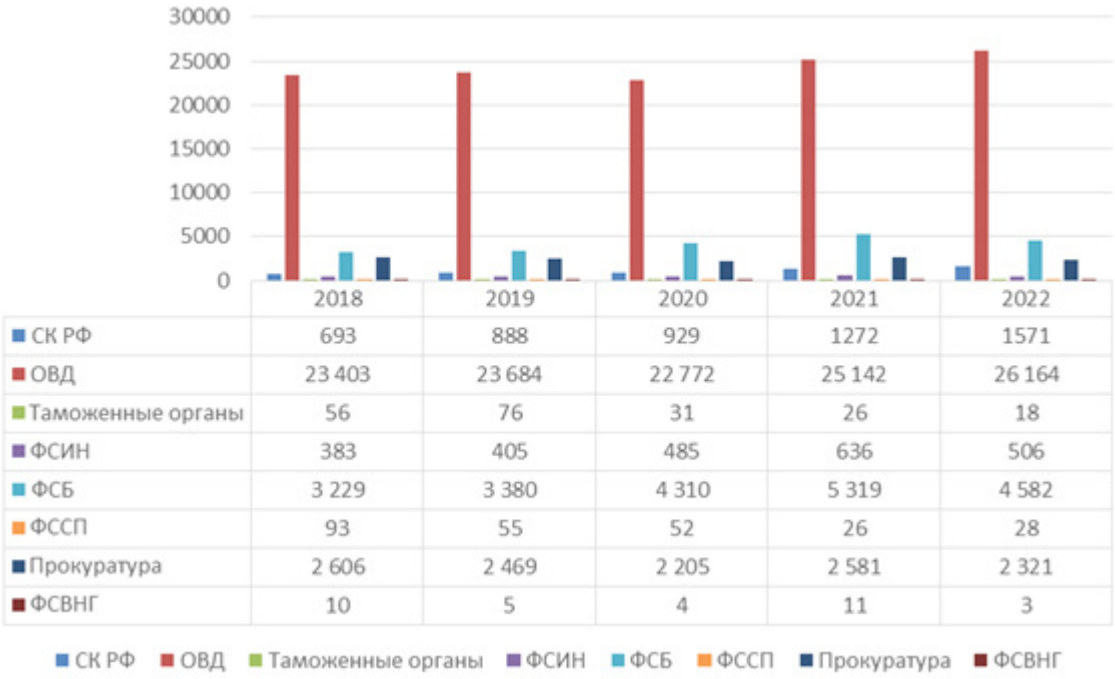
социальной сферы, системы государственного управления, взаимодействия граждан и государства закрепляет развитие технологий электронного взаимодействия граждан, организаций, государственных органов, органов местного самоуправления наряду с сохранением возможности взаимодействия граждан с указанными организациями и органами без применения информационных технологий (п. «д» ст. 40) [6]. Доктриной информационной безопасности РФ закреплено, что система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности РФ и осуществляется на основе сочетания правоохранительной и других форм деятельности государственных органов во взаимодействии с организациями и гражданами (ст. 30) [7].

Несмотря на развитость современного законодательства и передовых технологий сбора информации, эффективно организовать процедуру «внешнего разоблачения» с использованием Интернета не удалось пока ни в одной стране мира, в том числе и в России. Но во многих странах мира уже действуют и продолжают создаваться множество сайтов, которые служат общественности в качестве удобной платформы для объединения в борьбе с коррупцией.

Одной из самых известных интернет-платформ, специализирующихся на «информационной утечке», является сайт Wikileaks. WikiLeaks – некоммерческая организация СМИ, публикующая в Интернете секретную информацию о недобросовестных политических деятелях. Главная цель организации – борьба за прозрачность работы органов власти. Создатели ресурса обеспечивают инновационный, безопасный и анонимный путь к источникам, делают информацию доступной обычным людям, политикам, журналистам по всему миру. Рядом с каждой записью указан адрес первоисточника, чтобы каждый мог видеть исчерпывающие доказательства правдивости новостей. Источником финансирования проекта в основном являются добровольные пожертвования, но известно о весьма крупных организациях, которые также осуществляют финансовую поддержку WikiLeaks [1].

Среди основных направлений противодействия коррупции (профилактика, борьба и минимизация (ликвидация) наиболее сложным и ресурсоемким в осуществлении выступает процесс борьбы с данными преступлениями, в который задействован весь правоохранительный блок страны, основную же нагрузку по количеству выявленных преступлений коррупционной направленности среди них на протяжении многих лет, традиционно несут на себе ОВД как наиболее крупная правоохранительная структура (рис.).

Взаимодействие ОВД с институтами гражданского общества в противодействии коррупции требует системной организации, отвечающей современному генезису общественных отношений. Правоприменительная практика ОВД противодействия коррупции диктует необходимость построения инновационной модели совместной работы ОВД с заинтересованными институтами гражданского общества. Сущность данной модели состоит в использовании разнообразных коммуникационных путей сбора и накопления актуальной информации о коррупционных проявлениях, дальнейшего ее анализа с использованием современных информационных технологий [11].



	2018	2019	2020	2021	2022
СК РФ	693	888	929	1272	1571
ОВД	23 403	23 684	22 772	25 142	26 164
Таможенные органы	56	76	31	26	18
ФСИН	383	405	485	636	506
ФСБ	3 229	3 380	4 310	5 319	4 582
ФССП	93	55	52	26	28
Прокуратура	2 606	2 469	2 205	2 581	2 321
ФСВНГ	10	5	4	11	3

Рис. Сведения о количестве преступлений коррупционной направленности, выявленных субъектами учета

Взаимодействие ОВД с институтами гражданского общества в противодействии коррупции требует системной организации, отвечающей современному генезису общественных отношений. Правоприменительная практика ОВД противодействия коррупции диктует необходимость построения инновационной модели совместной работы ОВД с заинтересованными институтами гражданского общества. Сущность данной модели состоит в использовании разнообразных коммуникационных путей сбора и накопления актуальной информации о коррупционных проявлениях, дальнейшего ее анализа с использованием современных информационных технологий [11].

Одной из перспективных площадок сотрудничества ОВД с институтами гражданского общества по противодействию коррупции выступает «Цифровая платформа приема обращений предпринимателей» – «За бизнес» [9]. Платформа представляет собой электронный ресурс для приема обращений предпринимателей в связи с оказанием на них давления со стороны правоохранительных органов. МВД России через уполномоченные подразделения рассматривает поступающие через платформу обращения и дает заключения о правомерности действий своих сотрудников, остальные партнеры проекта (уполномоченный по правам предпринимателей, различные деловые объединения) осуществляют экспертную поддержку и общественный контроль за рассмотрением обращений.

Заключение. Предполагается, что кардинальное повышение эффективности противодействия коррупции возможно через цифровую трансформацию данной сферы государственного управления как новый способ противостояния данной глобальной проблеме. Среди целей цифровой трансформации Правительством Российской Федерации обозначено сокращение теневой экономики, взаимосвязанной с коррупцией. Основу этих действий составляют мероприятия, направленные

на развитие информационно-коммуникационных технологий, а также на вывод из эксплуатации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры [10].

Цифровизация организации деятельности ОВД Российской Федерации выступает эффективным средством противодействия коррупции. Современные технологические возможности позволяют совершенствовать ведомственную антикоррупционную политику, укреплять доверие к полиции, повышать правосознание общества на основе вовлечения участия институтов гражданского общества. Цифровые технологии выступают важным элементом цифровой трансформации, которые позволяют реализовывать электронное взаимодействие ОВД с институтами гражданского общества. Это повышает возможности оперативного обмена актуальной информацией для формирования объективной картины совокупных проблем и организационно-управленческих отношений.

В настоящее время уже заложены правовые основы цифровизации различных общественных отношений, однако дальнейший процесс цифровой трансформации антикоррупционной политики МВД России требует предметного исследования, анализа и оценки возможностей внедрения в данную сферу новых технологий. Все это требует модернизации правового регулирования возникающих общественных отношений, поскольку законодатель не всегда успевает реагировать на появление новых объектов правоотношений.

Список литературы

1. Бурова, Д. А. Интернет в сфере противодействии коррупции: разоблачительство и социальные сети / Д. А. Бурова // Электронный научно-публицистический журнал «Homo Cyberus». 2018. № 1(4). URL: http://journal.homocyberus.ru/internet_technologies_against_corruption_whistleblowing_and_social_networks?yscli d=lmg81xnsyl504717766

2. О противодействии коррупции: федеральный закон от 25.12.2008 № 273-ФЗ // Собрание законодательства РФ. 29.12.2008. № 52 (ч. 1). Ст. 6228.

3. Тихомиров Ю. А. Гражданское общество в фокусе права // Журнал российского права. 2013. № 10. С. 35–45.

4. Никитина Е. Е. Система институтов гражданского общества в России: конституционно-правовой аспект // Журнал российского права. 2017. № 6. С. 40.

5. Никитина Е. Е. Конституционно-правовые основы институционализации гражданского общества в Российской Федерации: монография. М.: 2019. С. 11–12.

6. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: утверждена Указом Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

7. Доктрина информационной безопасности Российской Федерации: утверждена Указом Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

8. Противодействие коррупции: новые вызовы: монография / отв. ред. Т. Я. Хабриева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Инфра-М, 2018.

9. За бизнес. Цифровая платформа для работы с обращениями предпринимателей. URL: http//забизнес.рф.

10. О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» (вместе с «Положением о ведомственных программах цифровой трансформации»): постановление Правительства РФ от 10.10.2020 № 1646 // Собрание законодательства РФ. 2020. № 42 (часть III). Ст. 6612.

11. Мальцева А. К., Хазов И. О., Борякин Д. В. Роль СМИ и сети интернет в антикоррупционной деятельности государства // Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок молодых ученых. В 5-ти томах. Т. 2. Отв. редактор А. А. Горохов. Курск: Юго-Западный государственный университет (Курск), 2020.

А. Б. Сергеев,
доктор юридических наук, профессор,
Челябинский государственный университет
А. Г. Гильмутдинова,
аспирант,
Челябинский государственный университет

ЦИФРОВОЙ РУБЛЬ КАК ПОВОД К НАЧАЛУ РАЗРАБОТОК НОВОГО НАПРАВЛЕНИЯ В СОЗДАНИИ ЧАСТНЫХ МЕТОДИК РАССЛЕДОВАНИЯ НАЛОГОВЫХ ПРЕСТУПЛЕНИЙ

Аннотация. Эволюционный процесс развития цифровых финансовых активов, цифровой валюты перед государством ставит цель придать этому процессу управляемость и определенность. Важность решения задачи связана с восполнением государством финансового ресурса посредством сбора налогов и минимизации угрозы преступных проявлений в этой сфере. Задача – на основе краткого анализа предпринятых законодателем мер в достижении названной цели государства выявить факторы сдерживания и перспективы создания эффективного механизма правового регулирования процесса развития цифровых финансовых средств. В заключение делается вывод о позитивности динамики урегулирования отношений в сфере использования цифровых финансовых активов, цифровой валюты, цифрового рубля. Указывается на необходимость начать научные исследования по созданию криминалистического обеспечения – разработки методик выявления и раскрытия преступлений с использованием цифровых финансовых активов, валюты, рубля.

Ключевые слова: правовой механизм регулирования, налоги, методика расследования, криптовалюта, цифровой рубль

DIGITAL RUBLE AS A REASON TO START DEVELOPING A NEW DIRECTION IN THE CREATION OF PRIVATE METHODS OF INVESTIGATION OF TAX CRIMES

Abstract. The evolutionary process of development of digital financial assets, digital currency, aims to give this process manageability and certainty to the state. The importance of solving the problem is connected with the replenishment of financial resources by the state through tax collection and minimizing the threat of criminal manifestations in this area. The purpose of the article is to identify deterrence factors and prospects for creating an effective mechanism for legal regulation of the process on the basis of a brief analysis of the measures taken by the legislator to achieve the goal. In conclusion, the conclusion is made about the positive dynamics of the settlement of relations in the sphere of the use of digital financial assets, digital currency, digital ruble. It is indicated that it is necessary to start scientific research on the creation of forensic support – the development of methods for detecting and solving crimes using the digital ruble.

Keywords: legal mechanism of regulation, taxes, investigation methodology, cryptocurrency, digital ruble

Развитие товарно-денежных отношений – процесс эволюционный и находится в неразрывном единстве и характеризует развитие самого общества. На современном этапе товарно-денежные отношения активно развиваются на основе криптовалютных технологий, блокчейна. Раз цифровое пространство все более адаптируется к расчетно-денежным отношениям и этот процесс объективно неизбежен [3. С. 3–8], то важной задачей государства становится создание правовой базы, которая позволяла бы весь процесс расчетных операций взять под контроль. Эффективный финансовый контроль обеспечивал бы прозрачность экономических правоотношений, вывел бы из теневого сектора уводимые от налогов результаты предпринимательской деятельности, позволил бы достичь важного результата – обеспечить реализацию конституционного положения об обязанности лиц, занимающихся предпринимательской деятельностью уплачивать налоги. Однако до настоящего времени законодателю не удалось достичь такого правового уровня, правовой механизм находится в процессе разработки. Правовой пробел, вызванный несформированным пониманием законодателя, как цифровое пространство можно урегулировать юридическими средствами, для государства представляет существенную опасность. Не контролируемое цифровое пространство с множеством расчетных операций:

а) заставляет государственную финансовую систему конкурировать с расчетами, производящимися посредством «цепочки набора цифр», и остающимися для налоговых органов невидимыми. Такое «состязательное» положение существенно ограничивает наполнение денежными средствами все виды налоговых отчислений, ослабляет государство экономически, способствует развитию инфляционных процессов;

б) снижает эффективность правоохранительных органов по выявлению преступных групп, финансовые средства расчетов за преступную деятельность которых «теряются» в полностью обезличенном цифровом пространстве виртуальной валюты;

в) используется в качестве формы вывода денежных средств в другие страны, легализации преступно приобретенного [5. С. 85–87];

г) может стать способом финансирования недружественных стран [4. С. 82].

Анализ законотворческой деятельности показывает, что законодатель предпринимает попытки упорядочить отношения в цифровом пространстве посредством закрепления способов, делающими более открытыми схемы расчетной деятельности. Анализ правотворческого процесса в этом направлении позволяет утверждать, что в России, в конечном счете, задача будет решена. Будет создан правовой механизм, в том числе по вопросу реализации конституционного установления (ст. 57 Конституции). Важным шагом в этом направлении стал Федеральный закон от 03.08.2020 № 259 [8].

Так, условиями официального функционирования финансовых активов на территории Российской Федерации является выполнение требований, чтобы организационно-финансовая деятельность цифрового пространства осуществлялась системно и через Банк России. Системность заключается в наличии у Банка России единого реестра учета операторов (физических или юридических лиц), отвечающих за функционирование своих информационных систем, в которых должны быть размещены цифровые финансовые активы. Банк осуществляет надзор за точным исполнением операторами своих функций по правилам российского законодательства. Без включения в реестр оператор лишен права выпуска цифровых финансовых активов.

Банк России дает оценку разработанным оператором правилам выпуска цифровых активов. Согласовываются алгоритм программ информационной системы каждого оператора, правила внесения изменений в программу. Согласовываются порядок выпуска активов.

Пользователи информационной системы должны следовать согласованным с Банком России правилам работы информационных систем (ст. 5 ФЗ). В свою очередь, операторы информационных систем обязаны создавать свои реестры по учету выпусков цифровых эмиссионных бумаг в своих информационных системах, в том числе реестры учета владельцев цифровых ценных бумаг (ст. 8 ФЗ-259).

Законодательно установленная система организации функционирования цифровых финансовых активов в Российском цифровом пространстве позволяет получать достаточно полную информацию о финансовых операциях с активами и контролировать выполнение конституционного права государства на часть финансовых средств в виде налога. Созданный правовой механизм функционирования цифровых ценных бумаг позволяет и правоохранительным органам организовывать работы по выявлению фактов преступных действий с цифровыми активами [2. С. 67–68].

Если с цифровыми финансовыми активами правовой механизм достаточно успешно проходит апробацию на практике, то в вопросе создания отечественного законодательства по созданию цифровых денежных средств такое продвижение с регулированием не столь определенно. Причина заключается в том, что для пользователей цифровыми денежными средствами намного предпочтительней расположенные вне российской территории площадки по обмену цифровых денежных средств (валюты).

Цифровая форма валюты, создание ее в виртуальной сфере обращения существенно осложняет государству распространить контроль на цифровые денежные средства. Цифровизация финансов и их обращение позволяют:

– размещать в открытом доступе в сети Интернет созданную инициатором программу платежной системы. Количество биткойнов определяется при создании и запуске самой системой. Распределение их не зависит от особенностей системы и определяется активностью участников платформы.

– большое количество организаторов (создателей) таких систем и инициативное их размещение на своих платформах делает цифровую сферу обращения виртуальной (цифровой) валюты децентрализованной, сложной для государственного наблюдения.

– электронные платежи осуществляются без посредников напрямую. Такое положение создает благоприятные условия для обращения в сети средств, полученных в результате преступных действий, в том числе финансирования терроризма, оказания финансовой поддержки националистических режимов и пр.

– автономность способа выхода на криптовалютные площадки (с любого компьютера) не требует каких-либо централизованных каналов, учета, а соответственно, максимально минимизируется риск попасть под наблюдение правоохранительных органов.

Слабые контрольные возможности над обращением цифровых денежных средств у государств, где созданы и функционируют эти площадки, наблюдаются и у России [1. С. 309]. Но так как названный процесс функционирования – процесс объективный и не подпадает под государственное санкционирование, то представляется оправданными попытки законодателя найти способ придания урегулированности этому процессу.

В исследуемом законе в статье 14 предпринята попытка создать основу цифровому обороту валюты.

Главная задача, которую поставил законодатель, заключается в создании территориальности обращения и создания цифровой валюты. Территориальность подразумевает границы Российской Федерации. Рамочные условия заключаются в том, чтобы доменная зона размещалась в России. Такой подход обеспечивает создание отечественных доменных имен и сетевых адресов. Другое условие касается программно-аппаратных средств. Они должны быть размещены на территории России. Закон содержит запрет на обмен криптовалюты на криптовалюту, сформированную за пределами России.

Названный закон, первые результаты его практической реализации показали достаточный потенциал и перспективу развития правового механизма регулирования криптовалютных операций на территории Российской Федерации. Несмотря на большую пробельность правового регулирования такой формы обращения, Федеральным законом от 24.07.2023 № 339 определен порядок расчета цифровыми рублями. Определено, что в ведении Банка России находится право открывать и вести счета граждан в цифровых рублях. Обращение цифровых рублей на специальной платформе обозначено в качестве объекта гражданских прав (ст. 128 ГК РФ, п. 1 ст. 140 ГК РФ) [7].

Изложенное позволяет сформулировать следующие выводные суждения.

1. Федеральным законом ФЗ-259 определен механизм правового регулирования порядка создания и обращения цифровых финансовых активов. Механизм позволяет государству распространить контроль на цифровое пространство функционирования финансовых активов.

Созданы благоприятные условия для своевременного обнаружения нарушения налогового законодательства в данной сфере обращения финансовых активов.

2. Признание государством цифрового рубля в качестве законного платежа своим следствием явит расширение расчетов рубля в этой форме, а следовательно, станет фактором снижения инфляционного процесса. Цифровой рубль как одно из средств платежа может стать предметом рассмотрения возможности уплаты налогов в этой форме денежного знака.

3. Признание законным платежом цифрового рубля ставит задачу перед криминалистическим обеспечением – создание методик [6] выявления и раскрытия преступлений с использованием цифрового рубля.

Список литературы

1. Выскребцев Б. С., Сергеев А. Б. Влияние социокультурной идентичности российского общества на формирование отечественного уголовно-процессуального законодательства и правовые позиции России в европейском суде по правам человека // Евразийский юридический журнал. 2020. № 6 (145). С. 307–310.

2. Зобнин П. А., Ткаченко Н. Б., Сергеев А. Б. Инициирование правоохранительными органами действий лица как способ выявления преступлений: правовая оценка // Российский следователь. 2023. № 8. С. 65–69.

3. Новоселова Л. А. О запрете использования криптовалют в Законе о цифровых финансовых активах // Хозяйство и право. 2021. № 3. С. 3–8.

4. Ображиев К. В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации // Журнал российского права. 2022. № 2. С. 71–87.

5. Сергеев А. Б. Порог легализации денежных средств, приобретенных преступным путем, как критерий уголовной ответственности // Социум и власть. 2012. № 1(33). С. 85–87.

6. Сергеев А. Б. Состояние и перспективы научного разрешения проблем дифференциации и унификации форм уголовно-процессуальных производств // Вестник Челябинского государственного университета. 2014. № 20(349). С. 119–124.

7. Федеральный закон от 24.07.2023 № 339-ФЗ «О внесении изменений в ст. 128 и 140 части первой, часть вторую и ст. 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» // СПС КонсультантПлюс.

8. Федеральный закон от 31.07.2020 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельныезаконодательные акты Российской Федерации» // Собр. законодательства Рос. Федерации. 2020. № 31 (ч. I). Ст. 5018.

9. Янин Д. Г., Сергеев А. Б. Один из аспектов соотношения международного и национального права по вопросу передачи лица, осужденного судом Российской Федерации за экстремизм, для отбывания наказания в государстве, гражданином которого оно является // Соотношение национального и международного права по противодействию национализму, фашизму и другим экстремистским преступлениям: материалы Международной научно-практической конференции посвященной выдающемуся российскому ученому Николаю Сергеевичу Алексееву. 2015. С. 212–215.

С. Н. Титов,
кандидат юридических наук, доцент,
Ульяновский государственный педагогический университет
имени И. Н. Ульянова

ПРЕСТУПЛЕНИЯ, ПОСЯГАЮЩИЕ НА ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, СОЗДАННЫЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Целью исследования является решение проблемы признания охраноспособности объектов, созданных искусственным интеллектом, в частности, уголовной ответственности за незаконные действия в отношении таких объектов. Анализируются отечественное и зарубежное законодательства по данному вопросу, судебная практика, а также предпринимается попытка исследования проблемы на основе различных теорий интеллектуальной собственности. Сделаны выводы о том, что произведениям, созданным искусственным интеллектом, должна предоставляться правовая охрана. Отмечены особенности уголовно-правовой характеристики соответствующих преступных деяний и определены последние как совершаемое с прямым умыслом в крупном размере незаконное использование объекта интеллектуальной собственности либо разглашение сущности объекта промышленной собственности, созданных с использованием информационных технологий и технологии искусственного интеллекта.

Ключевые слова: право, цифровые технологии, искусственный интеллект, уголовная ответственность, интеллектуальная собственность, плагиат, объекты авторского права

CRIMES INFRINGING ON INTELLECTUAL PROPERTY OBJECTS CREATED USING ARTIFICIAL INTELLIGENCE TECHNOLOGY

Abstract. The purpose of this study is to solve the problem of recognizing the protectability of objects created by artificial intelligence, in particular, criminal liability for illegal actions in relation to such objects. The author analyzes domestic and foreign legislation on this issue, judicial practice, and also makes an attempt to study the problem on the basis of various theories of intellectual property. The author comes to the conclusion that works created by artificial intelligence should be provided with legal protection.

The author also describes the features of the criminal legal characteristics of the relevant criminal acts and defines the latter as the illegal use of an object of intellectual property or disclosure of the essence of an object of industrial property created with the use of information technology and artificial intelligence technology, committed with direct intent on a large scale.

Keywords: law, digital technologies, artificial intelligence, criminal liability, intellectual property, plagiarism, copyright

Действующее законодательство предусматривает возможность создания объектов интеллектуальной собственности исключительно человеком (ст. 1228, 1257 ГК РФ).

Подобный подход является бесспорным для произведений, в процессе создания которых принимает участие только человек. Однако он требует как минимум дополнительной трактовки относительно произведений, в создании которых человек не принимает непосредственного участия. Все более частыми становятся практики создания результатов интеллектуальной деятельности, в которых искусственный интеллект не просто выступает инструментом в руках человека, но и вносит значительный вклад в результат.

Законодательный опыт зарубежных стран показывает, что на законодательном уровне вопрос пока решается образом так же, как он решен в настоящее время в российском гражданском праве. К произведениям применяются такие обязательные критерии, как личный характер (ФРГ) [11], оригинальность (Испания) [12], творческий (креативный) характер (Италия) [13]. В стратегической программе по интеллектуальной собственности Японии 2016 г. прямо указывается, что признание авторского права на произведения, созданные юнитами искусственного интеллекта, может быть нецелесообразным [14].

Проанализируем далее, как вопрос об авторстве произведений, созданных с участием искусственного интеллекта, решается в судебной практике.

Отечественная судебная практика в настоящее время исходит из традиционного подхода признания права на созданное произведение только в случае наличия творческого вклада физического лица, непосредственно создавшего его. Пленумом Верховного Суда Российской Федерации отмечается, что объектом авторского права могут признаваться только объекты, созданные творческим трудом, причем неважно, с участием техники или нет [15]. В то же время высшая судебная инстанция отмечает, что новизна не является непременным условием охраноспособности объекта [16].

Анализ зарубежной судебной практики показывает, что суды стоят на позиции непризнания за системами искусственного интеллекта возможности быть авторами произведений [17, 18, 19, 20, 21, 22].

По мнению Р. О. Оморова, в качестве автора изобретения, созданного программой, основанной на искусственном интеллекте, нужно признавать только человека или группу людей, создавших алгоритм. Последний может выступать лишь инструментом [3. С. 46]. В. Витко занимает противоположную позицию, утверждая, что создатель алгоритма в этом случае не проявляет творчества при создании произведения и потому автором быть не может [1. С. 9].

По А. Гурко, у произведений искусственного интеллекта нет авторов [2. С. 17–18].

Ю. Робертом предлагается подобные произведения признавать перешедшими в общественное достояние [10. С. 1265]. Звучат призывы признавать их правообладателями общество и государство [9. С. 2245]. В. С. Савина и другие авторы предлагают рассматривать произведения искусственного интеллекта как объекты смежных прав [4. С. 315–316]. В. Н. Синельников предлагает не признавать эти произведения объектами каких-либо прав, но вести их специальный учет с созданием специализированного реестра [5. С. 327].

По мнению Б. А. Шахназарова, изобретениям, созданным искусственным интеллектом, необходимо предоставлять патентную охрану, если они удовлетворяют критериям охраноспособности, объясняя это пользой для развития инноваций [6. С. 88]. Э. Бриди предлагает применять к ним концепцию служебных произведений [7. С. 27–28].

Целесообразно рассмотреть данную проблему с позиции теорий интеллектуальной собственности.

Наиболее взвешенным представляется утилитарный подход, который исследует правила интеллектуальной собственности в соответствии с их совокупной эффективностью и способностью способствовать всеобщему благосостоянию. Подход направлен на максимизацию общего общественного благосостояния общества с экономической точки зрения [8. С. 255].

Предоставление охраны объектам интеллектуальной собственности связано с двумя важнейшими факторами. С одной стороны, такие объекты имеют экономическую ценность, поэтому должны быть представлены в гражданском обороте, подлежать оценке и быть предметом сделок. С другой стороны, эти объекты имеют социальное значение и способны удовлетворять духовные потребности граждан.

Общество в целом получает выгоду от создания новых произведений и изобретений, поэтому правовая система должна поощрять их создание. Предоставление создателям монопольных прав на свои творения позволяет им больше зарабатывать на них и, таким образом, побуждает продолжать творческую деятельность.

В свете обозначенных теоретических подходов представляется наиболее рациональным не признавать авторство за объектами, созданными искусственным интеллектом. Что касается исключительных прав, они возникают у правообладателя систем искусственного интеллекта, производящих эти объекты. При такой конструкции понятным становится предмет преступления, а также потерпевший для целей судопроизводства.

Рассмотрим особенности уголовно-правовой характеристики преступлений против интеллектуальной собственности, созданной с использованием систем искусственного интеллекта.

В первую очередь нужно отметить, что в отношении таких произведений по понятным причинам невозможен плагиат.

Пункт 1 ст. 1229 ГК РФ закрепляет право автора или иного правообладателя использовать объект интеллектуальной собственности любым не запрещенным законом способом. Это право представляет собой исключительное право. В рамках

описанной нами концепции на объекты, созданные искусственным интеллектом, устанавливаются исключительные права. Только обладателем их становится не искусственный интеллект, а человек или юридическое лицо. В плане перечня правомочий, правовой природы, наполнения этих прав, возможных действий в отношении объекта эти исключительные права не отличаются от тех, что установлены в отношении традиционных, созданных творческой деятельностью человека, объектов.

В связи с этим незаконное использование – это первый вариант преступных деяний в отношении объектов, созданных искусственным интеллектом. Он представляет собой активные поведенческие акты, то есть действия, заключающиеся в использовании таких объектов любым способом без согласия правообладателя.

Разглашение сущности объекта промышленной собственности предполагает предание сведений об этих объектах огласке любым способом. Признание охраноспособности произведений, созданных искусственным интеллектом, не предполагает изменения системы патентования объектов промышленной собственности. Представляется, что для таких произведений не должно быть исключений. В связи с этим опасность разглашения сохраняется независимо от авторства изобретения, полезной модели или промышленного образца. Эта опасность напрямую зависит лишь от ценности указанных объектов, их потенциальной коммерциализации.

В связи с этим разглашение сущности объекта до его регистрации – второе из возможных преступных действий в отношении объектов, созданных искусственным интеллектом.

Общественная опасность подобных преступлений несколько отличается от опасности посягательства на объекты, созданные человеком. Права человека на результаты интеллектуальной деятельности отличаются двойственностью. В них присутствуют и личная («моральная»), и экономическая составляющие. Вследствие отсутствия характеристик личности у систем искусственного интеллекта первая из названных составляющих для них не актуальна. В связи с этим опасность преступных посягательств на соответствующие объекты в большей степени носит экономический характер.

Квалифицирующий признак «совершение деяния с использованием своего служебного положения» в случае с нарушением прав на объекты, созданные с использованием технологий искусственного интеллекта, получает дополнительное значение. Дело в том, что создание таких объектов предполагает серьезный технологический процесс, в котором задействованы значительные коллективы специалистов. Доступ к этим технологиям и к конечному продукту может облегчить совершение деяний, связанных с незаконным использованием объектов, созданных искусственным интеллектом. Последнее обстоятельство способно повысить общественную опасность таких деяний, что добавляет актуальности данному квалифицирующему признаку в описываемом составе.

В силу специфики предмета преступления в рассматриваемых составах возникает вопрос, должно ли охватываться умыслом виновного происхождение объекта интеллектуальной собственности. Иными словами, имеет ли значение для квалификации деяния то, был ли осведомлен виновный на момент совершения деяния о том, что объект, который он незаконно использует, создан с использованием технологий искусственного интеллекта.

Представляется, что для квалификации подобная осведомленность не должна иметь значения. По канонам науки о квалификации преступлений, виновный вовсе не обязательно должен быть осведомлен о всех деталях совершаемого преступления, а лишь о тех, которые имеют уголовно-правовое значение. Умыслом виновного должна охватываться не принадлежность объекта конкретному субъекту и не процесс его создания, а отсутствие у него самого прав на этот объект и наличие прав на этот объект у другого (не обязательно известного ему) субъекта.

С учетом описанных особенностей уголовно-правовой характеристики преступлений, посягающих на объекты интеллектуальной собственности, созданные с использованием информационных технологий и технологии искусственного интеллекта, последние можно определить как совершаемые с прямым умыслом в крупном размере незаконное использование объекта интеллектуальной собственности либо разглашение сущности объекта промышленной собственности, созданных с использованием информационных технологий и технологии искусственного интеллекта.

Список литературы

1. Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // ИС. Авторское право и смежные права. 2019. № 3. С. 2–22.

2. Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7–18.

3. Оморов Р. О. Интеллектуальная собственность и искусственный интеллект // E-Management. 2020. Т. 3, № 1. С. 43–49.

4. Савина В. С. Развитие права интеллектуальной собственности в современном информационном обществе // Пермский юридический альманах. 2019. С. 313–319.

5. Синельников В. Н. Правовой режим результатов интеллектуальной деятельности, созданных саморазвивающимися программами // Пермский юридический альманах. 2019. С. 321–328.

6. Шахназаров А. Ю. Применение технологий искусственного интеллекта при создании вакцин и иных объектов интеллектуальной собственности (правовые аспекты) // Актуальные проблемы российского права. 2020. Т. 15, № 7(116) июль. С. 76–90.

7. Bridy A. Coding Creativity: Copyright and the Artificially Intelligent Author // Stanford Technology Law Review. 2012. Vol.5. Pp. 1–28.

8. Margot E. Kaminski and Shlomit Yanisky-Ravid, The Marrakesh Treaty for Visually Impaired Persons: Why a Treaty Was Preferable to Soft Law, 75 U. PITT. L. REV. 2014. Pp. 255–301.

9. Yanisky-Ravid, Shlomit and Liu, Xiaoqiong (Jackie). When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law. 39 Cardozo Law Review. 2018. Pp. 2214–1262.

10. Yu R. The machine author: what level of copyright protection is appropriate for fully independent computer-generated works // University of Pennsylvania Law Review. 2017. Vol. 165. Pp. 1245–1270.

11. Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz). Сайт Федерального министерства юстиции ФРГ. URL: https://www.gesetze-im-internet.de/urhg/BJNR 012730965.htm

12. Real Decreto Legislativo № 1/1996, de 12 de abril de 1996, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia // Сайт Министерства президиума, по связям с судами и демократической памяти. URL: https://www.boe.es/buscar/act.php?id=BOEA-1996–8930

13. Legge del 22 aprile 1941 № 633 «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio // Историко-систематический указатель InterLex. URL: http://www.interlex.it/testi/l41_633.htm

14. Intellectual Property Strategic Program 2016. Сайт Офиса Премьер-министра Японии. URL: https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20160509_e.pdf

15. Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Сайт Верховного Суда Российской Федерации. URL: https://www.vsrf.ru/files/27771

16. Обзор судебной практики по делам, связанным с разрешением споров о защите интеллектуальных прав, утв. Президиумом Верховного Суда Российской Федерации 23.09.2015 // Сайт Верховного Суда Российской Федерации. URL: http://vsrf.ru/Show_pdf.php? Id=10333

17. Burrow-Giles Lithographic Co v Sarony. 111 U.S. 53, 4 S. Ct. 279 28 L. Ed. 349 (1884) // Сайт Информационного центра Верховного Суда США. URL: https://supreme.justia.com/cases/federal/us/111/53/case.html

18. Bridgeman art library, LTD. v. Corel corp., 36 F. Supp. 2d 191 (SDNY 999) / United States District Court for the Southern District of New York // Сайт Корнельского университета. URL: https://www.law.cornell.edu/copyright/cases/36_FSupp2d_191.htm

19. Naruto v. David John Slater et al / Decision of the United States District Court of Northern District of California of 2016 // Сайт Информационного центра Верховного Суда США. URL: https://law.justia.com/cases/federal/districtcourts/california/candce/3:2015cv04324/291324/45

20. Acohs Pty Ltd v Ucorp Pty Ltd» [Acohs Pty Ltd v Ucorp Pty Ltd [2012] FCAFC 16 / Judgment of the Federal Court of Australia, 02.02.2012 // Сайт Федерального Суда Австралии. URL: http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCAFC/2012/16.html

21. Telstra Corporation Limited v Phone Directories Company Pty Ltd [2010] FCAFC 149 / Judgment of the Federal Court of Australia, 15.12.2010 // Сайт Федерального Суда Австралии. URL: http://www.austlii.edu.au/cgibin/sinodisp/au/cases/cth/FCAFC/2010/149.html

22. Infopaq International A/S v. DanskeDagblades Forening / Judgment of the Court of Justice (Fourth Chamber) of 16 July 2009 // Сайт Европейского Суда Справедливости. URL: http://curia.europa.eu/juris/liste.jsf?num=C-5/08

Т. Г. Ухина,
аспирант,
Чувашский государственный университет
имени И. Н. Ульянова

УГОЛОВНО-ПРАВОВЫЕ ОСОБЕННОСТИ МОШЕННИЧЕСТВА В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Аннотация. В статье приводится сравнительный анализ уголовно-правовых норм о мошенничествах, совершенных с использованием цифровых технологий, на примере судебных актов, свидетельствующих о разных подходах правоприменителей к правовой оценке действий «кибермошенников», посягающих на имущественные права граждан в виде денежных средств (электронных средств платежа), хранящихся на счетах финансово-кредитных учреждений.

Ключевые слова: Интернет, мошенничество, электронные средства платежа, способ, цифровые технологии

CIVIL-LEGAL FEATURES OF FRAUD UNDER GLOBALIZATION OF DIGITAL TECHNOLOGIES: ISSUES OF THEORY AND PRACTICE

Abstract. The article provides a comparative analysis of criminal law norms on fraud committed using digital technologies on the example of judicial acts, indicating different approaches of law enforcement officers in giving a legal assessment of the actions of «cyber fraudsters» encroaching on the property rights of citizens in the form of money (electronic means of payment) stored in the light of financial and credit institutions. Proposals are made to improve the norms of the criminal law providing for liability for committing crimes using the information and digital space.

Keywords: Internet, fraud, electronic means of payment, method, digital technologies

В условиях глобального внедрения цифровых технологий во все сферы общественных отношений, наблюдается изменение криминогенной структуры преступности, совершенствуются способы конспирации преступной деятельности, совершаемые дистанционным способом. Предметами преступных посягательств все больше становятся имущественные права граждан, юридических лиц в виде денежных средств, хранящихся на счетах кредитных организаций, доступ к которым осуществляется с использованием инновационных цифровых технологий. Наиболее распространенным видом хищений дистанционным способом являются мошенничества, приобретающие за последние годы все более широкие масштабы.

К примеру, анализ состояния преступности в Российской Федерации за 2022 г., проведенный ФГКУ «ВНИИ МВД России» показывает, что в числе кибермошенничеств наибольшее число преступлений было «зарегистрировано по ст. 159 УК РФ (249 929; 47,87 %); по ст. 159.3 УК РФ (7 288; 1,40 %); 159.6 УК РФ (334; 0,06 %)» [1].

Как показывает статистика за 1 полугодие 2023 г., в числе мошенничеств, совершаемых с использованием цифровых инструментариев, преобладающее

большинство также приходится на преступления, предусмотренные ст. 159 УК РФ (163 666; 43,3 %). Вместе с тем наблюдается снижение на 31,7 % количества мошенничеств, совершенных с использованием электронных средств платежа, ответственность за которые предусмотрена ст. 159.3 УК РФ (2 870), а по фактам мошенничеств в сфере компьютерной информации (ст. 159.6 УК РФ) число зарегистрированных преступлений уменьшилось на 5,4 % (265) [2].

Несмотря на введение Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» дополнительных норм, предусматривающих ответственность за совершение мошенничеств с использованием цифровых технологий (ст. 159.1, 159.3, 159.6 УК РФ) [3], анализ судебно-следственной практики показывает, что существует проблематика в разграничении составов преступлений, предусмотренных статьями 159 и 159.3 УК РФ, которая выражается в том, что суды по одному и тому же общественно опасному деянию и способу совершения, предметом которых являются имущественные права граждан в виде денежных средств, хранящихся на счетах банковских учреждений с применением электронно-цифровых технологий, квалифицируются по-разному, в одном случае по ст. 159.3 УК РФ, в другом по ст. 159 УК РФ.

Например, из приговора Ленинского районного суда г. Чебоксары Чувашской Республики по уголовному делу № 21RS 0022–01–2022–001753–35 следует, что гражданин С. А. А., заведомо зная об отсутствии у него нет автомобильных колес, разместил на сайте Avito объявление об их продаже, на которое откликнулась потерпевшая. С. А. А., осуществляя переписку с потерпевшей и, преследуя цель незаконного получения денежных средств дистанционным способом путем их перевода с банковского счета потерпевшей на банковский счет, указанный С. А. А., убедил ее перейти по сгенерированному в мобильном приложении Telegram ложной ссылке с сайта Avito об оплате товара. После чего, потерпевшая, будучи введенной в заблуждение, перешла по указанной С. А. А. ссылке, ввела реквизиты принадлежащей ей банковской карты и перевела денежные средства в размере 21 тыс. рублей на расчетный счет злоумышленника. Действия С. А. А. квалифицированы судом по ч. 2 ст. 159.3 УК РФ [4].

Между тем аналогичные действия «кибермошенника» А.Т.Ю. приговором того же районного суда квалифицированы по ч. 2 ст. 159 УК РФ. [5].

Вместе с тем норма статьи 159 УК РФ и ее квалифицирующие признаки не достаточно содержат в качестве способа, характеризующего объективную сторону преступления, такого понятия, как «с использованием информационно-телекоммуникационной сети Интернет, средств мобильной сотовой связи, иных цифровых технологий». Отнесение мошенничества к преступлению, совершаемому с использованием цифровых технологий (киберпреступления), определяется лишь «Перечнем № 25 Указания Генеральной прокуратуры России № 401/11/2, МВД России № 1 от 19.06.2023 [6].

Вопросы дифференциации уголовной ответственности за хищения денежных средств с использованием цифровых технологий рассматривались в трудах современных ученых Е. А. Марковой [7. С. 13–15] А. С. Перетолчина [8. С. 13–14] и др.

Резюмируя изложенное с учетом обозначенной проблематики, в целях исключения неоднозначного толкования (применения) «цифровых мошенничеств», формирования единой правоприменительной практики, было бы целесообразным:

– закрепление в статье 159 УК РФ «Мошенничество» отдельного квалифицирующего признака, повышающего ответственность за совершение мошеннических действий с использованием цифровых технологий, и отнесение данного способа к категории не ниже средней тяжести, что послужит мерой превентивного характера и сдерживания к их широкому распространению, в условиях стремительного развития современных технологий;

– обязать органы расследования, субъектов, осуществляющих оперативно-розыскные мероприятия при выявлении, пресечении, раскрытии преступлений и расследовании уголовных дел, установление фактов использования при совершении всех видов преступлений применение цифровых технологий, определив их в качестве отягчающих обстоятельств путем внесения соответствующих дополнений в ст. 63 УК РФ, о чем автором освещалось ранее на Международной практической конференции в июле т. г. в г. Новосибирск [9. С. 268].

Список литературы

1. Аналитически обзор ФГКУ «ВНИИ МВД России» «О состоянии преступности в Российской Федерации и тенденциях ее развития с отражением количественных и качественных показателей, характеризующих криминальную ситуацию в Российской Федерации в сфере борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий. URL: https://ВНИИ.МВД.РФ

2. Статистические сведения ФКУ «ГИАЦ МВД России» // Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида (сформирован в соответствии с приказом Генерального прокурора Российской Федерации от 03.07.2023 № 429) за январь-июнь 2023 г. № 280, Раздел 1.

3. Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2012. № 49. Ст. 6752.

4. Приговор Ленинского районного суда г. Чебоксары. URL: https://Leninsky–chv.sudrf.ru

5. Указания Генеральной прокуратуры России № 401/11/2, МВД России № 1 от 19.06.2023 «О введение в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».

6. Маркова Е. А. Уголовно-правовая характеристика хищения, совершенного с использованием электронных средств платежа: автореф. дис. … канд. юрид. наук: 5.1.4. Маркова Елена Алексеевна. Санкт-Петербург, 2021. С. 13–15.

7. Перетолчин А. П. Уголовная ответственность за совершение мошенничества с использованием электронных средств платежа: автореф. дис. … канд. юрид. наук: 12.00.08. Перетолчин Артем Павлович. Иркутск, 2021. С. 13–14.

8. Ухина Т. Г. Электронное мошенничество как угроза национальной безопасности и пути совершенствования пресечения противоправных действий в сфере использования информационных технологий // Международно-практическая конференция «Внедрение передового опыта и практическое применение результатов инновационных исследований», г. Новосибирск, 30 июля 2023 г. Стерлитамак, 2023. Т. 2. С. 268.

Р. Р. Хайбрахманова,
преподаватель-методист факультета заочного обучения,
Казанский юридический институт
Министерства внутренних дел
Российской Федерации

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ МАТЕРИАЛОВ, СОДЕРЖАЩИХ СЦЕНЫ ЖЕСТОКОГО ОБРАЩЕНИЯ С ЖИВОТНЫМИ

Аннотация. Статья посвящена исследованию основ уголовно-правового противодействия распространению материалов, содержащих сцены жестокого обращения с животными. Исследованы современные тенденции развития преступлений, сопряженных с жестоким обращением с животными и публикацией содеянного в открытом доступе, а также способы сокрытия цифровых следов преступлений, что позволило предложить меры для решения выявленных проблем, в частности, посредством криминализации изготовления, распространения и оборота таких материалов.

Ключевые слова: жестокое обращение с животными, фотоматериалы, видеоматериалы, Интернет, публикация, информация, цифровые следы

COUNTERING THE DISSEMINATION OF MATERIAL CONTAINING SCENES OF ANIMAL ABUSE

Abstract. The article is devoted to the study of the foundations of criminal law counteraction to the distribution of materials containing scenes of cruelty to animals. The author studied the current trends in the development of crimes involving cruelty to animals and the publication of deeds in the public domain, as well as ways to hide the digital traces of crimes, which made it possible to propose measures to solve the identified problems, in particular, through the criminalization of the production, distribution and circulation of such materials.

Keywords: animal cruelty, photographic materials, video materials, Internet, publication, information, digital footprints

Исследование современных тенденций развития преступности в России и в мире, а также работ по данной проблематике, опубликованных российскими

и зарубежными авторами, позволяет отметить, что преступники все активнее используют передовые научно-технические разработки, информационные и телекоммуникационные технологии [2. С. 55]. При этом указанные технологии могут использоваться не только для непосредственно совершения преступлений, но и в ряде случаев для публичной демонстрации содеянного.

Многообразие современных средств коммуникации, а также интенсивно развивающаяся сфера сетевого обмена информацией, в частности блогов, форумов, мессенджеров, социальных сетей, привели к увеличению интенсивности процессов распространения криминальных практик и стали причиной активизации научных исследований в сфере уголовно-правового противодействия преступности в сфере информационных технологий [3. С. 9].

Особую озабоченность в этой связи, как среди теоретиков, так и среди правоприменителей, вызывает использование преступниками информационно-телекоммуникационной сети Интернет для публичной демонстрации результатов преступной деятельности. Активное использование преступниками социальных сетей, например, «ВКонтакте», «Одноклассники», Telegram, YouTube, TikTok негативно сказывается на состоянии общественной нравственности, может привести к ужесточению нравов, особенно среди самой активной части пользователей такими интернет-ресурсами, а именно молодежи. Данная категория населения является наиболее восприимчивой и подверженной влиянию, так как у молодежи, как правило, отсутствуют четко сформированные жизненные позиции и взгляды [4. С. 179].

Характерным примером такого деяния выступает жестокое обращение с животными, сопряженное с его публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (п. г ч. 2 ст. 245 УК РФ). Примечательно, что в Российской Федерации ежегодно увеличивается количество зарегистрированных фактов данного преступления: в 2010 г. было зарегистрировано 307 преступлений, предусмотренных ст. 245 УК РФ, в 2011 г. – 258, в 2012 г. – 247, в 2013 г. – 235, в 2014–228, в 2015–263, в 2016 г. – 263, в 2017 г. – 288, в 2018 г. – 446, в 2019–490, в 2020–576, в 2021–673, в 2022–709 [10]. Данное деяние, как правило, сопряжено с общественным резонансом, а также, безусловно, крайне негативно отражается на общественной морали и нравственности.

Например, в ноябре 2016 г. более чем в 93 городах России проводились митинги и пикеты против жестокого обращения с животными. Причиной тому послужили деяния двух девушек из города Хабаровск, а именно то, как они с особой жестокостью умерщвляли животных, взятых ими из приюта, снимая свои действия на фото и видео, в последующем распространяя их в социальных сетях [7]. Деяния женщин вызвали широкий общественный резонанс среди населения, спровоцировали массовые митинги и привели к общественной дискуссии о необходимости дополнительной криминализации жестокого обращения с животными.

Законодатель действительно существенно расширил перечень квалифицирующих признаков, а также дополнил санкции ст. 245 УК РФ [15], однако принимаемые меры не привели к снижению преступности данного вида.

Советский и российский психиатр, заслуженный врач Российской Федерации З. И. Кекелидзе, комментируя аналогичные факты жестокого обращения

с животными, отметил, что подобные проявления человеческой жестокости говорят о психических отклонениях личности. Человек, совершающий подобные деяния, возможно, страдает от опасных заболеваний психики, а потому может нуждаться в принудительном лечении. Кроме того, данное деяние есть проявление морального помешательства, это, в свою очередь, означает, что у человека отсутствует понятие морали [5].

Необходимо добавить, что жестокое обращение с животными, связанное с публичной демонстрацией содеянного посредством изготовления и распространения материалов, содержащих такие сцены, также совершается с корыстными мотивами и нередко имеет трансграничный характер.

Так, например, в 2020 г. было раскрыто преступное сообщество, действовавшее от Индонезии до Соединенных Штатов Америки, которое использовало социальные сети и веб-сервисы, позволяющие загружать и просматривать видео (видеохостинги) для распространения материалов, содержащих сцены жестокого обращения с животными. Подобные материалы распространялись за установленную стоимость в криптовалюте, также проводились специальные видеотрансляции, в которых зрители путем голосования выбирали способ истязания животного [1].

Удаление указанных материалов, размещенных на видеохостингах в публичном доступе, не разрешило проблему окончательно, поскольку фото- и видеоматериалы жестокого обращения с животными распространялось преимущественно в закрытых группах других социальных сетей, где остаются до настоящего времени.

Примечательно, что удалось установить лишь двух лиц, жителей Индонезии, виновных в указанных деяниях.

Исследование, проведенное экспертами ряда зоозащитных организаций, позволяет отметить, что преступниками используются сайты, не индексируемые обычными поисковыми системами, для размещения фото- и видеоматериалов, содержащих сцены жестокого обращения с животными, их распространения и продажи. Так, например, стоимость видеоматериалов с причинением вреда, пытками и истязаниями животного могут стоить от 10 до 300 долларов США, в зависимости от животного и иных обстоятельств [9]. Нередко для создания такого рода контента привлекаются девушки. Например, в 2020 г. была установлена жительница города Запорожье, которая снимала на видео процесс пытки животных с целью их последующей продажи. При проведении следственных действий по адресу ее места жительства было обнаружено множество материалов, содержащих сцены жестокого обращения с животными, а также банковские карты, на которые осуществлялись переводы денежных средств от лиц, желающих приобрести данные материалы [6].

В 2020 г. активисты зоозащитных организаций обнаружили в городе Санкт-Петербург несколько специальных студий, в которых осуществлялись съемки фото- и видеоматериалов с пытками и истязаниями животных, которые в последующем распространялись в публичном доступе, в том числе за установленную стоимость. Для съемок подобного контента активно привлекались девушки, которым предлагалось раздавить мелких животных своими ногами, например, кролика или щенка [13].

По-прежнему активно распространяются и показательные бои животных, в том числе на сайтах, размещенных в открытом доступе в сети Интернет.

Создание и распространение информации, содержащей сцены жестокого обращения с животными, безусловно, негативно сказываются на состоянии общественной нравственности, что требует принятия мер реагирования как уголовно-правового характера, так и иных отраслей права.

Раскрытие и расследование рассматриваемого преступления, в особенности совершенных с публичной демонстрацией содеянного, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях, нередко вызывает сложности у правоохранительных органов.

Исходя из исследования следственно-судебной практики по уголовным делам о жестоком обращении с животными за период 2016–2022 гг., более 50 % таких дел приостанавливается, как правило, в связи с тем, что лицо, подлежащее привлечению в качестве обвиняемого, не установлено, или подозреваемый или обвиняемый скрылся от следствия, либо место его нахождения не установлено по иным причинам. Причиной тому во многом является анонимность преступников и использование ими современных технических решений в целях сокрытия персональной информации.

В целом, жестокое обращение с животными, совершаемое с применением информационных технологий, предполагает необходимость осуществления комплекса следственных действий и оперативно-розыскных мероприятий, направленных на сбор необходимой информации, в частности, из дата-центров, облачных хранилищ, от провайдеров связи и из индивидуальных мобильных устройств.

Тем не менее использование преступниками передовых технологий в производстве и распространении материалов, содержащих изображения жестокого обращения с животными, требует наличия специализированного оборудования, нередко студий, лишенных примечательных особенностей, профессиональную фото- или видеосъемку, последующий монтаж, и так далее, а их распространение осуществляется с использованием защищенных телекоммуникационных технологий, например, посредством разработки сайтов в сети Интернет с использованием приемов сокрытия цифровых следов преступления, создания каналов анонимного взаимодействия в скрытых сегментах сети Интернет, и использования неперсонифицированных платежных средств. Преступниками также могут реализовываться и другие способы сокрытия цифровых следов с использованием современных телекоммуникационных технологий [14. С. 54].

С учетом широкого распространения средств цифрового обмена данными, включая высокоскоростную зашифрованную передачу фото- и видеофайлов, доступности этих технологий для преступников и возможностей доступа потребителей к результатам преступной деятельности, исследуемые действия приобретают все более широкое распространение.

В Российской Федерации органом, осуществляющим контрольно-надзорные функции в сфере оборота цифровой информации в сети Интернет, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). Ключевым направлением деятельности данного органа государственной власти является применение мер, направленных на ограничение доступа к информационным ресурсам в информационно-телекоммуникационных сетях, включая информационно-телекоммуникационную сеть

Интернет, в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» [12].

Согласно положениям Федерального закона от 27.12.2018 № 498-ФЗ, создание и распространение материалов, которые пропагандируют жестокое обращение с животными, запрещено [16]. Например, в Российской Федерации активно блокируются сайты движения «догхантеров» (охотников на собак), на которых размещались инструкции об убийствах безнадзорных домашних животных, в том числе с помощью пневматического и огнестрельного оружия, лекарственных препаратов с высокой степенью токсичности, фото- и видеоотчеты об убийствах и издевательствах над животными.

Однако следует констатировать, что реализация отмеченных функций зачастую не демонстрирует необходимой эффективности в противодействии распространению запрещенного законодательством Российской Федерации цифрового контента. Подобная информация по-прежнему активно распространяется в социальных сетях, предполагающих неограниченный доступ к ней.

Вышеуказанные факторы в совокупности с доступностью, потенциально неограниченной аудиторией, распространением средств обеспечения анонимности, высокой скоростью передачи данных и мультимедийными возможностями, предоставляемыми сетью «Интернет», способствуют использованию преступниками данной среды для распространения противоправной информации и привлечения финансирования для последующего совершения противоправных действий [11. С. 64].

В этой связи наиболее эффективным способом противодействия указанному деянию становится своевременное блокирование и удаление подобного контента внутренними автоматическими алгоритмами социальных сетей, а также жалобы других пользователей на размещение в публичном доступе подобных материалов, поскольку публикация видеоматериалов, содержащих сцены насилия, в том числе по отношению к животным, противоречит политике видеохостингов.

Автоматические алгоритмы видеохостингов сканируют видео, анализируют наличие специальных «маркеров» в ролике, указывающих на нарушение правил сервиса, ориентируется на другие косвенные сигналы, что позволяет определить наличие в видеофайле, например, порнографических материалов, сцен насилия и так далее в целях блокировки. Кроме непосредственного удаления, к аккаунту пользователя, нарушившего правила публичного видеохостинга, могут быть применены и другие меры, например:

– запрет на создание новых аккаунтов;

– ограничение на использование имеющихся аккаунтов.

Действительно, спорные видеофайлы могут быть заблокированы видеохостингом, однако новая публикация загруженных материалов сразу попадает в публичный доступ без предварительной проверки и обработки, что позволяет неограниченному кругу людей увидеть их.

Следует также отметить, что в современном российском законодательстве отсутствуют положения, устанавливающие обязанность передавать информацию о выявленных фактах противоправной деятельности, например, жестокого обращения с животными, сопряженного с публичной демонстрацией содеянного,

правоохранительным органам, что препятствует эффективному взаимодействию и оперативному обмену информацией.

Раскрытие и расследование данного деяния, как и других преступлений, совершаемых с использованием информационных технологий, является для органов внутренних дел трудной задачей ввиду совокупности объективных проблем, прежде всего, в информационно-аналитической деятельности. Исходя из вышеизложенного, имеется практическая необходимость установить обязанность информационным ресурсам, в частности, социальным сетям, сообщать информацию о выявленных признаках противоправных деяний в органы внутренних дел.

Необходимо также отметить, что в настоящее время отсутствует юридическая ответственность за создание и распространение фото- и видеоматериалов, содержащих сцены жестокого обращения с животными.

Исходя из изложенного, дополнительно актуализируется необходимость оптимизации уголовно-правового противодействия данному явлению ввиду активного использования виновными лицами информационно-телекоммуникационной сети «Интернет», а также распространения данного деяния среди несовершеннолетних. Так, например, в теории уголовного права и криминологии также неоднократно высказывались предложения установить меры ответственности за распространение материалов, содержащих сцены жестокого обращения с животными [8]. Мы, безусловно, поддерживаем данное решение, однако в данном случае необходимо разрешить вопрос с определением вида ответственности за создание и распространение таких материалов, а именно административной или уголовной.

Мы считаем, что, исходя из общественной опасности такого деяния, его совершения в корыстных целях, существует объективная необходимость криминализации данного деяния. В этой связи предлагаем дополнить главу 25 УК РФ проектной статьей 245.1, с диспозицией следующего содержания:

«Статья 245.1. Оборот материалов, пропагандирующих жестокое обращение с животными

Изготовление, распространение и (или) перемещение через Государственную границу Российской Федерации в целях распространения или публичной демонстрации материалов с изображением жестокого обращения с животным, –

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные:

а) группой лиц по предварительному сговору или организованной группой;

б) с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) с извлечением дохода в крупном размере».

Таким образом, проведенное исследование позволило нам сделать следующие выводы:

1. Сохраняется тенденция развития преступности, сопряженной с использованием информационных технологий, однако современные достижения науки и техники могут применяться не только с целью совершения противоправного деяния, но и для публичной демонстрации содеянного, что причиняет вред общественной нравственности. Характерным примером такого деяния выступает жестокое обращение с животными, сопряженное с публичной демонстрацией

содеянного, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях, включая сеть «Интернет» (п. «г» ч. 2 ст. 245 УК РФ);

2. Активное использование преступниками средств обеспечения анонимности, защищенных информационных каналов, а также сайтов, размещенных в «глубоком Интернете», позволяет им распространять фото- и видеоматериалы, содержащие сцены жестокого обращения с животными, в корыстных целях, тогда как у правоохранительных органов возникают объективные сложности в рамках деятельности по раскрытию, расследованию и предупреждению данных фактов;

Наиболее эффективным решением является своевременная блокировка информации, пропагандирующей жестокое обращение с животными, или содержащей такие сцены, однако видеохостинги не обязаны передавать информацию о признаках противоправной деятельности в правоохранительные органы, что препятствует оперативному и своевременному обмену информацией. Считаем, что существует объективная необходимость установления такой обязанности, что позволит органам внутренних дел провести своевременную проверку информации;

До настоящего времени не установлена юридическая ответственность за изготовление и оборот материалов, содержащих сцены жестокого обращения с животными, тогда как установление подобного запрета с санкциями за его нарушение – это объективная реакция на такое деяние, обусловленная его общественной опасностью. В этой связи предлагаем дополнить уголовное законодательство Российской Федерации проектной статьей 245.1 УК РФ «Оборот материалов, пропагандирующих жестокое обращение с животными».

Список литературы

1. Global network of sadistic monkey torture exposed by BBC. URL: https://www.bbc.com/news/world-65951188

2. Арипшев А. М. Развитие киберпреступности в цифровом обществе // Журнал прикладных исследований. 2023. № 5. С. 53–57.

3. Воронин Ю. А., Беляева И. М., Кухтина Т. В. Современные тенденции преступности в цифровой среде // Вестник ЮУрГУ. Серия: Право. 2021. № 1. С. 7–12.

4. Дороженко Е. К., Биккинин И. А. Преступления против несовершеннолетних в цифровой среде: обзор проблемы и пути противодействия // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. 2022. № 1–3 (62). С. 178–180.

5. Жестокое обращение с животными. URL: https://clck.ru/36rynk

6. Живодерка в Запорожье давила котят перед камерой. URL: https://www.kp.ru/daily/217184.5/4289712

7. Живодерки из Хабаровска // Комсомольская правда. Хабаровск. [Подборка статей за 2016–2021 гг.]. URL: https://www.hab. kp.ru/daily/theme/13966/

8. Законопроект № 395531–6 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях и Федеральный закон «Об информации, информационных технологиях и о защите информации». URL: http://asozd2.duma.gov.ru/main.nsf/ (дата обращения: 18.08.2023)

9. Коммерция на фетише. URL: https://fingernal. ru/manicure/zoozashchitniki-sochli-prigovor-habarovskim-zhivoderkam-slishkom-myagkim-sud-nakazal

10. На основании формы государственного статистического наблюдения. См.: Единый отчет о преступности (Форма 1-Г) за 2010–2022 гг. // ГИАЦ МВД России.

11. Осипенко А. Л., Луговик В. Ф. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений // Общество и право. 2021. № 2(76). С. 60–68.

12. Постановление правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Российская газета. 2009. № 49.

13. Кадры зверств над животными удалят из Сети // Intellect. 2020. 11 февр. URL: https://www.intellectpro.ru/press/commenters/kadry_zverstv_nad_zhivotnymi_udalyat_iz_seti

14. Соловьев В. С. Криминологическая типология механизмов совершения преступлений с использованием информационно-телекоммуникационных технологий // Вестник КРУ МВД России. 2021. № 4(54). С. 50–57.

15. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

16. Федеральный закон от 27 декабря 2018 г. № 498-ФЗ «Об ответственном обращении с животными и о внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета. 2018. № 295.

К. А. Ханджян,
аспирант,
Кубанский государственный университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН И СМАРТ-КОНТРАКТОВ НА ПУТИ ЛЕГАЛИЗАЦИИ ОНЛАЙН-КАЗИНО В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье исследуется онлайн игорная индустрия, а также опыт зарубежных стран с возможностью его ретрансляции на организацию и проведение азартных игр в сети Интернет в Российской Федерации. Для интеграции системы блокчейн в онлайн-казино необходимо выбрать подходящую блокчейн-платформу. Существует несколько различных платформ блокчейна, таких как Ethereum, EOS или TRON. Разработка смарт-контрактов – это программные коды, работающие на блокчейне, которые выполняют заданные действия при выполнении определенных условий. Для создания онлайн-казино на блокчейне потребуется разработать смарт-контракты для игровых операций, таких как ставки, выплаты выигрышей и управление игровым балансом. Кроме того, одним из главных преимуществ блокчейна для онлайн-казино является повышенная прозрачность и безопасность операций.

Ключевые слова: онлайн-казино, блокчейн, смарт-контракт, криптовалюта, цифровые технологии, онлайн-гемблинг

THE USING OF BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS ON THE WAY TO LEGALIZE ONLINE CASINO IN THE RUSSIAN FEDERATION

Abstract. This article examines the online gambling industry, as well as the experience of foreign countries with the possibility of its retransmission to the organization and conduct of gambling on the Internet in the Russian Federation. To integrate the blockchain system into an online casino, the following steps may be necessary: choosing a suitable blockchain platform: There are several different blockchain platforms, such as Ethereum, EOS or TRON. The development of smart contracts is software codes running on the blockchain that perform specified actions when certain conditions are met. To create an online casino on the blockchain, it will be necessary to develop smart contracts for gaming operations, such as betting, payout of winnings and game balance management. In addition, one of the main advantages of blockchain for online casinos is increased transparency and security of operations.

Keywords: online casino, blockchain, smart contract, cryptocurrency, digital technologies, online gambling

Введение. За последние пять лет индустрия онлайн-гемблинга росла значительными темпами благодаря развитию технологий, включая быстрое распространение смартфонов и беспроводных интернет-устройств. Это позволяет индустрии онлайн-гемблинга быть очень доступной, предоставляя игрокам необходимую конфиденциальность и удобство. Игорный бизнес в сети Интернет является быстрорастущей индустрией, которая привлекает миллионы игроков и обрабатывает огромные суммы денег. В силу развития современных цифровых технологий незаконная организация азартных игр в более чем 80 % случаях проводится с использованием сети Интернет, поскольку виртуальные казино позволяют участникам азартной игры, не выходя из дома делать ставки, вносить свои денежные средства для испытания своей удачи, что говорит об их большой криминальной опасности для финансовых институтов государства, а также психологической и нравственной безопасности населения [2. С. 4].

Основная часть. Очевидно, что организация азартных онлайн-игр причиняет ущерб не только государству в виде экономических потерь, таких как неуплата налогов, сокрытие незаконного дохода от государства, легализация денежных средств, полученных преступным путем, но и простым гражданам, которые испытывают постоянные стрессы, финансовые потери, психические расстройства, перерастающие в патологическую зависимость от игры.

Человек, который психически не устойчив, постоянно заключает пари, ставит все больше денежных средств, тем самым вынуждая себя оформлять кредиты, продавать имущество, что влечет в конечном итоге к банкротству и кабальному образу жизни. Говард Шаффер и Рейчел Кидман полагают, что психологическая

зависимость имеет трибинарную природу, а именно биологическую, включающую наследственную составляющую, социальную (поведенческую), т. е. азартные игры являются для человека его привычной общественной деятельностью, и психологический аспект, когда игрок уже не может остановить свой «животный» азарт и контролировать свои действия. В конечном итоге, данные ученые считают, что зависимость от азартных игр перетекает в патологию, нейроадапцию [6. P. 1–6].

Первое в мире онлайн-казино было открыто на Антигуа и Барбуда, небольшом островном государстве в Карибском море, в 1994 г. Компания под названием «Microgaming» разработала программное обеспечение для этого онлайн-казино, и с тех пор началось развитие онлайн-гемблинга. В данной стране был принят Закон о свободной торговле и обработке в 1994 г., что сделало его одним из первых государств, которое начало регулировать онлайн-гемблинг. Операторы онлайн-гемблинга, лицензированные юрисдикцией, должны размещать свои серверы на территории государства, и онлайн-игроманы, желающие играть на этих лицензированных игорных веб-сайтах, также должны физически находиться в пределах государственных границ.

Кроме того, в 2006 г. США приняли Закон о борьбе с незаконными азартными играми в Интернете с целью лишения компаний, занимающихся азартными онлайн-играми, возможности законно использовать финансовые транзакции и платежные системы, что, в свою очередь, ограничивает прибыль данной игорной индустрии. В этих условиях появились сайты онлайн-игр с биткойнами для расширения незаконной онлайн-деятельности.

В отличие от оффлайн-казино, которые требуют огромных вложений перед запуском, онлайн-гемблинг требует относительно простых вещей для создания сайта: доменного имени, сервера и программного обеспечения. Во-первых, веб-сайт должен зарегистрировать определенное доменное имя у регистратора доменов, который является уполномоченной компанией, регистрирующей доменные имена от имени владельца регистрации. Доменное имя, уникальный адрес для идентификации конкретной веб-страницы в Интернете, представляет собой один или несколько адресов Интернет-протокола (IP), которые представляют собой набор правил для обмена форматом данных через Интернет или ряд других сетей. После регистрации доменного имени владелец регистрации становится владельцем веб-сайта и имеет полномочия. Кроме того, контактная информация, относящаяся к зарегистрированным доменным именам, такая как имя, адрес, адрес электронной почты и номер телефона, должна храниться и публично отображаться в базе данных WHOIS, регулируемой Интернет-корпорацией по присвоению имен и номеров [5. P. 10–35]. Многие регистраторы доменов предоставляют услуги анонимной регистрации доменов, которые скрывают конфиденциальную информацию владельца от спама, маркетинговых фирм и сетевых мошенников.

Во-вторых, сайту онлайн-гемблинга нужны серверы, представляющие собой компьютеры, на которых хранятся все формы данных и файлы, необходимые для работы сайта. Чем больше места на сервере, тем больше игр может разместить сайт онлайн-гемблинга. Сервер предоставляется веб-хостинговой компанией, которая

предоставляет услугу, позволяющую клиентам размещать веб-сайт в Интернете. Имея свой собственный IP-адрес, хост-компьютер назначает IP-адрес для данных и файлов доменному имени через систему доменных имен, посредством чего веб-страницы могут быть доставлены через браузер на компьютер пользователей Интернета, которые вводят его доменное имя в свои браузер.

Наконец, для работы сайта требуется программное обеспечение для онлайн-гемблинга. Игорный сайт может либо получить программное обеспечение от разработчика программного обеспечения для азартных игр, либо разработать код самостоятельно. Программное обеспечение отвечает за игры, интерфейс, макет и графический дизайн и управляет сайтом, взаимодействуя с онлайн-игроками. Чтобы сделать ставку, как правило, игрок создает учетную запись и вносит деньги требуемым способом, таким как кредитная карта, банковский перевод или поставщик услуг онлайн-платежей. Для вывода выигрыша пользователю азартных игр необходимо обратиться к оператору и выбрать способ оплаты.

Существует также проблема, когда организаторы онлайн-казино используют криптовалюту при транзакционных операциях, в данной связи предлагаем следующий механизм ее решения. Перечисления через криптовалюту можно отследить с помощью блокчейн-эксплорера. Блокчейн-эксплорер – это инструмент, позволяющий просматривать информацию о транзакциях, произведенных в блокчейне. Для того чтобы отследить перевод криптовалюты через блокчейн-эксплорер, нужно знать номер кошелька отправителя и получателя, а также количество переводимых средств и дату проведения операции. С помощью этой информации можно найти транзакцию в блокчейне, и увидеть все детали операции, включая ее статус, время выполнения, комиссию и другие подробности. Некоторые из наиболее популярных блокчейн-эксплореров включают Blockchair, Etherscan (для эфира), BSCscan (для Binance Smart Chain) и т. д. Система блокчейн может быть полезна при расследовании онлайн-казино, так как она позволяет создавать децентрализованные и прозрачные системы, которые обеспечивают безопасность данных и транзакций.

Для начала можно использовать блокчейн для создания цифровой записи всех транзакций, связанных с онлайн-казино. Это позволит контролировать все финансовые потоки между игроками и казино. Все транзакции будут храниться в блокчейне, что позволит вести учет всего движения денежных средств и отслеживать любые необычные транзакции, которые могут указывать на мошенничество [4. С. 155–158].

Также можно использовать технологию смарт-контрактов на базе блокчейна, чтобы автоматизировать процессы выплат выигрышей и других финансовых операций. Смарт-контракты являются программными кодами и выполняются автоматически при выполнении определенного условия, например, получении выигрыша в игре. Это позволит избежать ошибок, связанных с ручным контролем выплат, и уменьшит вероятность мошенничества [1. С. 184–189].

Кроме того, блокчейн позволяет создавать прозрачные системы управления данными и защищать личную информацию пользователей [3]. В блокчейне каждый участник сети имеет доступ только к той информации, которая относится к его операциям, что повышает безопасность данных и уменьшает возможности для злоумышленников.

Таким образом, использование технологии блокчейн может значительно повысить прозрачность и безопасность в онлайн-казино, что, в свою очередь, поможет предотвратить мошенничество и улучшить опыт игроков, а также в случае необходимости расследовать преступления, связанные с этими технологиями, например, отмывание денежных средств, установление сбытчиков наркотических средств и другие виды экономических преступлений.

Заключение. Анонимный характер криптовалют позволяет индустрии онлайн-гемблинга справляться с регулированием, налагаемым властями, и расследованием правоохранительных органов. Мало того, что сама операция является незаконной, она также может привести к другим незаконным действиям в Интернете, таким как мошенничество, отмывание денег, азартные игры для подростков или проблемы с азартными играми. Чтобы лучше понять природу анонимных азартных игр, в этом исследовании изучалось, как работают сайты онлайн-гемблинга; какие факторы привлекают онлайн-пользователей к участию в нелегальной игорной деятельности; как незаконная деятельность, связанная с азартными играми в Интернете, может привести к другой преступной деятельности в Интернете; и как операторы онлайн-гемблинга сохраняют свою работу, находясь вдали от расследования правоохранительных органов.

Список литературы

1. Зиновьева Н. С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве // Вестник Восточно-Сибирского института МВД России. 2018. № 3 (86).

2. Лимарь А. С. Предупреждение преступлений, связанных с незаконными организацией и проведением азартных игр: автореф. дис. … канд. юрид. наук. М., 2021.

3. Мурадян С. В. Цифровые активы: правовое регулирование и оценка рисков / С. В. Мурадян // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 123–151. EDN RIZOKS.

4. Нагайцев К. Д. Использование технологии блокчейн и цифровых токенов при совершении преступлений, связанных с уклонением от уплаты налогов и сборов // Правовое государство: теория и практика. 2022. Т. 14, № 3(53). 155–158.

5. Choi Sinyong. Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory. In BSU Master's Theses and Projects. 2018. Item 64. URL: https://vc.bridgew.edu/theses/64

6. Shaffer H. J., Kidman R. Shifting Perspectives on Gambling and Addiction. Journal of Gambling Studies. 2003. Vol. 19, iss. 1. P. 1–6.

Б. Э. Шавалеев,
инспектор отдела кадров,
Казанский юридический институт
Министерства внутренних дел Российской Федерации

НЕГОСУДАРСТВЕННЫЕ СУБЪЕКТЫ ПРЕДУПРЕЖДЕНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Аннотация. Статья посвящена исследованию роли негосударственных субъектов системы предупреждения хищений электронных денежных средств на современном этапе. Исходя из состояния национальной платежной системы обосновывается необходимость активного участия негосударственных субъектов в предупреждении хищений электронных денежных средств, в связи с чем отмечена необходимость расширения перечня признаков операций, совершаемых без согласия клиента кредитной организации, а также применения биометрической аутентификации безналичных платежей.

Ключевые слова: электронные денежные средства, электронные средства платежа, биометрическая аутентификация, мошенничество, кража, предупреждение, субъекты, система предупреждения, преступность

NON-STATE ENTITIES PREVENTION OF THEFT OF ELECTRONIC MONEY

Abstract. The article is devoted to the study of the role of non-state actors in the system for preventing theft of electronic money at the present stage. Based on the state of the national payment system, the necessity of active participation of non-state actors in the prevention of theft of electronic money is substantiated, in connection with which it is noted the need to expand the list of signs of transactions performed without the consent of the client of a credit institution, as well as the use of biometric authentication of non-cash payments.

Keywords: electronic money, electronic means of payment, biometric authentication, fraud, theft, prevention, subjects, prevention system, crime

Современные достижения науки и техники оказывают решающее значение на общество и государство, выступая как криминогенным, так и антикриминогенным фактором. Согласно официальным статистическим сведениям, опубликованным ГИАЦ МВД России, несмотря на сохраняющуюся тенденцию по снижению преступности, усиливается динамика преступности в сфере информационных технологий. Так, в 2022 г. зарегистрировано 522,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8 % больше, чем за аналогичный период прошлого года [11].

За 6 месяцев 2023 г. указанная тенденция лишь усилилась – зарегистрировано 318,5 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 27,9 %

больше, чем за аналогичный период прошлого года. Более 70 % таких преступлений совершается представляют собой хищения электронных денежных средств [11].

В этой связи Я. И. Гилинский отмечает процесс «переструктуризации» преступности, когда общеуголовная преступность уступает место высоколатентным видам преступлений современности [3. С. 198].

К аналогичным выводам приходят и многие зарубежные авторы. Например, М. Гудман отмечает существенные изменения в структуре современной преступности, объясняя их широким распространением новейших технологий в области робототехники, виртуальной реальности, искусственного интеллекта и т. д. [2. С. 289].

Следует согласиться с мнением Ю. Ю. Комлева о том, что преступность становится «сетевым феноменом», недоступным для противодействия как традиционными методами уголовно-правового противодействия и криминологического предупреждения, так и практиками раскрытия, расследования и предупреждения правоохранительных органов [5. С. 74].

Указанная проблема свидетельствует о необходимости поиска современных решений в сфере предупреждения преступлений, совершаемых с использованием информационных технологий, в частности, хищений электронных денежных средств, как наиболее распространенного деяния в данной группе. Указанная проблема приобретает особенную актуальность в связи с фактическим отсутствием механизма возмещения вреда, причиненного таким преступлением, а также недостатками их раскрытия и расследования.

Следовательно очевидна необходимость разработки современной концепция предупреждения хищений электронных денежных средств, которая должна быть направлена на обеспечение единства действий государственных органов и негосударственных организаций, т. е., субъектов предупредительной деятельности, а также выступать обобщением опыта соответствующей научной и практической деятельности, а также учитывать особенности порядка и правил осуществления безналичных транзакций в условиях национальной платежной системы.

Мы считаем, что одну из ключевых ролей в системе предупреждения хищений электронных денежных средств должны занять именно негосударственные субъекты такой деятельности: кредитные организации, провайдеры, операторы по переводу электронных денежных средств и другие элементы национальной платежной системы, что объясняется особенностями рассматриваемых преступлений. Так, ключевой особенностью хищений электронных денежных средств является применение системы безналичного расчета, равно как и для правомерных банковских операций.

Всего по итогам 1 квартала 2023 г. в России совершено более 1,6 млрд переводов денежных средств на общую сумму более 759 трлн руб., из них более 1,2 млрд операций с использованием сервиса быстрых платежей [10].

По мнению специалистов ПАО «Сбербанк», порядка 95 % крупных компаний недостаточно эффективно справляются с отражением кибератак; по итогам 2022 г. было скомпрометировано 350 млн персональных записей граждан России (данные 65 млн граждан России) [6. С. 384].

Исходя из этого следует, что достижение результатов предупредительной деятельности во многом зависит от качества мониторинга системы безналичного расчета на предмет выявления противоправных операций.

В этой связи нами предлагаются следующие решения, направленные на совершенствование системы предупреждения хищений электронных денежных средств:

1. Обновление алгоритма мониторинга безналичных транзакций посредством расширения признаков операций, совершаемых без согласия клиента.

2. Введение биометрической аутентификации при совершении операций с использованием электронных средств платежа.

Разберем подробнее предлагаемые нами инициативы.

Согласно ст. 3 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации доходов», обязательный контроль – это совокупность принимаемых уполномоченным органом мер по контролю за операциями с денежными средствами или иным имуществом на основании информации, представляемой ему организациями, осуществляющими такие операции, а также по проверке этой информации в соответствии с законодательством Российской Федерации [7].

Так, например, участники платежной системы оказывают услуги по переводу денежных средств, а именно, операторы переводят электронные денежные средства. Провайдер осуществляет общую координацию процесса прохождения платежных средств (электронных денежных средств) между субъектами финансово-хозяйственной деятельности. Всего в России по состоянию на 1 квартал 2023 г. действуют 363 оператора по переводу денежных средств, в частности, кредитных организаций [10].

В специальной литературе, как правило, рассматриваются вопросы блокировки противоправных банковских операций, тогда как недостаточно внимания уделяется мониторингу всей совокупности транзакций в целях выявления операции, совершаемой без согласия клиента. Тогда как в данном случае необходимо учитывать, что установление закрытого перечня признаков противоправной операции не гарантирует обеспечение необходимой степени защищенности сферы безналичных платежей.

Центральный Банк России (далее – ЦБ РФ) установил признаки безналичной транзакции, совершаемой без согласия клиента, в частности, несовпадение характера, параметра, объема, места совершения операции или устройства, с которого она проводится, с данными об обычных для клиента транзакциях. ЦБ РФ также рекомендовал участникам платежной системы интегрировать ряд технологических решений для обеспечения безопасности безналичных операций, в том числе технологии виртуальных частных сетей, многофакторную аутентификацию, а также организовать мониторинг безналичных операций, однако далеко не все кредитные организации до настоящего времени имеют системы распознавания противоправных операций (антифрод). Сущность антифрод системы заключается в анализе закономерностей использования лицом электронных средств платежа, а также выявлении нетипичных для клиента переводов электронных денежных средств, что позволяет своевременно принять меры к блокированию противоправной операции. Следовательно, процесс антифрод-мониторинга представляет собой проверку безналичных операций на предмет наличия признаков противоправной операции с ее блокировкой или приостановкой для последующего расследования.

Любая антифрод система должна состоять из нескольких элементов, каждый из которых отвечает за определенный этап функционирования всей системы, и направлен на решение конкретной задачи. Например, элемент обнаружения выявляет

подозрительную банковскую операцию, элемент мониторинга производит анализ характеристик такой операции, модуль принятия решений определяет реакцию системы на совокупность выявленных признаков, модуль оповещений передает информацию специалисту для проверки принятого системой решения.

Недостаточная эффективность антифрод системы или ее фактическое отсутствие не позволяют добиться существенных результатов в сфере противодействия преступлениям с использованием информационных технологий [12]. Утвержденные ЦБ РФ признаки также не учитывают возможное завладение электронными средствами платежа, получение неправомерного доступа к электронному кошельку для последующего проведения операций и т. д. [9].

Длительное время наиболее распространенной в Российской Федерации системой антифрод мониторинга была Safer Payments, разработанная зарубежной компанией International Business Machines (IBM). Концепция работы данной системы заключалась в сравнительном анализе признаков совершаемых операций с загруженными в систему правилами, в которых описаны в формализованном виде условия блокировок банковских транзакций.

Концептуально иной подход используется, например, в Smart Fraud Detection, представленной в 2016 г. российскими разработчиками Fuzzy Logic Labs. Данная система работает в автономном режиме, используя алгоритмы машинного обучения для своевременного выявления и блокирования противоправных операций.

В ходе автоматического мониторинга операций, в зависимости от выявленных признаков, система получает ряд сигналов, например, BLOCK – блокировка транзакции, HOLD – приостановка транзакции, OK – проведение транзакции. В случае если система посчитала необходимым приостановить транзакцию, информация передается соответствующему специалисту для принятия решения. В свою очередь, специалист собирает дополнительные сведения, и при необходимости связывается с клиентом для уточнения информации или разъяснения происходящего. Исходя из имеющейся информации, специалист принимает решение: провести транзакцию или заблокировать ее. Принятое решение также становится прецендентом, который учитывается системой для дальнейшего мониторинга.

Однако в настоящее время, как отмечают специалисты, большинство программных решений, в частности, средства защиты и ИТ-системы, не соответствуют новым условиям финансово-хозяйственной деятельности, в которых им предстоит выполнять свои функции. Кроме того, после ухода зарубежных поставщиков программного обеспечения, на фоне введенного запрета на использование зарубежного программного обеспечения на объектах критической информационной инфраструктуры, актуализируется необходимость развития импортозамещения, том числе посредством развития отечественных антифрод систем.

Исходя из изложенного, обновление алгоритма мониторинга безналичных транзакций посредством расширения признаков операций, совершаемых без согласия клиента, а также совершенствование антифрод систем, обеспечит большую эффективность предупреждения хищений электронных денежных средств.

Однако, безусловно, система антифрод мониторинга не лишена недостатков. Среди таковых специалисты отмечают низкое быстродействие, являющееся причи-

ной возможной невысокой скорости проверки инцидентов. Кроме того, преступники совершенствуют методы противоправной деятельности и находят новые способы имитации правомерного характера операций.

Следовательно, применительно к системе антифрод мониторинга, необходимо обеспечить реализацию следующих задач:

разработать количественные и качественные признаки операций, совершаемых без согласия клиента;

реализовать механизм автоматического мониторинга операций на основе установленных признаков противоправных операций.

Перспективным решением в сфере специального предупреждения как хищений электронных денежных средств, так и других преступлений, совершаемых с использованием информационных технологий, также является применение технологии биометрической аутентификации при совершении безналичной транзакции. Механизм удаленной идентификации посредством биометрии является элементом системы трехфакторной аутентификации, которая состоит из авторизации в Единой системе идентификации и аутентификации (далее – ЕСИА) и двух биометрических факторов – динамического изображения лица и голоса пользователя.

Каждый человек имеет набор уникальных физиологических характеристик, незначительно изменяющихся в течение жизни, которые позволяют с необходимой степенью достоверности идентифицировать его, например, папиллярные узоры пальцев рук, изображение лица, радужная оболочка глаза, а также и некоторые другие. Такие характеристики называются биометрическими данными. В силу их уникальности указанные данные все чаще используются в практической деятельности для идентификации граждан.

Следовательно, верификация безналичных платежей путем использования биометрических данных, например, путем сканирования папиллярных узоров пальцев рук или лица собственника электронного средства платежа, качественно отличается безопасностью проводимых операций, поскольку не позволяет использовать электронное средство платежа третьим лицам.

Аналогичные выводы делают и зарубежные эксперты. Так, Европейское банковское управление (EBA) отметило перспективы верификации безналичных операций путем использования биометрических данных. Британский банк «NatWest» совместно с Mastercard в 2019 г. создал кредитную карту, операции по которой подтверждаются сканированием отпечатков пальцев [4].

Работа в рамках данного направления в Российской Федерации уже ведется. Так, в 2018 г. по инициативе ЦБ РФ и Министерства цифрового развития, связи и массовых коммуникаций РФ была запущена Единая биометрическая система (далее – ЕБС). Для идентификации ЕБС использует два фактора: лицо и голос [8]. В метро г. Москвы уже действует бесконтактная оплата проезда Face Pay [1]. Считаем возможным апробирование аналогичного алгоритма для верификации безналичных транзакций посредством как специальных камер для контрольно-кассовой техники, так и банковских приложений, установленных на мобильных устройствах собственников электронных средств платежа, установив максимальный лимит на операцию без биометрической аутентификации в размере 10 000 руб., что позволит обеспечить безопасность при проводимых операций.

В целях обеспечения интеграции биометрической аутентификации в систему безналичных платежей, считаем, кредитными организациями должен быть проведен комплекс дополнительных мероприятий, а именно:

– осуществление сбора биометрических данных физических лиц, в том числе посредством использования системы мобильного банкинга;

– применение указанных данных в расчетах посредством верификации платежей и иных операций, осуществления контроля доступа и т. д. Считаем целесообразным применение позитивной стимуляции клиентов кредитных организаций к подключению биометрической аутентификации платежей.

Безусловно, развитие системы биометрической идентификации в России сопряжено с необходимостью решения ряда проблем, к числу которых следует отнести, прежде всего, недостатки и пробелы нормативной правовой основы, регламентирующей ключевые вопросы, связанные с биометрической идентификацией и использованием биометрических данных граждан, недостаточным уровнем теоретического и научно-практического обеспечения биометрической идентификации, в частности, при безналичных расчетах. Важной проблемой выступает также недостаточное доверие граждан к системе ЕБС, гарантиям обеспечения безопасности и конфиденциальности хранящихся биометрических данных.

Кроме того, расширение и дальнейшее развитие биометрических сервисов, в том числе для верификации безналичных операций, увеличение количества ее субъектов, расширение перечня предоставляемых услуг с использованием биометрических данных требуют дополнительного финансирования, организационного и технического обеспечения со стороны заинтересованных субъектов. Однако развитие национальной платежной системы в указанном направлении, по мнению экспертного сообщества, является единственно возможным путем, который позволит технологии биометрической идентификации быть в перспективе массовой и достичь необходимых показателей эффективности ЕБС РФ, определенных стратегией и планами ее развития.

Таким образом, проведенное исследование позволило нам сделать следующие выводы:

Исходя их современного состояния национальной платежной системы Российской Федерации, тенденций развития преступности, актуализируется необходимость предупреждения хищений электронных денежных средств как одного из наиболее сложных уголовно-правовых деяний с точки зрения уголовно-правового противодействия.

Современная концепция предупреждения хищений электронных денежных средств предполагает усиление значимости роли негосударственных субъектов такой деятельности, в частности, посредством мониторинга системы безналичных операций, поскольку иные меры не позволяют обеспечить безопасность национальной платежной системы в достаточной степени.

Обновление алгоритма мониторинга безналичных транзакций посредством расширения признаков операций, совершаемых без согласия клиента, качественно отразится на безопасности национальной платежной системы. В данном случае кредитные организации, использующие антифрод системы, смогут своевременно приостановить подозрительную операцию до выяснения обстоятельств ее совершения.

Дополнительной мерой обеспечения общественных отношений в сферах реализации прав собственности и расчетов, совершаемых с использованием электронных средств платежа, станет биометрическая аутентификация, которая не позволит третьим лицам совершить операцию без согласия собственника электронных денежных средств, что потребует дополнительного оснащения контрольно-кассовой техники или использования смартфонов с приложениями онлайн-банкинга в целях верификации пользователя.

Список литературы

1. Face Pay // Мосметро. URL: https://mosmetro.ru/facepay (дата обращения: 09.08.2023)

2. Goodman M. Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It. New York: Doubleday, 2015. 563 p.

3. Гилинский Я. И. Человеческое, слишком человеческое / Я. И. Гилинский. СПб.: Алетейя, 2020. 240 с.

4. Как биометрия может помочь онлайн-ритейлерам // Ведомости. 2020. 06 янв. URL: https://www.vedomosti.ru/business/ articles/2020/01/06/819822-kak-biometriya-mozhet-pomoch-onlain-riteileram

5. Комлев Ю. Ю. Интегративная криминология: девиантологический очерк. Казань: КЮИ МВД России, 2018. 232 с.

6. Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. № 2. С. 383–390.

7. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 7 августа 2001 г. № 115-ФЗ // СПС «КонсультантПлюс».

8. 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: Федеральный закон от 29 декабря 2022 г. № 572-ФЗ // СПС «КонсультантПлюс».

9. Признаки осуществления перевода денежных средств без согласия клиента: Приказ Банка России от 27 сент. 2018 г. № ОД-2525. Текст: электронный // СПС «КонсультантПлюс».

10. Статистика национальной платежной системы // Банк России: офиц. сайт. URL: https://www.cbr.ru/statistics/nps/psrf

11. Статистические сведения о преступлениях за 2000–2022 гг. // ФКУ «ГИАЦ МВД России». URL: https://x. b1aew.x. p1ai/folder/101762

12. ЦБ впервые оштрафует банки за отсутствие систем распознавания мошеннических операций // Ведомости. 2019. 10 окт. URL: https://www.vedomosti.ru/finance/news/2019/10/10/813384-dva-banka

Н. Р. Шевко,
кандидат экономических наук, доцент,
Казанский филиал
Российского государственного университета правосудия

ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Аннотация. Статья посвящена обобщению официальных статистических данных о состоянии киберпреступности в Российской Федерации и Республике Татарстан. Проанализированы методы и способы совершения преступлений с использованием современных информационных технологий. На основе этого предложены меры противодействия киберпреступности, а также сделаны выводы по проведенному исследованию.

Ключевые слова: киберпреступность, киберпреступник, современные информационные технологии, гаджеты, преступления, совершенные с использованием цифровых технологий

PROBLEMS IN THE FIGHT AGAINST CYBERCRIME

Abstract. This article is devoted to summarizing official statistical data on the state of cybercrime in the Russian Federation and the Republic of Tatarstan. The author analyzed the methods and methods of committing crimes using modern information technologies. Based on this, measures to combat cybercrime are proposed, and conclusions are drawn from the study.

Keywords: cybercrime, cybercriminal, modern information technologies, gadgets, crimes committed using digital technologies

Современные информационные технологии прочно вошли в жизнь современного человека. Благодаря повсеместному распространению телекоммуникационных технологий, неважно в каком месте земного шара находится пользователь, – везде доступны дистанционные технологии обучения, выполнения служебных обязанностей в удаленном режиме, досуг, просмотр интересующих контентов, электронные платежи, интернет-магазины и т. д. В качестве средства удаленного взаимодействия в современном мире не надо иметь мощный компьютер или ноутбук, достаточно смартфона или любого другого гаджета, снабженного необходимым программным обеспечением и, самое главное, – выходом в Интернет.

К сожалению, этим уникальным способом связи пользуются не только в благих целях. В последнее время все чаще фиксируются факты совершения преступлений с использованием высоких технологий. Так, по официальным данным, количество киберпреступлений, зарегистрированных в Российской Федерации, за последние 15 лет возросло более, чем в 40 раз (с 12 тыс. в 2007 г. до 510 тыс. в 2022 [3]). Интересно, что в 2021 г. официально было зарегистрировано 518 тыс. преступлений с использованием информационных технологий, т. е. за год их число сократилось почти на 8 тыс. И это положительная динамика.

Если обратимся к данным официального сайта Генпрокуратуры Российской Федерации [2], то в 2021 г. на территории России их было зарегистрировано

более 770 тыс, т. е. рост более, чем в 60 раз. Причем, это только официально зарегистрированные преступления. Общеизвестно, что, как правило, более 85 % киберпреступности является латентной. Причин тому несколько. Прежде всего, это небольшие суммы ущерба для одного, конкретно взятого человека. Не все готовы пожертвовать своим личным временем для хождения по кабинетам в целях раскрытия и предупреждения данных преступных деяний. Кроме того, порой такие преступления совершаются без нанесения материального ущерба, – например, взлом странички в социальных сетях, либо в мессенджерах. Или сбор средств (на лечение детей, на помощь в СВО и т. п.) по подложному счету. Каждый перечисляет небольшую сумму. Для пресечения преступных действий киберпреступников никому не хочется тратить личное время на выяснение обстоятельств произошедшего. Более того, зачастую сотрудники правоохранительных органов, особенно в отделах полиции, неохотно принимают такие заявления и не так эффективно, как хотелось бы, занимаются расследованием и раскрытием подобного рода преступлений.

Только за 11 месяцев 2022 г. выявлено почти 10 тыс. лиц, совершивших кибермошенничество (по наиболее тяжкому составу преступления). Причем по сравнению с 2021 г. число выявленных преступников, совершивших злодеяния с использованием цифровых технологий, возросло почти на половину (на 45 %) [1].

Среди видов преступлений в виртуальном пространстве лидером является мошенничество – 224 тыс. (или 48 %). При этом количество краж с банковских карт сократилось почти втрое (на 28 %), но возросло число мошенничеств с электронными денежными средствами почти на 5 %.

За 11 месяцев 2022 г. наблюдается рост числа преступлений непосредственно в сфере компьютерной информации выявлено и пресечено почти 9 тыс. фактов проникновения в компьютерные базы и создание вредоносных программ против данных 2020 г. в 4,4 тыс. [4].

Однако возросло число наркопреступлений – бесконтактный сбыт наркотических средств и их прекурсоров на 21 % превышает данные предыдущего года.

Также наблюдается рост числа заведомо ложных сообщений об акте терроризма. Примечательно, что почти 92 % из них совершаются дистанционно.

По данным МВД РФ, раскрываемость преступлений, совершенных с использованием высоких технологий, выросла почти на 5 %.

Кроме того, специальная военная операция на Украине помогла пресечь деятельность ряда колл-центров, расположенных на территории Украины. Например, российские военные раскрыли колл-центр в Бердянске, в котором у мошенников были данные на почти 20 млн россиян, работало там порядка 300 сотрудников.

В целях совершенствования раскрытия, предупреждения и профилактики противодействия киберпреступлениям недостаточно только правовых мер. Современное российское законодательство в полной мере отвечает требованиям современности.

Для эффективного противодействия преступности в виртуальном пространстве необходимо привлекать квалифицированных специалистов. Например, при восстановлении данных на поврежденных серверах зачастую привлекают специалистов «Сбера», экспертов «Лаборатории Касперского». Кроме того, основы информационной безопасности введены практически во всех учебных планах высшего образования, по некоторым специальностям в среднем профессиональном образовании.

Помимо этого, на базе учебных заведений создаются дополнительные возможности для углубленного изучения проблем информационной безопасности и мер противодействия им. Так, на базе Казанского юридического института МВД России была создана факультативная группа курсантов старших курсов для детального рассмотрения наиболее часто встречающихся методов и способов совершения киберпреступлений в целях оперативного их пресечения. Для обучения в качестве преподавателей были привлечены сотрудники правоохранительных органов из соответствующих отделов ГСУ МВД по РТ, БТСМ МВД по РТ, а также ЭКЦ МВД по РТ.

В последнее время все чаще стали фиксироваться DDoS-атаки, отличающиеся профессиональным исполнением. Современные кибератаки стали отличаться от предыдущих длительностью, увеличенной в разы, а также уровнем их исполнения. Кроме того, все чаще наблюдаются целевые кибератаки, в которых злоумышленники учитывают специфику архитектуры и мельчайшие детали отдельных сайтов. В целях противодействия профессиональным хакерам в Оренбурге на базе госуниверситета открылся центр Национального киберполигона, отвечающего самым современным требованиям. На этой базе моделируются возможные кибератаки, что позволяет студентам и профильным специалистам без ущерба для инфраструктуры организации учиться и реально отражать кибератаки.

Еще одним из основных направлений обеспечения противодействия киберпреступности является информационная грамотность населения. Элементарные правила создания и хранения паролей, запрета на распространение информации о личных счетах, банковских картах и пр. третьим лицам в современном мире должны знать и соблюдать все, от мала до велика. Необходимо увеличить количество социальной рекламы, в том числе по противодействию киберпреступности, в средствах массовой информации, по телевизору, в общественных местах, на транспорте и т. д.

Для эффективного противодействия киберпреступности необходимо знать причины, мотив, цель совершения преступлений, а также более детально изучить криминалистическую характеристику киберпреступника и его жертвы. Только объединив усилия правоохранительных органов, высококвалифицированных специалистов в компьютерной сфере, законодателей, а также общественности, возможно будет противостоять распространению и увеличению количества преступлений, совершенных с использованием информационных технологий.

Список литературы

1. МВД: ИТ-преступность снизилась из-за закрытия украинских колл-центров // Официальный сайт МВД Медиа. URL: https://mvdmedia.ru/news/official/vladimir-kolokoltsev-prinyal-uchastie-v-soveshchanii-ministrov-vnutrennikh-del-i-obshchestvennoy-bez

2. Портал правовой статистики // Официальный сайт Генеральной прокуратуры РФ. URL: http://crimestat.ru/offenses_chart

3. Потери от киберпреступности // TAdvise. российский интернет-портал и аналитическое агентство. URL: https://www.tadviser.ru/index.php

4. Сводные статистические сведения о состоянии судимости в России за 2010–2022 годы // Официальный сайт Судебного департамента при ВС РФ. URL: http:/cdep.ru

В. Н. Щепетильников,
кандидат юридических наук,
Елецкий государственный университет имени И. А. Бунина

ЕЩЕ РАЗ К ВОПРОСУ О ПОНЯТИЯХ В УГОЛОВНОМ ПРАВЕ

Аннотация. Цифровые технологии не только привносят в мир удобства и эффективность, но дают почву для видоизменения преступников и преступности. В статье затрагивается проблема роста количества киберпреступлений, регулярного внесения изменений в уголовный закон, сложностей, возникающих при квалификаций преступлений в свете развития цифровых технологий и трансформации общественных отношений.

Ключевые слова: уголовное право, цифровые технологии, уголовно-правовые отношения, система, преступление, наказание, закон

ONCE AGAIN TO THE QUESTION OF CONCEPTS IN CRIMINAL LAW

Abstract. Digital technologies not only bring convenience and efficiency to the world, but also enable the transformation of criminals and crime. The article touches on the problem of the increase in the number of cybercrimes, regular changes to the criminal law, and difficulties arising in the classification of crimes in the light of the development of digital technologies and the transformation of social relations.

Keywords: criminal law, digital technologies, criminal law relations, system, crime, punishment, law

В теории уголовного права под уголовно-правовыми отношениями принято понимать отношения, возникающие в связи с совершением преступления [11. С. 7]. Причем, у ряда ученых это лишь одна из разновидностей отношений, именуемых охранительными и возникающих между государством и преступником [10. С. 5]. Кроме того, это могут быть отношения, возникающие вследствие обстоятельств, исключающих преступность деяния; а также отношения, связанные с воздержанием лица от преступного поведения под угрозой уголовного наказания. Схожую точку зрения мы видим и у наших уральских коллег [6. С. 2; 8–29].

На наш взгляд, в систему уголовно-правовых отношений следует включать любые отношения, порождающие, изменяющие или прекращающие своим возникновением определенные уголовным законодательством РФ права, обязанности и ответственность для их непосредственных участников и лиц, включенных в их оборот опосредованно.

Участником этих отношений являются:

– лицо, совершившее преступное деяние (подозреваемый, обвиняемый, подсудимый, отбывающий наказание), а также все его соучастники.

– со стороны государства – это суд и иные участники уголовного судопроизводства со стороны обвинения по смыслу раздела 2 УПК РФ [1]: прокурор, следователь, руководитель следственного органа, органы дознания и их начальники,

потерпевший, частный обвинитель и гражданский истец, а также представители потерпевшего, гражданского истца и частного обвинителя.

– со стороны защиты – соответственно это законные представители несовершеннолетнего подозреваемого или обвиняемого, защитник, гражданский ответчик и его представитель.

– свидетели, эксперты, специалисты, переводчики, понятые.

Все вышеназванные лица вступают в уголовно-правовое отношение в определенный момент, на определенной стадии. Хотя, разумеется, не всегда их участие обязательно, с учетом специфики уголовного деяния. Здесь, вроде бы, все понятно.

В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3] есть термин информационные технологии, под которыми подразумеваются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Других близких по смыслу и значению терминов в законодательстве России не встречается.

Можно было бы поставить знак равенства между понятиями «цифровые технологии» и «информационные технологии», поскольку и в том, и в другом случаях мы имеем дело с преобразованием информации различной природы и ценности в цифровую форму для ее последующего использования по назначению в интересах личности, общества или государства.

Например, Указом Президента Российской Федерации от 30 сентября 2022 г. № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации» [4] Центру биометрических технологий поручено заниматься развитием цифровых технологий идентификации и аутентификации, в том числе на основе биометрических персональных данных, а также сервисов подписания и хранения документов, включая создание, развитие и эксплуатацию коммерческих сервисов и типовых решений. Т. е. в данном случае речь идет о таких технологиях, которые позволят бездокументарно подтвердить, что конкретный человек является именно тем, с которым связаны определенные юридические факты. Кстати, очень перспективная технология, которая безусловно приведет к попыткам применения и злоумышленниками. Ведь сегодня уже распространилась так называемая методика синтеза изображения или голоса, основанная на искусственном интеллекте, используемая для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики (deepfake).

Любая технология, призванная облегчить, автоматизировать, повысить эффективность и КПД рутинных действий человека, может стать объектом (предметом) преступного посягательства. С другой стороны, подобные технологии призваны наоборот помогать в выявлении, расследовании преступлений, в том числе и так называемых высокотехнологичных.

В системе уголовно-правовых отношений такие технологии занимают особое место. Например, деятельность «онлайн-платформ», используемых в преступной деятельности, пока не нашла своего места в УК РФ, хотя фактически такая платформа «дает возможность скрыть факт совершения преступления и его следы

посредством анонимизации пользователя и осуществления платежей с помощью криптовалют. То есть платформа предоставляет лицам, сбывающим незаконные товары, необходимые средства для совершения преступлений и устраняет препятствия для совершения таких действий» [5. С. 53].

С другой стороны, в литературе рассматриваются возможности и необходимость создания цифрового уголовно-правового ресурса в помощь государству для борьбы с криминальным элементом [7. С. 361–366]. Действительно, обсуждаемая концепция С. Я. Лебедева, связанная с использованием цифровых технологий, заслуживает внимания. По мнению автора, в киберпространстве должен быть разработан самостоятельный цифровой уголовно-правовой сегмент, позволяющий обуздать киберпреступность. В основе такой системы должен лежать адекватный цифровой уголовно-правовой ресурс (ЦУПР). Эта система должна обеспечивать контроль как за реальными деяниями, так и за виртуальными, что позволит на законных основаниях мгновенно блокировать террористический или экстремистский ресурс при выявлении лингвистических или вербальных признаков.

Можно конечно порассуждать о появлении такой системы, которая при мониторинге позволит блокировать попытки загрузить/скачать в сеть порнографические материалы, а также защитить авторские права от незаконных «закачек» и т. д. Неплохо было бы вначале предупреждать пользователя, что его действия в сети подпадают под уголовную ответственность, и если он не прекратит свои действия, то факт совершения преступного деяния будет зафиксирован, данные автоматически будут направлены в специальное хранилище электронных доказательств, а сам компьютер заблокирован, злоумышленник будет идентифицирован и задержан. Как знать, может, скоро так и будет.

Если говорить о технологиях применительно к участникам этих отношений, то с учетом вышеназванных лиц следует иметь ввиду цифровые технологии, используемые для позитивной общественно-полезной деятельности, в частности для выявления и расследования преступлений, а также технологии, которые наоборот могут быть использованы в качестве средства, орудия преступления. В обоих случаях они оказываются вовлечены в систему уголовно-правовых отношений, но на разных временных этапах.

Так, новой разновидностью преступлений стали «криптопреступления», о необходимости подробного изучения которых с точки зрения их квалификации, определения ущерба, возможности дифференциации уголовной ответственности за их совершение пишут коллеги [8. С. 113]. Авторами анализируется необходимость криминологического изучения криптопреступности, с точки зрения разработки системы мер противодействия и подготовки кадров для его осуществления. Между тем, в УК РФ нет пока норм об уголовной ответственности за преступления с цифровыми финансовыми активами, цифровой валютой…

На проблему «отставания социального контроля от развития общества и изменения преступности» обращают внимание ряд наших коллег [9. С. 585–598], связанную с необходимостью адаптации норм уголовного закона к условиям информационного общества без «цифровых двойников» традиционных уголовно-правовых запретов. Нынешним преступным деяниям в сфере высоких технологий действительно присущи такие черты, как экстерриториальность, виртуальность,

масштабность, воспроизводство, многоликость, скрытность. И потому возможность появления «цифровой личности» уже не представляется такой фантастической, как еще десять-пятнадцать лет назад.

В одной работе наших молодых коллег встретилось название «Преступления в сфере цифровой информации: понятие и виды» [12]. Уж сколько было сломано копий еще в начале 2000-х относительно того, как же нужно назвать главу 28 УК с учетом происходящих изменений? Практика показала, что здесь законодатель непоколебим. Мы в свое время предлагали законодателю пойти по одному из двух направлений [15. С. 41]. Первое: путем изменения наименования и содержания главы 28 УК РФ «Преступления в сфере компьютерной информации» на «Преступления в сфере электронной информации», куда войдут новые составы преступлений с учетом реалий информационных технологий. Второе: путем внесения дополнений в некоторые составы преступлений с указанием на способ их совершения. Оказалось, что второй путь стал реалистичнее. Хотя и здесь с появлением новых составов возникли сразу споры о неуместном расположении этих норм применительно к объектам посягательства.

В этой связи представляет особый интерес монография Е. А. Русскевича «Уголовное право и «цифровая» преступность»: проблемы и решения» [13], в которой автор анализирует вопросы противодействия цифровой преступности, предложив свой вариант главы 28 УК РФ.

В то же время наши белорусские коллеги не так радужно оценивают приход цифровых технологий [14. С. 214], считая их использование в уголовном праве и криминалистике преждевременным, до устранения различий в понимании объекта преступления в уголовном праве и криминалистике.

Казалось бы, законодатель регулярно вносит изменения в Уголовный закон. Почему же количество киберпреступлений не уменьшается, а наоборот? По данным МВД РФ, только за 7 месяцев 2023 г. на 27,9 % возросло количество зарегистрированных киберпреступлений (371,4 тыс. – январь-июль 2023; 290,3 тыс. – январь-июль 2022) [16]. В то же время на 24,8 % уменьшилось количество мошенничеств с использованием электронных средств платежа и на 8,7 % – мошенничеств в сфере компьютерной информации.

Справляется ли уголовный закон со своей задачей применительно к киберпреступлениям в настоящее время? Однозначно ответить нельзя. Это побуждает всю когорту правоприменителей, ученых, законодателя работать в одном порыве, приближая тот день, когда кривая киберпреступности неуклонно пойдет вниз. Не последнюю роль в этих процессах должна сыграть интеграция, формирование единообразного понятийного аппарата, чтобы сначала любой правоприменитель, а позднее и суд не сомневался при квалификации содеянного. И конечно же, государство должно быть заинтересовано в ликвидации отставания стражей порядка в оснащенности, техническом вооружении и подготовке от преступников, чтобы не дать им шансов.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СПС «ГАРАНТ». URL: https://internet.garant.ru/#/document/12125178/paragraph/53424899:13

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «ГАРАНТ». URL: https://internet.garant.ru/#/document/10108000/paragraph/26654339:0

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» СПС «ГАРАНТ». URL: https://internet.garant.ru/#/document/12148555/paragraph/3471:8

4. Указ Президента РФ от 30 сентября 2022 г. № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации» // СПС «ГАРАНТ». URL: https://internet.garant.ru/#/document/405365909/paragraph/1/doclist/1176/1/0/0/цифровые%20технологии:0

5. Дремлюга Р. И., Коробеев А. И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности // Всероссийский криминологический журнал. 2022. Т. 16, № 1.

6. Козаченко И. Я., Г. П. Новоселов. Уголовное право. Общая часть: учебник для вузов. 6-е изд., перераб. и доп. М.: Юрайт, 2023. 430 с. (Высшее образование) // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/510665

7. Корчагин А. Г., Гомзякова Е. М. К вопросу о создании цифрового уголовно-правового ресурса // Балтийский гуманитарный журнал. 2021. Т. 10. № 4.

8. Репецкая А. Л., Миронов А. О. Криптовалюта как объект уголовно-правового и криминологического исследования // Вестник Восточно-Сибирского института МВД России. 2022. № 3.

9. Русскевич Е. А., Дмитренко А. П., Кадников Н. Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. Т. 13. Вып. 3.

10. Уголовное право. Общая часть: Учебник. Издание второе перераб. и доп. / под ред. доктора юридических наук, профессора Л. В. Иногамовой-Хегай, доктора юридических наук, профессора А. И. Рарога, доктора юридических наук, профессора А. И. Чучаева. М.: Юридическая фирма «Контракт»: Инфра-М, 2008.

11. Уголовное право России. Части Общая и Особенная: учебник (коллектив авторов; под ред. д. ю.н., проф. А. В. Бриллиантова; 3-е изд., перераб. и доп.). М.: Проспект, 2021.

12. Феткулин Р. Р., Арюков А. К. Преступления в сфере цифровой информации: понятие и виды // Baikal Research Journal. 2019. Т. 10, № 3. DOI:10.17150/2411–6262.2019.10(3).17

13. Фоменко Е. В., Каменева З. В. Рецензия на монографию Е. А. Русскевича «Уголовное право и «цифровая» преступность»: проблемы и решения» // Правовая культура. 2022. № 4.

14. Хлус А. М. Цифровизация уголовно-правовых дисциплин в аспекте унификации систем их знаний и развития интеграции // Обеспечение национальной безопасности в свете глобальных вызовов современности: материалы Международной научно-практической конференции. Иркутск, 2021.

15. Щепетильников В. Н. Уголовно-правовая охрана электронной информации: дис. ... канд. юрид. наук. Елец, 2006.

16. Краткая характеристика состояния преступности в Российской Федерации за январь–июль 2023 года. URL: https://мвд.рф/reports/item/40874008

К. Ю. Щербак,
аспирант,
Институт правовых исследований,
Национальный центр законодательства и правовых исследований
Республики Беларусь

НЕКОТОРЫЕ АСПЕКТЫ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ В СЕТИ «ИНТЕРНЕТ»

Аннотация. Целью исследования является рассмотрение некоторых аспектов защиты прав потребителей в сети Интернет. Анализ показал, что продавцами интернет-площадок допускаются ряд нарушений нормативных положений, что влечет за собой риск оборота и реализации потребителю небезопасной продукции. Решение такой проблемы носит комплексный характер и предполагает принятие не только мер реагирования в рамках одного государства, но и противодействие совместными усилиями в рамках интеграционных образований. В статье сделан акцент на уголовно-правовой защите права потребителей на безопасную продукцию.

Ключевые слова: права потребителей, электронная торговля, преступление, ЕАЭС, безопасность продукции, e-commerce, интернет-магазин

SOME ASPECTS OF CRIMINAL LEGAL PROTECTION OF CONSUMER RIGHTS ON THE INTERNET

Abstract. The purpose of the study is to consider some aspects of consumer protection on the Internet. The analysis showed that sellers of Internet sites commit a number of violations of regulations, which entails the risk of circulation and sale to the consumer of unsafe products. The solution of such a problem is complex in nature, it involves the adoption of not only response measures within the framework of one state, but also counteraction by joint efforts within the framework of integration entities. The article focuses on the study of issues of criminal law protection of the right of consumers to safe products.

Keywords: consumer rights, e-commerce, crime, EAEU, product safety, e-commerce, online store

Введение. С каждым годом на просторах мирового пространства, в том числе и в странах Евразийского экономического союза (далее – ЕАЭС), участницей которого является и Республика Беларусь, увеличивается количество лиц, пользующихся ресурсами сети Интернет. И если когда-то совершение покупок посредством глобальной сети Интернет не было столь популярным, то уже сегодня это явление можно наблюдать повсеместно. О стремительном росте интернет-торговли свидетельствует и возрастающее число интернет-магазинов, которых на 1 января 2023 г. в Республике Беларусь было зарегистрировано 28 927 (по сравнению с началом 2022 г. увеличилось на 3,7 % (или на 1036 единиц) [5]. В контексте цифровой эпохи и развития электронного рынка насущным вопросом является обеспечение защиты права потребителей на приобретение безопасной продукции.

Основная часть. Большинство потребителей считают, что совершать покупки онлайн безопасно и что безопасность обеспечивается в той же мере, что и на традиционных рынках [6]. Однако выявляемые нарушения в деятельности интернет-магазинов говорят об обратном: потребители в интернет-среде могут приобрести опасную продукцию, причем риск возрастает из-за виртуальности среды. В качестве примера можно привести случай, выявленный в результате проверки деятельности интернет-магазина в Республике Беларусь, в ходе которого был установлен факт предложения к реализации небезопасных погружных вибрационных электронасосов. Что больше всего вызывает озабоченность, так это то, что применение таких приборов не допускается детьми, людям с пониженными физическими, сенсорными или умственными способностями, однако никакой предупреждающей информации об этом не содержалось [2].

Такие примеры не являются единичными как и в Республике Беларусь, так и на мировой пространстве. Такое положение дел вызывает озабоченность, ведь использование небезопасных товаров, как и одежды, игрушек, продуктов питания, электрических приборов, приобретенных на торговых интернет-площадках, может нести риск причинения вреда жизни и(или) здоровью населения.

В связи с чем защита права потребителей на безопасную продукцию, каковой она должна быть, в том числе, если и находится в торговом обороте в сети Интернет, требует пристального внимания со стороны государств. Обеспечить защиту в онлайн-среде можно лишь принятием комплекса мер, охватывающих и нормативно-правовое регулирование, и обеспечение их практической реализации через деятельность органов, обеспечивающих обращение в торговом пространстве безопасной продукции. Ведь принятие нормативного регулирования в данной сфере еще не означает, что все субъекты являются добросовестными и будут следовать нормативным предписаниям. В качестве действий таких субъектов могут быть, как и, казалось бы, простое игнорирование требований о размещение на сайте интернет-магазина информации о наименовании производителя, организации, уполномоченной на устранение недостатков, регистрации интернет-магазина в торговом реестре, указании адреса места нахождения производителя и импортера и т. п., но которые могут свидетельствовать о нарушении прав потребителя.

В связи с развитием рынка электронной торговли в рамках ЕАЭС, вопросы защиты прав потребителей, совершающих покупки в сети Интернет, все чаще становятся предметом для обсуждения, вызывают необходимость создания единых норм права ЕАЭС в сфере e-commerce [1. С. 90]. Вопросам цифровой трансформатизации ЕАЭС посвящен документ «Цифровая повестка ЕАЭС до 2025 г.» [4. С. 104]. Страны-участницы ЕАЭС осознали, что в условиях элетронной торговли обеспечение безопасности потребителей требует принятия общих подходов к защите прав потребителей в электронной торговле, получивших отражение в распоряжении Коллегии Евразийской экономической коллегии от 20 июня 2023 г. № 88 «О проекте Соглашения об электронной торговле в Евразийском экономическом союзе».

Ранее мы отметили, что защита права потребителей на безопасную продукцию требует комплекса мер, одним из способов реагирования на факты нарушений являются и меры уголовной ответственности, установленные и в Республике Беларусь. В уголовном законодательстве в качестве основной уголовно-правовой нормы,

которая охраняет отношения в сфере здоровья населения от недобросовестных субъектов, выступает ст. 337 Уголовного кодекса Республики Беларусь от 9 июля 1999 г. № 275-З (далее – УК). Сфера действия данной статьи распространяется на случаи, когда субъект осуществляет и реализацию продукции, которая не отвечает требованиям безопасности, потребителю. Несмотря на ранее рассмотренные выявленные случаи реализации продукции с использование сети Интернет, которая представляла опасность и не отвечала требованиям технических стандартов, в тексте уголовно-правовой ст. 337 УК не используется указание на признак использования сети Интернет как обязательного признака преступления. Такой признак не закреплен и в нормах уголовных законов других государств-членов ЕАЭС.

В Особенной части УК упоминание о глобальной компьютерной сети Интернет в качестве основного или квалифицирующего признака преступления есть в ряде норм, преимущественно это связано с совершением деяний в отношении государственных интересов (например, ст. 341–1, 361, 367, 369 УК и др.).

Особенностью уголовного закона в Российской Федерации является включение в качестве признака преступления в ч. 1.1 ст. 238–1 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ признака «использование средств массовой информации или информационно-телекоммуникационных сетей, в том числе сети «Интернет» в отношении лекарственных средств медицинских изделий [3. С. 32]. Такое преступление по классификации В. С. Соловьева можно отнести к группе деяний, имеющих своей целью привлечь внимание потребителя к приобретению товаров, продаваемых незаконно [3. С. 32]. По аналогии с этим, преступление и ст. 337 УК, а также и уголовно-правовые нормы стран-участниц ЕАЭС в этой сфере, можно отнести к этой группе.

Заключение. В связи с постоянно возрастающим ростом товарооборота интернет-магазинов крайне важным является соблюдение продавцами предусмотренных законодательством требований. Основной момент заключается в том, что, несмотря на реализацию товаров с помощью интернет-площадок, они должны отвечать свойствам безопасности.

В заключение отметим, что, учитывая возможные факты использования сети Интернет для совершения преступления, выразившегося в реализации продукции, не отвечающей требованиям безопасности, перспективным направлением усиления уголовно-правовой защиты прав потребителей на безопасную продукцию видится внесением изменений и дополнений в основные уголовные законы стран-участниц ЕАЭС и включение такого признака в качестве признака преступления. Применительно к уголовному закону Республики Беларусь нам видится правильным включить признак «с использованием сети Интернет» в основной состав преступления, предусмотренный ч. 1 ст. 337 УК («Выпуск на товарный рынок или реализация продукции, в том числе и с использованием сети Интернет…»).

Список литературы

1. Валовенко М. В. Направления развития регулирования трансграничной электронной торговли на пространстве ЕАЭС // Молодой ученый. 2023. № 9(456). С. 90. URL: https://moluch.ru/archive/456/100485

2. Интернет-магазин в Витебске продавал небезопасные погружные электронасосы. URL: https://www.belta.by/regions/view/internet-magazin-v-vitebske-prodaval-nebezopasnye-pogruzhnye-elektronasosy-572195–2023/?ysclid=lm6o8g8i2r482516569

3. Соловьев В. С. Криминализация деяний, совершаемых с использованием сети Интернет: опыт Российской Федерации и Республики Беларусь / В. С. Соловьев // Вестник Могилевского института МВД: научно-практический журнал. 2020. № 2. С. 32.

4. Лямцева А. А. Цифровая трансформация в странах-членах ЕАЭС как фактор повышения национальной конкурентоспособности продукции / А. А. Лямцева // Молодой ученый. 2021. № 48(390). С. 104. URL: https://moluch.ru/archive/390/85976

5. Растущую интернет-торговлю хотят отрегулировать. Что может измениться. URL: https://ilex.by/rastushhuyu-internet-torgovlyu-hotyat-otregulirovat-chto-mozhet-izmenitsya

6. The Consumers international guidelines for online product safety. URL: https://www.consumersinternational.org/media/368991/online-product-safety-guidelines-report_final.pdf

А. А. Юсупова,
адъюнкт,
Казанский юридический институт
Министерства внутренних дел Российской Федерации

ЦИФРОВАЯ ПРЕСТУПНОСТЬ В УСЛОВИЯХ ПАНДЕМИИ

Аннотация. В статье описывается влияние цифровых технологий на киберпреступность во время пандемии COVID-19. Приводятся статистические данные активных абонентов подвижной радиотелефонной связи, которые используют услуги доступа к сети Интернет. Рассматриваются основные цели киберпреступников во время пандемии, приводятся примеры мошеннических схем. Предлагаются меры профилактики киберпреступности в период пандемии.

Ключевые слова: право, коронавирус, COVID-19, пандемия, цифровая преступность, цифровые технологии, киберпреступники, киберпреступность, цифровая преступность, кибератака, кибербезопасность

DIGITAL CRIME IN A PANDEMIC

Abstract. The article describes the impact of digital technologies on cybercrime during the COVID-19 pandemic. Statistical data of the population using the Internet for the last 8 years are given. The statistics of the number of active mobile radiotelephone subscribers who use Internet access services are given. The main goals of cybercriminals during the pandemic are considered, examples of fraudulent schemes are given. Suggestions are made for the prevention of cybercrime during a pandemic.

Keywords: law, coronavirus, COVID-19, pandemic, digital crime, digital technologies, cybercriminals, cybercrime, digital crime, cyberattack, cybersecurity

Во время пандемии COVID-19 произошло изменение в экономической и социальной сферах жизни людей во всем мире (рис. 1). Из-за повышения роли дистанционной работы и онлайн-обучения, и большего времяпровождения гражданами в сети Интернет увеличилось число жертв потенциальных киберпреступников. Работа в Интернете в период самоизоляции подвергла людей большему риску из-за новых видов атак киберпреступников.

Киберпреступление – это деятельность преступной направленности, целью которой является неправомерное использование цифровой среды [8. С. 239].

Общество и преступность имеют тенденцию постоянно видоизменяться и совершенствоваться из-за появления социальных и технологических инноваций. Инновации носят в себе не только прогрессивные изменения, которые влияют на новый тип общества, но и порождают новые технологически детерминированные формы преступности [2. С. 17].

В соответствии со стратегией национальной безопасности Российской Федерации стремительное развитие информационных технологий может привести к вероятному возникновению угроз безопасности граждан, общества и государства.

В уголовном кодексе нет четкого определения киберпреступности. Киберпреступлениye – понятие больше криминологическое, чем уголовно-правовое, которое основывается на способе совершения уголовного наказуемого деяния при помощи высоких технологий.

Новая коронавирусная инфекция нанесла серьезный удар по всем сферам общества [9], а также внесла свои коррективы в правовую и судебную систему во многих странах мира. В России были внесены изменения в статью 6.3, 13.15 КоАП РФ [1]. Введены новые статьи 207.1, 207.2 УК РФ и внесены изменения в статью 236 УК РФ [5].

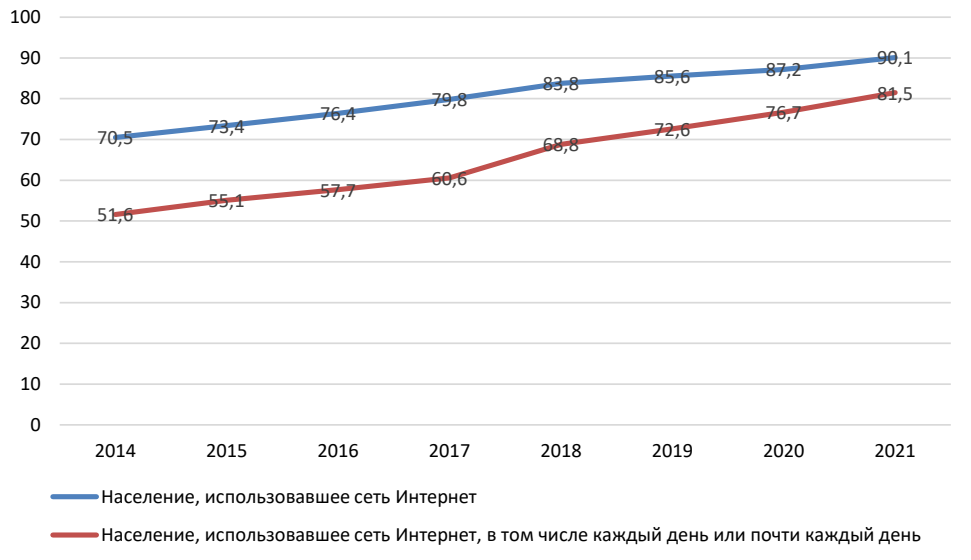


Рис. 1. Население, использовавшее сеть Интернет, в том числе каждый день или почти каждый день [7]

Согласно данным сборника социально-экономических показателей России федеральной службы государственной статистики, население, использовавшее сеть Интернет с 2014 г. по 2021 г., постоянно растет (рис. 1). Количество людей с 2019 г. использовавшие Интернет почти каждый день выросло, по сравнению с 2014–2018 годами.

Согласно данным сборника социально-экономических показателей Российской федеральной службы государственной статистики, число активных абонентов подвижной радиотелефонной связи, использующих услуги доступа к сети Интернет, за 2019 по 2021 г. больше чем за 2016 по 2018 год (рис. 2).

Рис. 2. Число активных абонентов подвижной радиотелефонной связи, использующих услуги доступа к сети Интернет, тыс. [7]

В информационном пространстве не стоит забывать про цифровую гигиену. Цифровой мир – это джунгли, которые иногда населены не самыми приятными формами жизни и в период пандемии не все были морально, технически и психологически готовы в него погрузиться с головой. Данный мир таил в себе новые неизведанные опасности, с которыми до этого пользователь информационной сети еще не сталкивался. Как и в живой природе, в ней есть «жертва», а есть «хищник», где при любой неосторожности ты можешь попасться в сеть киберпреступников.

Так как люди из «реальной» жизни были вынуждены переместиться в «виртуальную» жизнь, а преступники, в свою очередь, по аналогии из офлайн жизни переместились в онлайн. Данное явление можно назвать перетеканием преступности, либо перераспределением преступности.

«Инструментами» киберпреступников служат использование средств социальной инженерии (получения личной информации путем злоупотребления доверием) или распространение вирусных программ, программ вымогателей. Из видов атак можно выделить телефонную, компьютерную атаку, а также атаку путем удаленного управления персональным компьютером.

Рассмотрим статистические данные попыток использования программ-вымогателей во всем мире под влиянием пандемии (рис. 3).

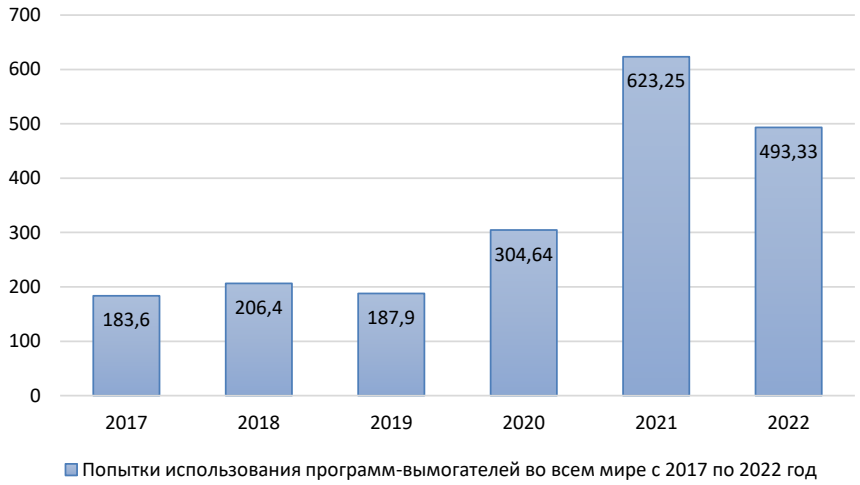


Рис. 3. Попытки использования программ-вымогателей во всем мире 2017 по 2022 г. (в млн) [10]

Согласно данным сайта статиста.ком, самое наибольшее количество попыток использования программ-вымогателей во всем мире с 2017 по 2022 г., наблюдался в 2021 г. Мы можем наблюдать к значительный рост начиная с 2020 г. В первую очередь это может быть связано с тем, что киберпреступники целенаправленно переквалифицировались на информационное пространство. Из-за роста количества человек в период самоизоляции в сети Интернет, выросло и число киберпреступников.

Согласно данным сайта статиста.ком, годовая доля организаций, которые больше пострадали от атак программ-вымогателей по всему миру, наблюдается с 2020 года по сегодняшний день (рис. 4). До пандемии COVID-19 в 2018–2019 гг. данный показатель находился примерно на одном уровне.

Рис. 4. Годовая доля организаций, пострадавших от атак программ-вымогателей по всему миру, с 2018 по 2023 г. [11]

Рассмотрим основные цели киберпреступников во время пандемии COVID-19:

1. Экономическая цель, которая преследует получение материальной выгоды.

Из-за страха людей перед коронавирусной инфекцией, киберпреступники наживались на своих жертвах, предлагали медицинские консультации, диагностику, лечение COVID-19, занимались продажей фейковых цифровых пропусков, поддельных лекарств, либо продавали несуществующие дезинфицирующие и медицинские средства индивидуальной защиты, где требовали внести предоплату, получали деньги, но товар не предоставляли.

ООН подчеркивает, что для укрепления нормативно-правовой базы необходимо использовать масштабный подход для криминализации производства и контрабанды фальсифицированной продукции медицинского назначения [3].

Из-за высокой активности граждан онлайн-покупок в сети Интернет, приобретения продуктов питания и товаров повседневного спроса, киберпреступники при помощи поддельных страниц служб доставки, похищали информацию о банковских картах и денежных средствах пользователей интернет-пространства.

Также были популярны предложения по обработке квартиры от коронавирусной инфекции (псевдодезинфекторы) и продажа ложных экспресс-тестов на коронавирус.

2. Политическая цель, которая выражается в нанесении ущерба репутации различных государственных структур путем подрыва у общества доверия к действующей власти.

Согласно стратегии национальной безопасности Российской Федерации, расширение использования информационных технологий ведет вмешательству во внутренние дела государства, подрыву суверенитета и нарушению территориальной целостности. Большинство подобных информационных атак осуществляется с территорий иностранных государств.

В сфере высоких технологий утекали данные исследований о COVID-19. Каналом утечек информации, связанной с пандемией, стала сеть Интернет. Киберпреступники целенаправленно взламывали и похищали данные разработок COVID-19 для их разглашения в средствах массовой информации. Также в данном вопросе можно выделить страх и неготовность россиян вакцинироваться отечественной вакциной.

3. Идеологическая цель, которая выражается в распространении идей и различного рода идеологий, которые подрывают традиционные государственные ценности. Данная цель тесно взаимосвязана с политической целью, которая направлена на создание и распространение новых идеологий о COVID-19.

Пожилые граждане в большинстве случаев менее осведомлены об онлайн-опасностях в сети Интернет и часто становились целью киберпреступников. Пожилое население часто загружали и пересылали ссылки, которые заражены вирусами, через спам-сообщения о коронавирусной инфекции и неосознанно распространяли дезинформацию среди своих знакомых. В данном вопросе стоит проблема инфодемии в период пандемии, то есть распространение дезинформации о коронавирусной инфекции.

4. Социальная цель, которая преследует получение персональных данных человека, для дальнейшего их использования.

Согласно исследованию экспертно-аналитическому центру ГК InfoWatc, из государственных и муниципальных учреждений утекали персональные данные лиц, которые находились на карантине, лиц, которые являлись нарушителями режима самоизоляции. Утечка персональных данных является острой проблемой, которая требует новых современных решений.

Также было распространено создание сайтов с раздачей бесплатных масок, где происходил сбор персональных данных (ФИО, адрес, телефон, номера банковских карт и т. д.).

5. Психологическую цель, с намерением нанесения морального вреда гражданам в условиях стресса людей, которые крайне восприимчивы к теме COVID-19. Так, людям присылались письма с тематикой коронавирусной инфекции якобы от официальных организаций, с ссылками на вредоносные программы, программы вымогатели. Либо киберпреступники создавали фейковые веб-порталы, замаскированные под различные организации.

Среди предложений профилактики киберпреступности в период COVID-19 можно выделить:

Во-первых, усиление просветительской деятельности. Необходимо повышать осведомленность граждан об опасности, которая исходит из Интернет-пространства. На тему информационной безопасности требуется проводить открытые лекции, семинары, конференции среди граждан. Оповещать население о популярных интернет-мошенничествах с помощью рассылки SMS сообщений, рассылать буклеты с возможными мошенническими схемами в почтовые ящики. Вести пропаганду базовых правил «цифровой гигиены».

Во-вторых, следует организовать проверку на стратегически значимых объектах государственной инфраструктуры на готовность к отражению кибератак. В 2022 г. Россия вошла в топ-10 стран по цифровизации государственного управления [4]. Из-за этого стоит острая необходимость проведения профессионального анализа информационной безопасности.

В-третьих, необходимо поддерживать и развивать разработки отечественного программного обеспечения, направленные на защиту от киберугроз.

Согласно стратегии национальной безопасности Российской Федерации, использование иностранных информационных технологий повышает уязвимость российских информационных ресурсов к воздействию из-за рубежа.

В-четвертых, отсутствует отечественный сбор статистических данных о киберпреступности, вследствие чего сложно определять общие тенденции и закономерности киберпреступности для дальнейшего их изучения. Требуется организовать ведение статистических данных по разным видам киберпреступлений.

В-пятых, организовать разработку общей методики расследования киберпреступлений.

Можно предположить причины и условия распространения киберпреступлений:

1. Анонимность пользователей в сети Интернет.

В соответствии со стратегией национальной безопасности Российской Федерации, анонимность, которая возникает в связи с использованием информационных технологий, упрощает возможность совершения преступлений. В связи

с этим расширяется возможность легализации доходов, которые были получены преступным путем, упрощается возможность распространения наркотических средств и психотропных веществ.

2. Низкий уровень информационной защиты.

Некоторые сотрудники различных организаций в период пандемии вели свою рабочую деятельность на личных ноутбуках или компьютерах, которые имеют более слабый уровень защиты.

3. Финансовая неграмотность людей и техническая отсталость гражданских и правоохранительных органов. Недостаточный уровень знаний у сотрудников правил информационной безопасности.

4. Недостаточность финансирования обеспечения информационной безопасности.

5. Нехватка времени на оперативное принятие решений.

В период пандемии организациям пришлось в течение нескольких дней принимать решения по обеспечению своих сотрудников оборудованием и пересмотреть подходы к информационно безопасной организации труда.

В июле 2020 г. в пик пандемии генерал-майор ФСБ России Александр Михайлов высказался об необходимости создания киберполиции. По его мнению, необходимо иметь высококвалифицированных специалистов не только в юридическом поле, но и в IT-сфере, чтобы они были подготовлены именно для борьбы с преступностью в информационном пространстве. Развитие дистанционных мошенничеств, по его мнению, это следствие низкого уровня профилактической работы правоохранительных органов. Борьба и раскрываемость интернет-мошенничеств на сегодняшний день остается на крайне низком уровне.

Можно сделать вывод, что COVID-19 стал триггером процесса цифровизации общества, неким толчком, который ускоряет потребность использования цифровых технологий, что в итоге привело к неотвратимым процессам видоизменения преступности во всем мировом пространстве.

Список литературы

1. Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. 07.01.2002. № 1 (ч. 1). Ст. 1.

2. Комлев Ю. Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. № 2(1). С. 17–26.

3. Пандемия COVID-19 вызвала всплеск контрабанды поддельными лекарствами и товарами. URL: https://news.un.org/ru/story/2020/07/1381641

4. Россия вошла в топ-10 стран по цифровизации госуправления 2023. URL: https://digital.gov.ru/ru/events/42223

5. Уголовный кодекс Российской Федерации: от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

6. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_389271

7. Федеральная служба государственной статистики. URL: https://rosstat.gov.ru/folder/210/document/13204

8. Шеленина О. В. Цифровая преступность // Сборник научных статей 5-й Международной научной конференци. Курск: Юго-Западный государственный университет, 2022. С. 239–241.

9. Хисамова З. И., Бегишев И. Р. Цифровая преступность в условиях пандемии: основные тренды // Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 185–198. EDN GNPYZX.

10. Annual number of ransomware attempts worldwide from 2017 to 2022. URL: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide

11. Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023. URL: statista.com/statistics/204457/businesses-ransomware-attack-rate

А. А. Юсупова,
адъюнкт,
Казанский юридический институт
Министерства внутренних дел Российской Федерации

ВВЕДЕНИЕ QR-КОДОВ В ПЕРИОД ПАНДЕМИИ КАК ФАКТОР РАЗВИТИЯ ПРЕСТУПНОСТИ

Аннотация. В статье отмечается значимость использования цифровых технологий во всех сферах общества. На основе статистических данных и опросов респондентов исследуется влияние внедрения QR-кодов на изменение преступности, указываются отдельные виды преступлений в связи с введенными ограничительными мерами. Выявлены причины и недостатки введения QR-кодов.

Ключевые слова: QR-код, пандемия, преступность, взятка, фальсификация документов, мошенничество, злоупотребление служебными полномочиями, служебный подлог, нарушение санитарно-эпидемиологических правил, права и свободы человека

INTRODUCTION OF QR CODES DURING THE PANDEMIC AS A FACTOR IN THE DEVELOPMENT OF CRIME

Abstract. This article points out the importance of the use of digital technologies in all spheres of society. The influence of the introduction of QR codes on the change in crime is investigated, certain types of crimes are indicated in connection with the introduced restrictive measures. Surveys of respondents of the CORONAF project are being investigated. Statistical data of the Russian Ministry of Internal Affairs are given. The reasons and disadvantages of introducing QR codes are being studied. The types of subjects of the QR code are determined.

Keywords: QR code, pandemic, crime, bribery, falsification of documents, fraud, abuse of official authority, forgery, violation of sanitary and epidemiological rules, human rights and freedoms

Цифровое пространство – это реальность 21 века [5. С. 101]. Внедрение цифровых технологий оказало влияние не только на все сферы жизни человека, но и на правовую систему всего мира. Социальные и технологические инновации появляются в обществе в связи с развитием человечества. QR-код является той новацией, которая вторглась в правовое пространство в период пандемии. Государство для борьбы против коронавирусной инфекции, стало водить так называемые ковидные ограничения. Одним из средств обеспечения данной борьбы стала система QR-кодов.

QR-код, так называемый штрих код, создан в 1994 г. для маркирования автомобильных деталей. В связи с удобством и легкостью его использования он получил широкое распространение в большинстве сфер общественной жизни. В период пандемии многие страны применили данный инструмент для введения ограничительных мер.

Для начала стоит выяснить причину введения QR-кода в период пандемии. Это важно выделить для выявление самой сути его внедрения. Попробуем составить логическую цепочку введения данного ограничительного инструмента (рис. 1).

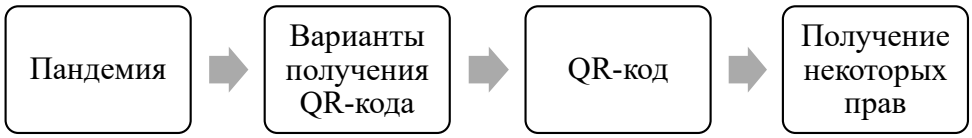


Рис. 1. Причина введения QR-кода

Согласно рис. 1, причиной введения QR-кодов стала сама коронавирусная инфекция. Пандемия – это вспышка инфекции глобального масштаба. То есть стоит учитывать массовость внедрения QR-кодов. Так, государство в целях защиты здоровья граждан в период пандемии принимает решение, что необходимо достигнуть коллективного иммунитета к коронавирусу. Коллективный иммунитет помог бы справиться с COVID-19. Многие государства проявили настойчивость и метод принуждения, так как вакцинация шла в самом начале своего пути медленными темпами и необходимо было принимать быстрые решения.

Стоит рассмотреть некоторые причины, почему люди отказывались от вакцинации, согласно исследованию центра социального проектирования. В ТОП-5 попали следующие ответы граждан: страх перед долгосрочными последствиями для здоровья; вакцинацию должны сделать больше людей, чтобы были понятны ее последствия; не верят в эффективность вакцинации; могут заболеть COVID-19 и с прививкой; не доверяют российским вакцинам [8].

Доверие граждан к власти, медицине, системе здравоохранения, науки, становится ключевым фактором принятия решения о вакцинации большей части населения [11]. Данное доверие к вакцинации пошатнулось, когда увеличилось количество

ложных публичных высказываний в сети Интернет против прививок, тем самым создавая угрозу общественному здоровью. Одной из проблем стало движение антипрививочников, которые осложнили борьбу с коронавирусной инфекцией. В соответствии со ст. 207.1 УК РФ публичное распространение заведомо ложной информации об обстоятельствах, которые представляют угрозу жизни и безопасности граждан, что наказывается уголовным законодательством.

По данным ГИАЦ МВД России, количество зарегистрированных преступлений, которые предусмотрены ст. 207.1 УК РФ, за 2020 г. – 36, в 2021 г. – 5, за 6 месяцев 2022 г. – 13.

Государству необходимо обратить вынимание на тему официального информирования граждан в период нестабильной санитарно-эпидемиологической обстановки.

Вернемся к теме QR-кодов. Так, согласно проекту Федерального закона № 17357–8 «О внесении изменений в Федеральный закон "О санитарно-эпидемиологическом благополучии населения"» [2], были предложения в части введения некоторых ограничительных мер по предотвращению распространения COVID-19. Согласно определению QR-кода в данном законопроекте, это двухмерный штриховой код. QR-коды, стали тем самым средством, ограничивающим свободное перемещение человека.

Совет Государственной Думы 17 января 2022 г. снял с рассмотрения данный законопроект. Но мы должны быть готовы к возникновению похожих пандемии в ближайшем будущем. Поэтому очень важно изучить все аспекты введенных инноваций в правовом пространстве.

Согласно рис. 2, мы разграничили виды субъектов QR-кодов в период пандемии. Дадим оценку каждому типу данной личности. Начнем с ПЦР-отрицательными, которые сделали тест на наличие инфекции у них в организме. Они являются самыми безопасными для окружающих из выше представленных. Далее разберем лиц, которые являются переболевшими и априори должны быть таковыми полностью, без каких-либо легких остаточных симптоматик. Процент безопасности для других окружающих высокий, но не стопроцентный. Отдельный вопрос возникает к лицам, которые вакцинировались, но есть вероятность что они могут заболеть в легкой форме, но при этом не знать этого. То есть нет полной гарантии того, что они не могут представлять опасность для окружающих. Далее рассмотрим лиц, имеющие противопоказания. Если смотреть с медицинской точки зрения, то данные лица в большинстве случаев в общем могут иметь проблемы со здоровьем и попадают в поле риска при возникновении каких-либо инфекций. Процент опасности для окружающих высокий. Так возникает вопрос, правильно ли разграничивать людей по данному принципу.

Рис. 2. Виды субъектов QR-кодов в период пандемии

Среди минусов введения QR-кодов можно выделить:

1. Само название QR-код носит в себе более «товарное» понятие. Штрих-коды как правило используются для учета и идентификация товаров. Употребление данного значения к человеку при проверке его личности является не совсем корректным.

2. Общественное вынуждение.

Так, согласно проведенному опросу респондентов проекта коронаФОМ, 12 % среди опрошенных сделали прививку под угрозой увольнения или отстранения от работы, 3 % из-за ограничения мест посещения, 2 % из-за ограничения выезда за границу [6].

В связи с затруднительным положением люди начали вынужденно подделывать сертификаты вакцинации, использовать QR-коды третьих лиц, а также незаконно приобретать и реализовывать данные документы. Любой из данных способов влечет ответственность согласно действующему законодательству [4. С. 357].

К поддельным документам можно отнести сертификат, который официально является подтверждением наличия у лица вакцинации. Если же гражданин с помощью поддельного сертификата, поехал за границу и массово заразил других людей, то его привлекут к ответственности по ст. 236 УК РФ «Нарушение санитарно-эпидемиологических правил».

Противоправные деяния, связанные в том числе с оформлением, выдачей сертификата и QR-кода, могут быть квалифицированы как должностные преступления, например дача взятки (ст. 291 УК РФ), злоупотребление служебными полномочиями (ст. 285 УК РФ), служебный подлог (ст. 292 УК РФ).

Также участились случаи продажи несуществующих QR-кодов при помощи сайтов однодневок в сети Интернет [7]. Мошенники хотят заработать на доверчивых гражданах, а люди готовы пойти на все существующие способы его приобретения. Данный пример попадает под статью 159 УК РФ «Мошенничество».

3. Вынужденное законодательное ограничение прав и свобод человека.

Так, согласно ч. 3 ст. 55 Конституции Российской Федерации, права и свободы человека могут быть ограничены федеральным законом только если это необходимо в целях защиты здоровья, прав и законных интересов других лиц. Во время пандемии COVID-19 были ограничены следующие права и свободы человека: на свободное передвижение (ст. 27 Конституции), на труд (ст. 37 Конституции), на обращение в государственные органы и органы местного самоуправления (ст. 33 Конституции), на отказ от профилактических прививок (п. 1 ст. 5 Федерального закона от 17.09.1998 № 157-ФЗ «Об иммунопрофилактике инфекционных болезней») и т. д.

Можно сделать вывод о том, что введение QR-кодов в период пандемии повлияло на развитие преступности. QR-код – это информационная инновация в правовом пространстве, которая была вынужденной мерой в период пандемии COVID-19. Необходимо провести еще больше исследований влияния пандемии на жизнь людей во всех сферах общества, в особенности в правовом пространстве. Впереди у человечества еще много различных смертоносных и опасных пандемий, которые потребуют использование текущего опыта нашего поколения.

Список литературы

1. Вакцинация: дефицит легитимности. URL: https://covid19.fom.ru/post/vakcinaciya-deficit-legitimnosti

2. Законопроект № 17357–8. URL: https://sozd.duma.gov.ru/bill/17357–8#bh_histras

3. Конституция Российской Федерации (принятая всенародным голосованием 12.12.1993) // Собрание законодательства РФ. 01.07.2020. № 31. Ст. 4398.

4. Макарычева О. С. Введение QR-кодов как фактор развития преступности // Ежегодная научно-практическая конференция: сборник трудов конференции. М.: Российский новый университет, 2022. С. 355–358.

5. Малышева, И. В. QR-код как новая правовая реальность // Русский закон. 2022. Т. 75, № 7(188). С. 100–107.

6. Об оборотной стороне принуждения к вакцинации. https://covid19.fom.ru/post/vakcinaciya-deficit-legitimnosti

7. Хисамова, З. И., Бегишев И. Р. Цифровая преступность в условиях пандемии: основные тренды // Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 185–198. EDN GNPYZX.

8. Россияне назвали причины отказа от вакцинации. URL: https://www.rbc.ru/society/29/06/2021

9. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

10. Федеральный закон РФ от 17.09.1998 № 157-ФЗ «Об иммунопрофилактике инфекционных болезней» // СПС «Гарант».

11. Психология вакцинации. URL: https://стопкоронавирус.рф/news/20210430–0900.html

СОДЕРЖАНИЕ | CONTENTS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM CRIMINAL LEGAL RELATIONS

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 2

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

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технический редакторы: *О. А. Аймурзаева, С. Р. Каримова*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0815-4

Подписано в печать 30.11.2023. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 18,37. Уч.-изд. л. 17,38.
Тираж 500 экз. (1-й завод – 30 экз.) Заказ № 97.

Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17