

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ТРИБУНА МОЛОДЫХ УЧЕНЫХ

Сборник научных статей

Выпуск 20

ЦИФРОВИЗАЦИЯ ОБЩЕСТВА
И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Воронеж
Издательский дом ВГУ
2024

УДК 340.1
ББК 67.0
Т67

Научный редактор –
доктор юридических наук, профессор *О. С. Рогачева*

Трибуна молодых ученых : сборник научных трудов.
Т67 Вып. 20 : Цифровизация общества и государственного
управления / под ред. О. С. Рогачевой ; Воронежский го-
сударственный университет. – Воронеж : Издательский
дом ВГУ, 2024. – 120 с.
ISBN 978-5-9273-4040-8

В сборник научных трудов вошли статьи студентов юри-
дического факультета Воронежского государственного уни-
верситета по материалам Международной студенческой на-
учно-практической конференции «Цифровизация общества и
государственного управления», посвященной 105-летию юби-
лею юридического факультета ВГУ.

Для студентов, аспирантов, преподавателей, а также науч-
ных работников и практикующих юристов.

УДК 340.1
ББК 67.0

ISBN 978-5-9273-4040-8

© Воронежский государственный
университет, 2024
© Оформление, оригинал-макет.
Издательский дом ВГУ, 2024

СОДЕРЖАНИЕ

Предисловие	5
Гельбанд Э. Е. Технология blockchain как средство противодействия коррупции	6
Глазунова Е. В. Перспективы и проблемы электронного голосования (на примере региональных и муниципальных выборов)	13
Гринев И. В. Проблемы электронного правосудия при рассмотрении вещно-правовых споров	19
Журавлева С. С. Сведения о способе вымогательства в социальных сетях как теоретическая основа планирования расследования и предупреждения преступления	25
Кирдяпкина В. Ф. Социальная обусловленность уголовно-правовой охраны интеллектуальной собственности и модернизация системы наказания за преступления против ее объектов в условиях цифровой экономики	33
Кожемяко И. А. Цифровизация и наблюдение за выборами: правовое регулирование и практика (на примере центров общественного наблюдения)	38
Курлянчик В. С. Практика применения электронных навигационных пломб в евразийском экономическом союзе.....	45
Малыхина В. В. Искусственный интеллект в цифровой трансформации права	51
Пономарева Л. А. Заключение и исполнение смарт-контрактов в современном гражданском праве.....	57
Попова В. П. Электронные ресурсы в системе государственного управления	63
Проценко Е. О. Реализация принципа гласности и открытости судебного разбирательства в условиях цифровизации административного судопроизводства	69
Садкеева Д. Д. Правовая охрана интеллектуальной собственности в сфере физической культуры и спорта	75
Сарычева А. С. Цифровые следы преступления	81

Сульдина Е. Д. Понятие и правовое регулирование кибертехнических преступлений в уголовном праве РФ	86
Трофимова М. Ю. Правовое регулирование договоров купли-продажи на маркетплейсах	94
Филипенко Н. А. Налогообложение криптовалют	100
Хорошенькова В. М. Электронный аукцион по предоставлению земельных участков, находящихся в публичной собственности	105
Чеботарев Д. А. Проблема соблюдения права человека на неприкосновенность частной жизни в эпоху цифровизации	110
Чернецова В. В. Уголовно-правовое регулирование информационной безопасности в условиях цифровизации	116

ПРЕДИСЛОВИЕ

25 ноября 2023 года состоялась **Международная студенческая научно-практическая конференция «Цифровизация общества и государственного управления»**, посвященная 105-летию юридического факультета Воронежского государственного университета и 60-летию деятельности Студенческого научного общества. Участниками конференции стали студенты не только юридического факультета ВГУ, но и других вузов России и Беларуси. Выступающие – представители различных отраслевых правовых наук – в своих докладах затронули разные аспекты цифровизации общества и государственного управления. Участники активно обсуждали поднятые докладчиками вопросы правового регулирования в условиях цифровой трансформации, новых направлений правопонимания и правоприменения. Конференция позволила начинающим ученым апробировать свои исследования, отточить навыки публичных выступлений, а всем присутствующим и интересующимся вопросами цифровизации дала новые темы для размышления и зарядила атмосферой научного поиска.

Хотелось бы пожелать студентам больше участвовать в конференциях, проявлять внимание к проблеме, которая стала для каждого предметом исследования; видеть соответствующий правовой институт в развитии, моделировать ситуацию в связи с законодательными нововведениями; внимательно отслеживать результаты правоприменения в соответствующей сфере правоотношений, творчески обобщать их и на этой основе разрабатывать предложения и рекомендации, аргументируя свои подходы новыми теоретическими суждениями и доводами.

*Доктор юридических наук,
заместитель декана по научной работе и аспирантуре
О. С. Рогачева*

Гельбанд Эмилия Исаевна

Воронежский государственный университет

ТЕХНОЛОГИЯ BLOCKCHAIN КАК СРЕДСТВО ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ

Gelband Emiliia Isaevna

Voronezh State University

BLOCKCHAIN TECHNOLOGY AS A MEANS ANTI-CORRUPTION MEASURES

Аннотация: цель исследования заключается в изучении технологии *blockchain*, вопроса ее внедрения и использования как инновационного средства в борьбе с коррупцией. В данной статье особое внимание уделяется механизму функционирования данной технологии, её преимуществам и недостаткам. Сделан вывод о перспективах использования технологии *blockchain* в России, которые являются весьма эффективными в процессе противодействия коррупции в условиях современной жизни.

Abstract: the purpose of the study is to study blockchain technology, the issue of its implementation and use as an innovative tool in the fight against corruption. In this article, special attention is paid to the mechanism of functioning of this technology, its advantages and disadvantages. The conclusion is made about the prospects of using blockchain technology in Russia, which are very effective in the process of countering corruption in modern life.

Ключевые слова: технология *blockchain*, коррупция, средства противодействия коррупции, перспективы.

Keywords: blockchain technology, corruption, anti-corruption tools, prospects.

Тема коррупции сегодня является одной из самых обсуждаемых в специальной и юридической литературе. В ежегодных посланиях Президента Российской Федерации Федеральному

Собранию Российской Федерации отмечается приоритетный характер противодействия коррупции и ее проявлениям; необходимость реализации данных мер распространяется на все уровни и направления государственного управления, начиная с совершенствования системы законодательства, деятельности правоохранительных и судебных органов¹. Однако в последнее время тенденции развития научно-технологического прогресса открывают новые горизонты в области криминалистической профилактики. Проблема современного состояния борьбы с коррупцией в РФ характеризуется не только недостаточностью разработки соответствующих правовых мер, но упущением организационных моментов эффективного противодействия. Диалектика прогресса подсказывает пути решения некоторых задач макроуровня, в том числе и возможный алгоритм искоренения коррупции. Речь идет о создании технологий, предотвращающих появление преступного намерения, позволяющих устранить причину криминального явления. Это блокчейн-системы.

Блокчейн – выдающаяся технология, способная в корне изменить принцип коммуникации и взаимодействия. Простой пример: принимая решение об инвестировании или сотрудничестве, не придется полагаться на заявления бизнеса о росте выручки и количестве вкладчиков. Достаточно будет прочитать это в истории транзакций.

Некоторые учёные отмечают, что блокчейн – главный технологический прорыв двадцать первого века и самый значимый рывок человечества после появления и распространения интернета по всему миру². Изучением блокчейн-технологий всерьез занялись на государственном уровне в РФ в 2016-2017 годах. Однако попытки предпринимаются крайне осторожно. На сегодняшний день криптовалюта в России регулируется федеральным законом от 31.07.2020 № 259-ФЗ, вступившим в силу с 01.01.2021. При этом проблемы, с которыми сталкиваются участники криптоиндустрии, указывают на массу пробелов в регулировании³.

Данные высокотехнологичные механизмы создаются не для борьбы с негативными преступными проявлениями, а в целях нового источника получения прибыли: на платформах-блокчейн в первую очередь существуют уже известные криптовалюты (биткоин, эфир, лайткоин и т.п.). Однако перспективы приме-

нения блокчейн-технологий более разнообразны, чем простое получение прибыли. В основе данной технологии лежит распределенная база данных общего пользования, состоящей из «цепочки блоков». Блокчейн не имеет центрального органа, поэтому транзакции проверяются всеми участниками системы⁴. Это позволяет упростить процедуру, гарантировать достоверность и избавиться от посредников. Данная технология позволяет нам пересылать деньги, документы и иные сведения безопасно и напрямую от человека к человеку, минуя банк, госорганы, аудиторов, страховые компании и нотариусов.

Для того чтобы точно понимать, как именно функционирует блокчейн и как данная система может помочь в борьбе с коррупцией, необходимо разобраться в механизме ее работы. Блоки представляют собой структурированную систему различных данных, непосредственно вводимых пользователями системы блокчейн. К таким данным относятся, например, сведения о транзакциях (под транзакцией может быть все, что может быть зашифровано, и это будет храниться в блоке), данные о сделках, соглашениях и контрактах и многое другое. Каждый блок имеет прямую связь с другим блоком, ранее введенным в базу, что и создает ту самую «цепочку»⁵. Эта связь определяется тем фактом, что для записи нового блока информация, содержащаяся в старом блоке, должна быть последовательно считана. Таким образом, каждый новый блок, который добавляется в общую базу, будет включать в себя весь материал цепочки, начиная с самого первого блока⁶.

У каждой блокчейн-платформы есть целевое использование. Основным принципом построения блокчейн-системы является децентрализация. Оценивая данное свойство с точки зрения профилактики коррупции – подобное начало функционирования обусловит невозможность предложить взятку за внесение изменений в реестр прав собственности, за подделку документов, поскольку субъект направленного действия не определен⁷. Вторым существенным плюсом рассматриваемой системы можно выделить ее надежность. Заложенные в основу работы системы блокчейн алгоритмы не позволят внести изменения, соответствующих данных, если они не будут соответствовать уже ранее внесенным. Проверка соответствия осуществляется путем

достижения консенсуса между каждым пользователем, поскольку, как уже упоминалось выше, все данные представляют собой единую цепочку. Третье преимущество системы блокчейн – прозрачность. Вся информация о валютных операциях, контрактах и других данных является публичной. Таким образом, каждый желающий может ознакомиться с активами и операциями пользователя в свободной форме, что, помимо прочего, позволяет отслеживать подозрительное поведение, действия и вычислять незаконные операции злоумышленников-коррупционеров⁸.

Субъект В. хочет перевести деньги субъекту Г. Для этого он вносит в систему блокчейн новый блок, который содержит хеш предыдущего блока и новый, присущий только ему. Так как технология блокчейн не имеет единого сервера, а поддерживает работу на основе большого количества персональных компьютеров пользователей, каждый уже существующий в общей цепочке блок вместе с новым отправляются всем участникам системы для проверки на соответствие друг другу и конечному результату. В случае если ошибок не будет выявлено, каждым участником новый блок будет добавлен в свой образец базы данных. После успешно пройденной проверки и осуществления вышеуказанных механизмов новый блок, вносимый субъектом В., может быть добавлен в «цепочку блоков», которая содержит информацию обо всех предыдущих транзакциях. Результатом будет служить успешный денежный перевод от субъекта В. субъекту Г. Соответственно, такая информация не будет внесена в общую базу, платеж не пройдет, а новый блок будет признан некорректным и неработающим. Итак, пока еще осторожно, но стоит обозначить, что блокчейн-платформа исключает возможность создания условий для появления коррупционных намерений⁹.

Кроме того, с точки зрения криминалистической профилактики на блокчейн-рельсах могут быть созданы цифровые идентификаторы личности, с помощью которых окажется возможным усовершенствовать привычные паспорта и иные документы, удостоверяющие личность, их аналогами. Их основным преимуществом перед бумажным носителем идентификационной криптоинформации станет невозможность подделки. Система блокчейн как эффективный способ борьбы с коррупцией может быть применима в России, однако для ее успешной реализации

необходимо учитывать особенности функционирования правовой системы нашего государства, тенденции распространения коррупции в определенных сферах экономики и государственного управления, а самое главное, наличие современных информационных технологий¹⁰.

Казалось бы, вот она – панацея от коррупции, но не все так просто. По мнению отдельных авторов, использование такой технологии на территории России затруднительно из-за наличия сложностей, возникающих с законодательным регулированием, а точнее отсутствием нормативного закрепления статуса блокчейн¹¹. Трудоемкость процесса внесения данных в блокчейн-реестры, а также возможные злоупотребления в системах блокчейн. Второй недостаток связан с внедрением блокчейн: на больших участках территории возможны перегрузки и сбой системы из-за масштаба использования этой технологии.

Следует отметить, что многие страны уже предпринимают попытки внедрения технологий распределенных регистров в жизнь государства. Например, в начале сентября 2020 года Министерство сотрудничества в области развития Дании опубликовало отчет, в котором блокчейн признан эффективным инструментом борьбы с коррупцией. Он обеспечивает усиленный надзор за предприятиями, правительствами и заинтересованными сторонами, тем самым обрывая многие коррупционные связи. Блокчейн-технологии определены как один из четырех способов борьбы с коррупцией. Таким образом, использование системы в противодействии коррупции набирает необходимые обороты в зарубежных странах: последовательно вводятся нормы правового регулирования данной технологии, разрабатываются соответствующие компьютерные программы¹².

В рамках решения задач борьбы с коррупцией в ходе модернизации действующей системы публичного управления технология блокчейн может быть использована на следующих направлениях: кардинальное переформатирование и оптимизация систем документооборота и оказания публичных услуг в рамках реализации концепции цифрового правительства, что позволит снизить коррупционные издержки населения и бизнеса, возникающие в результате стремления упростить и сократить время предоставления услуг и сведений; развитие избирательных тех-

нологий посредством внедрения систем электронного голосования в целях, с одной стороны, повышения достоверности результатов выборного процесса, с другой – пресечения различного рода фальсификаций и иных коррупционных проявлений; повышение надежности и прозрачности государственных закупок; упрощение и прозрачность управления государственным имуществом, в том числе процедур приватизации государственных активов; разработки прозрачных систем учёта и контроля реализации государственных программ, в том числе в части процедур принятия решений в ходе предоставления средств государственной поддержки в целях наиболее рационального распределения средств и недопущения различного рода злоупотреблений¹³.

¹ Послание Президента Российской Федерации Федеральному Собранию Российской Федерации: послание Президента Рос. Федерации Федеральному Собранию Рос. Федерации от апр. 2021 г.

² Афонасова М. А. Системная трансформация и блокчейн технологии в сфере государственного управления. Системный анализ в проектировании и управлении. Сб. науч. тр. XXII Международной научно-практической конференции. СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2018. С. 315-319.

³ Центральный Банк Российской Федерации: официальный сайт. – Москва. – URL: <http://www.cbr.ru> (дата обращения 08.12.2022).

⁴ Что такое блокчейн и почему эта технология вскоре изменит мир [Электронный ресурс]. Режим доступа: <https://www.gazeta.ru/tech/2016/02/01/8038769/blockchain.shtml/> (дата обращения: 08.12.2022)

⁵ Генкин А., Михеев А. Блокчейн: как это работает и что ждет нас завтра // Издательство Альпина, 2018. С. 20-22.

⁶ Матюшкина А.В. Блокчейн-платформа – нет повода для коррупции // Гуманитарные и политико-правовые исследования. 2018. №3 (3). С.36-44.

⁷ Соколова Т.Н., Волошин И.П., Петрунин И.А. Преимущества и недостатки технологии блокчейн // Экономическая безопасность и качество. 2019. №1 (34). С. 49-52.

⁸ Куликов, А.В. Современный способ борьбы с коррупцией – использование технологии блокчейн / А.В. Куликов, Д.А. Символокова // Известия ТулГУ. Экономические и юридические науки. – 2021. – № 4. – С. 36-42

⁹ Куликов А.С., Символокова Д.А. Современный способ борьбы с коррупцией – использование технологии Блокчейн // Известия Тульского государственного университета. Экономические и юридические науки. – 2021. – №4. – С. 36-42.

¹⁰ Блокчейн для борьбы с коррупцией в государственных закупках: доклад Всемирного экономического форума. Анतिकоррупционный центр НИУ

ВШЭ [Электронный ресурс] URL:https://anticor.hse.ru/main/news_page/blokcheyn_dlya_borby_s_korrupsiy_v_gosudarstvennyh_zakupkah_doklad_vsemirnogo_ekonomicheskogo_foruma (дата обращения: 08.12.2022).

¹¹ Соколова Т.Н., Волошин И.П., Петрунин И.А. Преимущества и недостатки технологии блокчейн // Экономическая безопасность и качество. 2019. №1 (34). С. 51.

¹² Как используют блокчейн. Министерство в Дании рассказало, как блокчейн победит коррупцию [Электронный ресурс]. URL: <https://www.tadviser.ru/index.php/-> (Blockchain) (дата обращения: 08.12.2022).

¹³ Халатенкова Е.Ю. Значение антикоррупционных интернет-проектов и пути их дальнейшего совершенствования // Сборник тезисов, докладов, статей международной интерактивной онлайн-конференции «Организационно-управленческие механизмы антикоррупционной деятельности (российский и зарубежный опыт)» / отв. ред. Р.А. Абрамов – Москва: ИД «Третьяковъ», 2013 г.

*Воронежский государственный
университет
Гельбанд Эмилия Исаевна
E-mail: emiliia.2017@yandex.ru*

*Voronezh State University
Gelband Emiliia Isaevna
E-mail: emiliia.2017@yandex.ru*

Глазунова Елизавета Викторовна

Воронежский государственный университет

**ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ ЭЛЕКТРОННОГО
ГОЛОСОВАНИЯ (НА ПРИМЕРЕ РЕГИОНАЛЬНЫХ
И МУНИЦИПАЛЬНЫХ ВЫБОРОВ)**

Glazunova Elizaveta Victorovna

Voronezh State University

**PROSPECTS AND PROBLEMS
OF ELECTRONIC VOTING (USING THE EXAMPLE
OF REGIONAL AND MUNICIPAL ELECTIONS)**

Аннотация: цель исследования заключается в изучении электронного голосования, которое представляет собой значительный шаг в цифровизации избирательного процесса и государственного управления в целом. В данной статье особое внимание уделяется перспективам развития данного явления, а также возможным проблемам, в процессе применения электронного голосования на выборах.

Abstract: the purpose of the study is to study electronic voting, which represents a significant step in the digitalization of the electoral process and public administration in general. In this article, special attention is paid to the prospects for the development of this phenomenon, as well as possible problems in the process of using electronic voting in elections.

Ключевые слова: дистанционное электронное голосование, выборы, избиратели, цифровизация, избирательный процесс.

Keywords: remote electronic voting, elections, voters, digitalization, electoral process.

Цифровизация – это процесс, который активно проникает во все сферы жизни современного человека. На данный момент мы даже представить не можем нашу жизнь без многих цифровых

технологий, которые буквально еще несколько лет назад не имели применения в мире. Это явление коснулось и избирательного процесса, которое породило новое электоральное явление – электронное голосование. Следует отметить, что внедрение данного элемента не было чем-то неожиданным или внезапным, это был вполне закономерный процесс, который обуславливался тем, что многие сферы жизни человека получают «электронный формат» и, как следствие, происходит цифровизация государственного и муниципального управления¹. В 2023 году дистанционное электронное голосование проводилось на территории 25 регионов РФ, что говорит о достаточно эффективной интеграции данного процесса в избирательную систему РФ.

Нужно понимать, что внедрение чего-то нового – это в определенной мере эксперимент, который может иметь как положительный результат, и тогда данное явление получит широкое распространение, так и отрицательный. С одной стороны, это хорошая основа для развития законодательства и в целом правовой системы РФ, которая открывает для нашей страны новые перспективы. С другой стороны, даже в случае положительного исхода, не стоит забывать о том, что существует масса нюансов, которые нужно будет учесть при реализации данного нововведения. Обычно при внедрении нового возникает множество проблем реализации данного процесса, так как он порождает определенные правовые последствия, и не всегда они могут быть решены удовлетворительно, а порой могут выливаться в серьезные нарушения законодательства.

Электронное голосование не является исключением. Это явление имеет как свои перспективы реализации, так и проблемы. Рассмотрим их на примере проведения дистанционного электронного голосования на муниципальных выборах, которое направлено на решение актуальных задач избирательного процесса, его совершенствование.

Одним из плюсов развития дистанционного электронного голосования является – повышение доступности процедуры голосования. Внедрение цифровых (электронных) технологий существенно повысило доступность государственных и муниципальных услуг, самих органов публичной власти для населения. Электронные обращения граждан, электронные покупки, элек-

тронные очереди, удалённая работа стали реальностью. Очевидно, что электронное голосование, в т. ч. дистанционное, – важная часть электронной реальности, цифровизации политической сферы. Учитывая протяжённость территории России и невысокую плотность населения, цифровизация голосования в форме электронного голосования необходима. Электронное голосование во многом решает эти проблемы. Кроме того, внедрение электронного голосования – настоящее спасение для людей, которые не могут покинуть свое место жительства или имеют определённые препятствия для этого, для людей, которые на момент голосования находятся не на территории муниципального образования или вовсе за пределами России. Таким образом, ДЭГ позволяет гражданам, выразит свое мнения по поставленному вопросу в случае, если у них отсутствует возможность лично прийти на избирательный участок и отдать свой голос, посредством чего повышается, как раз, и общая доступность к выборам².

Также внедрение цифровизации в избирательный процесс позволяет повысить процент общей привлекательности выборов, доверия к ним и явки избирателей. По результатам опроса Всероссийского центра изучения общественного мнения уровень доверия граждан к проведению выборов достаточно вырос. На 2020 год процент тех, кто доверял составлял 61%, а вот на 2023 года этот процент вырос до 69%.

Если граждане не доверяют выборам, не участвуют в них, что особенно характерно для муниципальных выборов, возникает вопрос, можем мы ли мы говорить о подлинности народовластия в данном муниципальном образовании, и, как следствие, под вопрос ставится уровень развития местного самоуправления и процент участия в нем граждан. Также возникает и проблема легитимности власти кандидатов и партий, победивших на выборах. Электронное голосование должно не просто сделать выборы удобнее для граждан, оно должно способствовать подлинному народовластию, вовлечённости большинства в принятие решений на государственном и муниципальном уровнях, прежде всего, в вопросе о том, кто будет управлять публичными делами и представлять интересы населения, поэтому весьма желательно повышение явки избирателей на выборах. В России на муниципальных выборах явка низкая не только в труднодо-

ступных местностях, но и в мегаполисах. Использование информационных технологий голосования привлечёт к выборам жителей городов, прежде всего молодого и среднего возраста. Так, в 2018 году явка на выборы мэра в городе Москва составила 30,9%, а вот уже 2023 процент участия граждан составил 42,5%. Данный случай, как раз таки, является одним из ярких примеров повышения общей привлекательности выборов, а также доверия к ним. Конечно, и в этом случае, мы не можем говорить о полном, абсолютном доверии со стороны граждан, но видя повышение процента явки избирателей, можно сделать вывод, что сами граждане хотят больше доверять государству, хотят участвовать в его жизни и жизни своего народа.

Следующим положительным моментом можно отметить удешевление процедуры выборов. Для муниципальных бюджетов любая экономия будет желательной, учитывая глобальную нестабильность в экономике. Разумеется, экономия не может вести к снижению качества или прозрачности выборов. Сам ЦИК РФ отмечает, что электронное дистанционное голосование ведёт и к усилению гарантий реализации избирателями своих прав, и даёт значительную экономию денежных ресурсов.

Если говорить о проблемах, которые связаны с проведением ДЭГ, то в первую очередь к ним можно отнести возможность утечки конфиденциальной информации граждан, посредством взлома информационной платформы. Киберпреступления с развитием информационных технологий, все больше стали проникать в нашу жизнь. Постепенно появляются новые виды преступлений в сфере компьютерной безопасности, которые как раз и ставят под угрозу конфиденциальность выборов и степень защищенности личных данных граждан³.

С целью защиты избирательных прав граждан необходимо модернизировать механизмы административной и уголовной ответственности применительно к дистанционному электронному голосованию. Действительно, одним из серьёзнейших факторов, которые необходимо учитывать при разработке мер ответственности, является усиление противодействия как фальсификации волеизъявления избирателей, так и оказания давления на избирателя, в т. ч. и косвенного. Так, недопустимость предвыборной

агитации в Интернете в «день тишины» или непосредственно в день голосования декларируется, но сложно обеспечивается⁴.

Таким образом, можно уяснить, что дистанционное электронное голосование всерьёз и надолго вошли в муниципальный и региональный избирательные процессы России. Электронное голосование на данных выборах стало технически более совершенным, чем было ранее, но проблема доверия избирателей к дистанционному электронному голосованию сохраняется.

К основным задачам развития дистанционного электронного голосования в муниципальном избирательном процессе, которые в настоящее время остаются и основными проблемами, можно отнести: повышение и сохранение тайности дистанционного электронного голосования, обеспечение подлинности волеизъявления гражданами своего мнения⁵.

Для решения названных задач необходимо всестороннее обеспечение безопасности механизма дистанционного электронного голосования как от попыток вмешательства неопределённого круга лиц с преступным умыслом, так и от злоупотреблений со стороны должностных лиц органов публичной власти. Для решения данной проблемы, необходимо совершенствование административного и уголовного законодательства. Вместе с тем наличие проблем должно вести не к отказу от самой технологии, а к её совершенствованию.

¹ Авакьян С. А. Информационное пространство знаний, цифровой мир и конституционное право // Конституционное и муниципальное право. - 2019. № 7. – С. 23-28.

² Григорьев А. В. Правовое регулирование электронного дистанционного голосования: перспективы развития // Вестник Московского университета. Серия 26. Государственный аудит. – 2018. № 3. – С. 118-131.

³ Котикова Д. В. К проблеме правового регулирования дистанционного электронного голосования // Гражданин. Выборы. Власть. – 2020. № 2. – С. 174-184.

⁴ Чертков А. Н. Риски электронного голосования (Перспективы защиты избирательных прав граждан вызывают обеспокоенность) [Электронный ресурс] // Адвокатская газета. URL: [https:// www.advgazeta.ru/mneniya/riski-elektronnogo-golosovaniya](https://www.advgazeta.ru/mneniya/riski-elektronnogo-golosovaniya) (дата обращения: 03.06.2021).

⁵ Федоров В. И. Проекты по автоматизации голосования в исторической ретроспективе // Гражданин. Выборы. Власть. – 2020. № 1. – С. 34-55.

Воронежский государственный
университет
Глазунова Елизавета Викторовна
E-mail: glazunovaliza04@gmail.com

Voronezh State University
Glazunova Elizaveta Victorovna
E-mail: glazunovaliza04@gmail.com

Гринев Илья Владимирович

Воронежский государственный университет

**ПРОБЛЕМЫ ЭЛЕКТРОННОГО ПРАВОСУДИЯ
ПРИ РАССМОТРЕНИИ ВЕЩНО-ПРАВОВЫХ СПОРОВ**

Grinev Ilya Vladimirovich

Voronezh State University

**PROBLEMS OF ELECTRONIC JUSTICE
IN THE CONSIDERATION OF PROPERTY DISPUTES
IN THE FRAMEWORK OF CIVIL PROCEEDINGS**

Аннотация: в статье рассматриваются вопросы исследования и оценки судами электронных средств доказывания. Дается оценка общедоступным картографическим сервисам типа «Яндекс.Карты» как важного доказательства в вещно-правовых спорах. Анализируются потенциальные риски получения доказательственной информации из информационно-телекоммуникационной сети «Интернет» которые связаны с их легко изменяемым характером.

Abstract: the article deals with the issues of research and evaluation by courts of electronic means of evidence. The assessment of publicly available cartographic services such as Yandex.Maps as an important evidence in property disputes is given. The potential risks of obtaining evidentiary information from the information and telecommunications network "Internet" are analyzed, which are associated with their easily changeable nature.

Ключевые слова: гражданское судопроизводство, электронные доказательства, общедоступные сведения.

Keywords: civil proceedings, electronic evidence, publicly available information.

«Абсолютно очевидно, что применение «цифры» в судопроизводстве будет только расширяться, и наша судебная система должна быть к этому полностью готова – и технически, и орга-

низационно, а главное, чтобы при этом неукоснительно соблюдались конституционные права граждан" – заявил Президент РФ Владимир Путин в начале 2023 года в рамках ежегодного совещания судей Российской Федерации.

Система электронного правосудия в Российской Федерации – это комплекс информационных технологий и электронных сервисов, который внедряется для автоматизации и повышения эффективности процессов судопроизводства. Он включает в себя различные электронные сервисы, такие как электронное делопроизводство, электронная подача документов и жалоб, электронное распространение судебных решений и другие инструменты, которые позволяют сделать работу судебных органов более эффективной, прозрачной и удобной для граждан и юридических лиц. Уже существует достаточно большой массив сервисов, выполняющих данную работу (ГАС «Правосудие», автоматизированная информационная система Верховного Суда РФ, система «Мой арбитр», КИС СОЮ, АИС «Мировые судьи»), а также планируется ввести в действие новые технологии, например суперсервис «Правосудие онлайн», технические возможности которого должны вывести электронное правосудие на новый уровень. Однако же, введение нового сервиса нацелено на решение разного рода проблем, связанных как с устареванием внедренных много лет назад технологий электронного судопроизводства, так и с развитием общественных отношений и потребностей современного гражданского общества в быстром и качественном правосудии.

В частности, Анатолий Наквас, Председатель Верховного суда Республики Карелия отмечает следующие тенденции: «Помимо традиционных форм доступа к правосудию в настоящее время развивается и электронный вид доступа. Это электронный документооборот, это возможность обратиться в суд не через бумажные носители, а через Госуслуги посредством электронного обращения, предоставления электронного искового заявления».

Частыми причинами отклонения электронных обращений в суды становятся неверная адресация или дублирование ранее направленных документов, плохая читаемость сканов, неправильный формат прикрепленных файлов и так далее. Как видно, в условиях цифровизации общества в судебной практике все

чаще стало встречаться использование в качестве средства доказывания электронных доказательств, с чем и связано множество проблем.

Законодатель на данный момент времени всё ещё не успел создать чёткое определение для этого крайне распространенного явления, в связи с чем, в доктрине и судебной практике существуют разные подходы к данной категории доказательств: восприятие их как письменных, как вещественных доказательств, а также как самостоятельного класса средств доказывания. Важно отметить, что стоит различать цифровую форму доказательства и электронное доказательство. Первое имеет оригинал на материальном носителе и по своей сути является цифровой копией, а второе существует исключительно в электронном формате, то есть в формате двоичного кода. Если электронное доказательство переносится на бумажный носитель (распечатка скриншота), оно теряет, по мнению многих учёных, режим электронного¹.

В последние годы в практике судов общей юрисдикции и арбитражных судов начали активно применяться сведения, получаемые из открытых информационных источников, ярким представителем которого является сервис «Яндекс.Карты». Быстрота и удобность получения информации о местоположении земельного участка, объектов на земной поверхности, проходящих границ соседних участков заметно упрощает судебный процесс. Если раньше некоторые суды ссылались на то, что доказательства, полученные из этих источников невозможно проверить на достоверность в связи с отсутствием необходимых государственных органов, на которые возложена данная обязанность, то сейчас отрицательные решения стали редкостью. Также большое число исследователей всё чаще отмечают, что и в арбитражном процессе открытые картографические сервисы играют важную роль в процессе доказывания. Так, например, активно используются панорамные снимки с «Яндекс.Карты» и «Гугл.карты» в качестве доказательств при установлении присутствия объекта на конкретной территории, в том числе периода такого присутствия². При этом отмечается, что суды предпочитают использовать именно картографические сервисы, пренебрегая «живым» посещением спорных объектов. В рамках ст. 89 АПК РФ³ данные сведения относятся к «иным документам и материалам».

Однако же, с нашей точки зрения, проводить более тщательную верификацию подобных документов крайне необходимо, ведь они касаются индивидуально-определенных предметов материального мира, для работы с которыми крайне важно иметь точное представление об их форме и местоположении. Во-первых, нужно обратить внимание на ст. 67 ГПК РФ⁴, суд не может считать доказанными обстоятельства, подтверждаемые только копией документа или иного письменного доказательства. В большинстве известных примеров суду предоставляются копии и распечатка скриншотов, что, по нашему мнению, не является должной формой подобных сведений, так как их «оригинал» находится в цифровой форме и подвержен постоянному обновлению. Подобные документы необходимо принимать лишь в электронной форме через официальные государственные сервисы в установленном законом порядке. При этом обязательна цифровая ссылка на источник.

Во-вторых, как отмечает Г.В. Савенко, перед судом необходимо доказать допустимость использования картографических изображений, спутниковых снимков, особенно в делах о причинении вреда участкам, о самовольном занятии части участков, о создании препятствий для собственников. Расхождение с реальным объектом может составлять более десятков метров, что является критической величиной, так как средняя квадратическая погрешность местоположения характерных точек земельных участков, отнесенные к землям сельскохозяйственного назначения и предоставленные для ведения личного подсобного, огородничества, садоводства, индивидуального гаражного или индивидуального жилищного строительства, составляет 0,20 м, земельных участков, отнесенных к землям сельскохозяйственного назначения и не входящих в предыдущую группу – 2,5 м; земельных участков, отнесенных к землям населенных пунктов – 0,10 м⁵.

В-третьих, представляется сомнительным также система исправления неточностей и ошибок, система добавления объектов на данные карты. Так, любой пользователь может добавить дополнительную дорогу, проезд к спорному земельному участку, изменить границы участка, либо же «построить» новое здание там, где его в реальности не существовало⁶. Система модерации, которая используется компанией «Яндекс», не всегда способна

противодействовать намеренному искажению информации на картах. Так, например, постоянно появляются «фейковые» объекты, принадлежащие различным реальным организациям, возникшие «клоны» организаций и их собственности⁷.

Таким образом, представляется необходимым в процессе развития цифрового судопроизводства сформулировать более строгие требования к картографическим и иным данным, получаемым из общедоступных сервисов, так как современные информационные источники являются интерактивными и более сложными по своему составу, требующими не менее профессиональной оценки, чем классические письменные и вещественные. Необходимо установить обязательный порядок для онлайн оценки предоставляемых в суд доказательств из таких общедоступных сервисов, как «Яндекс.Карты», потому что сведения из данного источника сегодня играют важную роль при рассмотрении вещных споров. Данные доказательства должны предоставляться в судебный орган вместе с активной ссылкой на ресурс в сети «Интернет», иметь в своём комплекте сведения из других открытых источников, для обеспечения быстрого сравнительного анализа, в том числе сведения из Публичной кадастровой карты.

Электронные доказательства теряют ряд своих свойств, если представлять их в суд исключительно на бумажных носителях в форме распечатанных копий. Проверка достоверности сведений, содержащихся в данном и подобных сервисах необходимо осуществлять в рамках специальных сервисов электронного правосудия. В рамках подготовки к запуску суперсервиса «Правосудие онлайн» было бы верным решением подключить собственную версию публичной кадастровой карты к этой системе, что позволило бы судам не тратить время и ресурсы для проверки сведения из открытых картографических источников в сети «Интернет».

¹ Власова С.А. Электронные доказательства как часть информационных технологий в гражданском судопроизводстве // *Ius publicum et privatum*. 2019. № 3(5). С. 15-18.

² Шкурова П.Д. Использование сведений, полученных из сервисов Google Maps и «Яндекс.Карты», в качестве доказательств в практике арбитражных судов Российской Федерации // *Сибирское юридическое обозрение*. 2021. № 18(1). С. 83-91.

³ Арбитражный процессуальный кодекс Российской Федерации [Электронный ресурс] // СПС КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_37800/ (дата обращения: 28.11.2023).

⁴ Гражданский процессуальный кодекс Российской Федерации [Электронный ресурс] // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_39570/ (дата обращения: 28.11.2023).

⁵ Приказ Федеральной службы государственной регистрации, кадастра и картографии от 23 октября 2020 г. № П/0393 «Об утверждении требований к точности и методам определения координат характерных точек границ земельного участка, требований к точности и методам определения координат характерных точек контура здания, сооружения или объекта незавершенного строительства на земельном участке, а также требований к определению площади зданий, сооружения, помещения, машино-места» [Электронный ресурс] // Гарант.ру (информационно-правовой портал). URL: <https://www.garant.ru/products/ipo/prime/doc/74812016/> (дата обращения: 28.11.2023).

⁶ Яндекс Справка: Добавление информации [Электронный ресурс] // URL: <https://yandex.ru/support/m-maps/add-info.html#organization> (дата обращения: 28.11.2023).

⁷ Поддельные отели-дубли организаций на Яндекс Картах [Электронный ресурс] // ДАО и Я. Личный блог. URL: <https://dao-and-i.ru/promotion/poddelnye-oteli-dubli-organizacij-na-yandeks-kartax.html#servis> (дата обращения: 28.11.2023).

*Воронежский государственный
университет
Гринеv Илья Владимирович
E-mail: vova.grnv@yandex.ru*

*Voronezh State University
Grinev Ilya Vladimirovich
E-mail: vova.grnv@yandex.ru*

Журавлева Софья Сергеевна

Краснодарский университет МВД России

**СВЕДЕНИЯ О СПОСОБЕ ВЫМОГАТЕЛЬСТВА
В СОЦИАЛЬНЫХ СЕТЯХ КАК ТЕОРЕТИЧЕСКАЯ
ОСНОВА ПЛАНИРОВАНИЯ РАССЛЕДОВАНИЯ
И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЯ**

Zhuravleva Sofya Sergeevna

Krasnodar University of the Ministry of Internal Affairs of Russia

**INFORMATION ABOUT THE METHOD OF EXTORTION
IN SOCIAL NETWORKS AS A THEORETICAL BASIS
FOR PLANNING AN INVESTIGATION AND
PREVENTION OF CRIME**

Аннотация: в статье рассмотрен способ вымогательства в социальных сетях как основа планирования и предупреждения преступлений, освещены основные виды кибервымогательства. Автор акцентирует внимание на способах, которые используются кибервымогателями в социальной сети. Сформулирован вывод о том, какие направления предупредительной деятельности имеют место в данной области.

Abstract: the article considers the method of extortion in social networks as a basis for planning and preventing crimes, highlights the main types of cyber extortion. The author focuses on the methods used by cybercriminals in the social network. The conclusion is formulated about which areas of preventive activity have a place in this area.

Ключевые слова: кибервымогательство, расследование, виды современного вымогательства, способы вымогательства в социальной сети, предупреждение вымогательства в социальной сети.

Keywords: cyber extortion, investigation, types of modern extortion, methods of extortion in a social network, prevention of extortion in a social network.

История развития информационных технологий неразрывно связана с компьютерной сетью ARPANET, разработанной в 1969 году в США, которая была предназначена для передачи информации на случай войны, а именно отправки сообщений. На сегодняшний день ARPANET считают не только прародительницей Интернета, но и прототипом первых социальных сетей. С широким распространением IT-технологий в цифровом мире наблюдается тревожный рост числа случаев так называемых кибервымогательств. Виртуальное пространство сегодня становится все более криминогенным. Одной из новейших разновидностей хакерских атак является компьютерное вымогательство¹. Кибервымогательства по способу передачи требования может быть разделено на три группы:

- Вымогательства с использованием DDoS-атак;
- Вымогательства с использованием «программ-вымогателей»;
- Вымогательства в социальных сетях.

Социальные сети выступают неотъемлемой частью современного общества, объединяя миллиарды пользователей по всему миру. К сожалению, повсеместный характер этих платформ также привлек внимание злоумышленников, стремящихся использовать ничего не подозревающих людей для получения финансовой выгоды. Социальные сети сейчас служат отнюдь не только элементом коммуникации, но и являются «ареалом» значительного количества интернет-мошенников, вымогателей. Вымогательство в социальных сетях стало распространенным видом киберпреступности, создающим угрозы репутации, конфиденциальности и финансовому благополучию пользователей.

Вымогатели в сети стремятся получить доступ к хранящимся на личных страницах пользователей социальных сетей сведениям о личной жизни жертвы, после чего начинают ее шантажировать распространением дискредитирующей и порочащей репутацию информации. Примером тому может служить ситуация, сложившаяся в Пермском крае. Соликамским городским судом Пермского края виновным был признан гражданин Ш., который, реализуя свой преступный умысел, вступил в переписку в социальной сети с Ч., после чего получил от нее фотографию интимного характера, а затем выдвинул требование о передачи денежного вознаграждения. Схожая ситуация возникла и в Иркутской

области². Усольский городской суд Иркутской области признал виновной гражданку Н., которая также выдвинула посредством использования социальной сети («Одноклассники») требование гражданке Б. об отправке на свою банковскую карту денежных средств взамен на отказ от распространения имеющихся у нее видеозаписей с обнаженной Б³.

Эффективность процесса расследования любого преступления, в том числе и вымогательства, зависит от обладания следователем знаниями относительно механизма совершения преступления. Одним из основных элементов механизма преступления является способ совершения преступления, знание которого необходимо для планирования действий по сбору криминалистически значимых следов преступления, определения отдельных особенностей личности преступника. Такая криминалистическая информация, в том числе, может быть положена и в основу формирования мер, направленных на предупреждение преступлений. Рассмотрим более детально способ реализации вымогательства, совершаемых в социальных сетях.

Под вымогательством понимают требование передачи имущества или права на него под угрозами:

- применения насилия;
- уничтожения или повреждения чужого имущества;
- распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких⁴.

В социальной сети преступниками чаще используется именно *угроза о распространении* определенного рода сведений. При этом стоит отметить, что обычно вымогатели в социальной сети заведомо не знакомы с жертвой, то есть не владеют необходимой информацией о ее личной жизни. Поэтому, как правило, ими используются сведения, подбираемые произвольно и не имеющие связи с личностью отдельного человека, следовательно, и потерпевшие – случайные лица. Для шантажа вымогатели в социальной сети используют различные способы:

1. «Выдача себя за другое лицо». Злоумышленники создают поддельные профили или взламывают аккаунты существующих людей, а затем выдают себя за знакомых, обманом заставляя

вступать жертву в компрометирующее взаимодействие. Используя это доверие, они собирают конфиденциальную информацию: видео, документы или изображения, чтобы использовать их в целях дальнейшего вымогательства. Вымогатели не только отправляют текстовые сообщения от имени другого человека, но и поддельные голосовые сообщения, что устанавливает наиболее прочный контакт с жертвой.

2. «Сексторция» (Sextortion). Сексторция (иначе сексуальное вымогательство) – новый термин, обозначающий вымогательство с использованием материалов сексуального характера. Обычно такое вымогательство начинается с обращения злоумышленника к жертве через платформы социальных сетей. Далее, как только устанавливается определенный уровень доверия, эмоциональной связи, преступник, вступая в откровенный разговор с потенциальным потерпевшим, принуждает его отправлять интимные изображения или видео. Впоследствии злоумышленник угрожает распространением имеющегося откровенного контента, если выдвинутые им требования не будут выполнены. Зачастую эти требования включают в себя выплату выкупа, отправку более откровенных материалов или совершение иных дискредитирующих действий. Если подобного рода контент станет общественным достоянием, жертвы имеют риск пострадать от испорченных отношений со знакомыми, потерять работу, а потому становятся более уязвимыми и продолжают выполнять требования вымогателя на протяжении долгого времени.

3. «Атака на бренд и репутацию». Предприятия и общественные деятели также не застрахованы от вымогательства в социальных сетях и могут выступать потерпевшей стороной. Злоумышленники могут распространять порочащую информацию или ложные слухи, угрожая запятнать репутацию организаций. Вымогателей в сети в данном случае интересует финансовая компенсация, которую они требуют от медийных личностей, популярных организаций взамен на неразглашение порочащей их репутацию информации.

Основной целью интернет-вымогателей в социальных сетях является финансовая выгода, что не отличает традиционное вымогательство от кибервымогательства. Цель вымогательства в социальных сетях – корыстная. Преступники требуют выплаты

выкупа в различных формах, таких как: использование данных банковских карт или онлайн-переводов, а также криптовалютных транзакций.

Весьма остро перед правоохранительными органами в настоящее время стоит и вопрос профилактики данной категории преступлений. На наш взгляд, профилактика вымогательства в социальных сетях должна включать в себя упреждающие меры и методы цифрового расследования, направленные не только на выявление самого преступления, но и на сдерживание и смягчение потенциальных угроз до того, как они перерастут в оконченное преступление.

Стратегии предотвращения вымогательства в социальной сети могут включать в себя несколько направлений профилактической деятельности:

1. *Обучение (информирование) пользователей.* Данная стратегия позволит повысить осведомленность граждан о новых видах преступности, в частности о вымогательстве в социальных сетях, а также о способах, используемых при реализации своих замыслов преступниками. Информирование пользователей социальной сети важный элемент, который должен проводиться в рамках профилактики киберпреступности, которая зачастую берет начало от привычных составов вымогательства, мошенничества и так далее, но имеет существенное отличие – базируется не в реальном мире, а в виртуальном. Данное отличие вызывает рост преступности, в первую очередь вследствие неосведомленности пользователей, следовательно, увеличивает и поток уголовных дел правоохранительным органам. Пользователям социальных сетей при взаимодействии онлайн необходимо соблюдать главное правило – правило осторожности и помнить, что любой материал, попадающий в руки злоумышленников, способен в будущем стать почвой для шантажа. Если внимательно относиться к знакомствам в сети, не делиться личной информацией, ставить под сомнение каждое предложение незнакомого собеседника, то возможно с большей долей вероятности удастся предотвратить взлом аккаунта и вымогательство в интернет-пространстве⁵.

Трансляция по телевидению или в онлайн-режиме (рекламные блоки в лентах социальных сетей) примеров безопасного поведения в социальной сети позволит пользователям с большей

вероятностью распознать подозрительные действия злоумышленников, а также сформирует знание об алгоритмах поведения в той или иной ситуации. Как результат, значительно уменьшается риск стать жертвой вымогателя в социальной сети.

2. *Настройки конфиденциальности.* В любых социальных сетях на сегодняшний день пользователь может перейти в раздел безопасности и установить так называемую двухфакторную аутентификацию. Она является вторым уровнем защиты аккаунта и личных данных, расположенных в профиле социальной сети. Так, если злоумышленники подобрали пароль к вашей странице в социальной сети, при включенной двухфакторной аутентификации им не удастся войти в профиль, поскольку система запросит код-подтверждения, отправленный, к примеру, на номер вашего мобильного телефона или электронную почту. Конечно, в век современных технологий, сложно сказать, что двухфакторная аутентификация – гарантированная защита ваших данных, но с уверенностью можно заявить, что именно она дополнительный уровень защиты, а иногда сигнал, позволяющий пользователю понять, что его социальная сеть прямо сейчас в руках у злоумышленников и ему стоит сменить пароль. Таким образом, на сегодняшний день социальные сети должны применять надежные механизмы аутентификации и настройки конфиденциальности, чтобы свести к минимуму риск несанкционированного доступа к учетным записям пользователей.

3. *Политика социальных сетей.* На наш взгляд была бы интересной политика быстрого удаления контента или блокирования профиля при несанкционированном входе с другого устройства, неразрешенного ранее пользователем-владельцем аккаунта. В таком случае была бы возможность уменьшить распространение вредоносных и компрометирующих материалов пользователей, размещенных в социальной сети.

4. *Развитие криминалистических инструментов и возможностей.* Анализ данные о личности интернет-вымогателей, их социально-демографической характеристике, могут быть положены в основу разработки *криминалистического портрета* вымогателя в социальной сети. Данный портрет должен содержать в себе особенности личности злоумышленника, те его характерные черты, манеры поведения, знания и навыки, по ко-

торым он может быть узнаваем. Подобная информация может быть использована на первоначальном этапе расследования для сужения круга подозреваемых, выдвижения версий о личности преступника.

5. *Разработка и внедрение методических рекомендаций по предупреждению, выявлению, раскрытию и расследованию подобных преступлений.* Основной криминалистической мерой предупреждения кибервымогательства в частности и киберпреступности в целом будет выступать разработка, а также внедрение в повседневную деятельность органов внутренних дел соответствующих методических рекомендаций.

6. *Предиктивная профилактическая деятельность ОВД.* Анализ типичного механизма совершения вымогательств в социальных сетях позволяет прогнозировать преступную деятельность, упреждать ее, эффективно расследовать. Сотрудники правоохранительных органов, понимая цели, мотивы, способы реализации преступления, обладая знаниями об особенностях тактики расследования отдельных видов вымогательств с учетом ситуационного подхода, способны принимать своевременные и эффективные меры по выявлению, расследованию и предотвращению вымогательств в социальных сетях.

Таким образом, вымогательство в социальных сетях представляет собой многогранную проблему для пользователей, различных организаций и общества в целом. Понимая тактику и цели кибервымогателей, заинтересованные стороны могут работать сообща над созданием более безопасной цифровой среды. Сочетание *эффективной работы* правоохранителей, причем не только относительно расследования уголовных дел, но и относительно их профилактической деятельности, и *обучения пользователей* сети имеет решающее значение для смягчения последствий вымогательства в социальных сетях, снижения уровня совершения таких преступлений.

¹ Лопатина Татьяна Михайловна Условноцифровое вымогательство, или кибершантаж // Журнал российского права. 2015. №1 (217). URL: <https://cyberleninka.ru/article/n/uslovnotsifrovoye-vymogatelstvo-ili-kibershantazh> (дата обращения: 19.10.2023).

² Приговор Соликамского городского суда Пермского края №1-134/2018 от 28 мая 2018 г. (<https://sudact.ru/regular/doc/Ryd0STKiCLO/>) (дата обращения: 21.10.2023)

³ Приговор Усольского городского суда Иркутской области №1-335/2019 от 13 июня 2019 г. (<https://sudact.ru/regular/doc/GysbQmNQhIJh/>) (дата обращения: 21.10.2023)

⁴ Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 10.07.2023) <https://base.garant.ru/10108000/>

⁵ Турутина, Е. Э. Интернет-вымогательство как проблема информационного общества / Е. Э. Турутина // Ученые записки Казанского филиала "Российского государственного университета правосудия". – 2021. – Вып. 17. – С. 391-395. – EDN PZRCYN. (дата обращения: 22.10.2023)

*Краснодарский университет МВД
России
Журавлева Софья Сергеевна
E-mail: zhuravlenochek02@mail.ru*

*Krasnodar University of the Ministry
of Internal Affairs of Russia
Zhuravleva Sofya Sergeevna
E-mail: zhuravlenochek02@mail.ru*

Кирдяпкина Валерия Федоровна

Саратовская государственная юридическая академия

**СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ
УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
И МОДЕРНИЗАЦИЯ СИСТЕМЫ НАКАЗАНИЯ
ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ ЕЕ ОБЪЕКТОВ
В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ**

Kirdyapkina Valeria Fedorovna

Saratov State Law Academy

**SOCIAL CONDITIONALITY OF CRIMINAL
LAW PROTECTION OF INTELLECTUAL PROPERTY
AND MODERNIZATION OF THE PUNISHMENT
SYSTEM FOR CRIMES AGAINST ITS OBJECTS
IN THE DIGITAL ECONOMY**

Аннотация: в статье рассмотрена актуальность и роль интеллектуальной собственности в условиях развития цифровой экономики. Авторами рассмотрена динамика преступлений против интеллектуальной собственности, дана основная характеристика системе наказаний уголовного законодательства. В завершение, сформулированы меры модернизации состава преступлений против объектов интеллектуальной собственности.

Abstract: the article examines the relevance and role of intellectual property in the context of the development of the digital economy. The authors consider the dynamics of crimes against intellectual property, and give the main characteristic of the penal system of criminal legislation. In conclusion, measures have been formulated to modernize the corpus delicti against intellectual property objects.

Ключевые слова: интеллектуальная собственность, преступление, санкция, цифровизация, социальная обусловленность.

Keywords: *intellectual property, crime, sanction, digitalization, social conditioning.*

В условиях развития цифровой экономики возрастает роль уголовно-правовой охраны интеллектуальной собственности. Научно-технический прогресс во многом создает благоприятную почву для кражи и незаконного использования результатов интеллектуальной деятельности, поэтому актуальным становится вопрос совершенствования системы уголовного наказания за преступления против интеллектуальной собственности.

Концептуальной основой исследования является понятие интеллектуальной собственности, закрепленное в ст. 1225 Гражданского Кодекса Российской Федерации¹.

Социальная обусловленность охраны интеллектуальной собственности выражается, прежде всего, в возрастании ее экономической ценности при становлении информационного общества. Еще одним фактором выступает то, что развитие информационных технологий способствовало росту числа преступлений против объектов интеллектуальной деятельности. Согласно статистическим данным, опубликованным Генеральной прокуратурой, 25% всех преступлений совершается посредством сети Интернет. В абсолютных значениях данный показатель увеличился в 12 раз за последние 7 лет².

Вызывает беспокойство и тот факт, что половина преступлений, совершаемых в телекоммуникационных сетях, относятся к категориям тяжким и особо тяжким. В научной литературе информационные технологии называют «кровеносной системой» преступности, они не только упрощают процесс совершения традиционных видов преступлений, но и порождают возможность возникновения новых видов.

Многие исследователи отмечают влияние цифровизации на рост преступлений против интеллектуальной собственности. По данным отчета Евразийского экономического союза в 2022 году ущерб от международной торговли контрафактной продукцией составил не менее 991 млрд. долларов³.

Опасность преступлений в отношении объектов интеллектуальной собственности заключается и в том, что они носят скрытый характер, это подтверждает и достаточно высокий коэффициент латентности, равный 3,5. Эксперты могут только прогнозировать число таких деяний так, как практика показывает, что из года в год скрытых преступлений в данной области всегда больше, чем выявленных.

Рост противоправных деяний в отношении результатов интеллектуальной деятельности обусловлен так же неэффективной системой уголовного наказания за преступления в сфере интеллектуальной собственности. Побегайло Э. Ф. называл проблему санкций «Ахиллесовой пятой» Уголовного кодекса Российской Федерации⁴. Титов С. Н. в своих работах нередко упоминал, что система санкций уголовного законодательства часто вступает в противоречие с общественными интересами и принципами социальной справедливости⁵.

Указанные недостатки в части санкций проявляются и в составах преступлений против интеллектуальной собственности. Ответственность за такие противоправные деяния предусмотрена статьями 146, 147, 180 и 183 Уголовного кодекса Российской Федерации⁶.

Модернизацию системы уголовного наказания в данной области представляется необходимым начать с систематизации видов и размеров санкционных ограничений за преступления схожей степени общественной опасности. Другим важным направлением можно считать гуманизацию системы уголовных санкций, использование альтернативных наказаний, не связанных с лишением свободы.

Анализ законодательства показывает, что в отношении преступлений против интеллектуальной собственности возможно усовершенствовать использование потенциала санкции в виде ограничения свободы. Стоит заметить, что ограничение свободы достаточно не систематизировано используется в санкциях преступлений в области экономической деятельности.

Тенденция применения альтернативных наказаний соответствует международным стандартам по защите прав человека и его интересов. Исходя из этого, ограничение свободы рассматривается как эффективный прием индивидуализации наказа-

ния. Его также можно рассматривать как альтернативный метод наложению штрафа, когда назначение второго не целесообразно в виду экономического положения виновного или его семьи. В случае возможности исправления преступника без применения к нему наказания в виде лишения свободы тоже можно применять ее ограничение.

Стоит разграничивать ограничение свободы и условное осуждение так, как первое несет в себе карательное воздействие, а второе рассматривается как освобождение от наказания.

Бриллиантов А. В. говорит, что применение штрафа впадает в большую зависимость от уровня жизни человека, а также характера преступных деяний⁷. Штраф как альтернатива лишению свободы широко применяется в Уголовном кодексе и включен в 453 санкции в виде основной меры наказания. В целях систематизации и гуманизации системы наказаний, многие правоведы предлагают включить штраф в качестве основного наказания в санкции ч. 3 ст. 146 УК РФ и ч. 4 ст. 183 УК РФ. О том, что такое решение назрело, говорит судебная статистика. Она показывает, что суды назначают штраф как основное наказание по ч. 3 ст. 146 УК РФ.

Состав преступлений против интеллектуальной собственности включает три вида трудового воздействия в качестве наказания. Исследования и многолетняя зарубежная практика говорит об эффективности применения данных мер. Маликов Б. З. отмечает, что обязательные, принудительные и исправительные работы имеют исторические корни, а и эффективность применения зависит от организации контроля и надзора их исполнения⁸.

На данном этапе развития законодательства применение мер трудового воздействия не систематизировано. Безусловно, возникает вопрос их систематизации, так Титов С. Н. предлагает включить исправительные и обязательные работы в санкции статей о преступлениях против интеллектуальной собственности в качестве альтернативных основных наказаний, если эти преступления относятся к преступлениям небольшой тяжести и средней тяжести.

Исходя из выше упомянутого, можно сделать вывод о том, что развитие института интеллектуальной собственности обусловлено трансформацией экономики и переходом к информа-

ционному обществу. Правовая охрана результатов интеллектуальной деятельности обусловлено их стратегической важностью для дальнейшего развития человечества. На сегодняшний день система уголовного наказания в Российской Федерации требует модернизации и усовершенствования согласно требованиям научно-технического прогресса и развития цифрового сознания общественности.

¹ Гражданский кодекс Российской Федерации // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 15.10.2023).

² Число совершенных через мобильную связь и интернет преступлений в России // TACC URL: <https://tass.ru/obschestvo/18417795> (дата обращения: 15.10.2023).

³ Изгагина Т. Ю. Противодействие распространению контрафактной продукции в условиях ЕАЭС // Юридический вестник Самарского университета. 2022. №3. URL: <https://cyberleninka.ru/article/n/protivodeystvie-rasprostraneniyu-kontrafaktnoy-produktsii-v-usloviyah-eaes> (дата обращения: 15.10.2023).

⁴ Алексеев А.И., Овчинский В.С., Побегайло Э.Ф. Российская уголовная политика: преодоление кризиса. М.: Норма, 2006. С. 48.

⁵ Титов, С. Н. Перспективы модернизации системы уголовного наказания за преступления против интеллектуальной собственности / С. Н. Титов // Пенитенциарная система и общество: опыт взаимодействия: сборник материалов X международной научно-практической конференции, Пермь, 05–07 апреля 2023 года. Том 1. – Пермь: Пермский институт Федеральной службы исполнения наказаний, 2023. – С. 236-240.

⁶ "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.11.2023) URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 15.10.2023).

⁷ Комментарий к Уголовному кодексу Российской Федерации. В 2. Т. 1 / под ред. А.В. Бриллиантова. М.: Проспект.

⁸ Маликов А.М. Наказания в виде обязательных и исправительных работ (теоретические и практические проблемы): дис. ... канд. юрид. н. Махачкала, 2011. С. 8–9.

*Саратовская государственная
юридическая академия
Кирдяпкина Валерия Федоровна
E-mail: lera.kirdyapkina.03@mail.ru*

*Saratov State Law Academy
Kirdyapina Valeria Fedorovna
E-mail: lera.kirdyapkina.03@mail*

Кожемяко Иван Александрович

Воронежский государственный университет

**ЦИФРОВИЗАЦИЯ И НАБЛЮДЕНИЕ ЗА ВЫБОРАМИ:
ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ПРАКТИКА
(НА ПРИМЕРЕ ЦЕНТРОВ
ОБЩЕСТВЕННОГО НАБЛЮДЕНИЯ)**

Kozhemyako Ivan Alexandrovich

Voronezh State University

**DIGITALIZATION AND ELECTION OBSERVATION:
LEGAL REGULATION AND PRACTICE
(BY THE EXAMPLE OF PUBLIC
OBSERVATION CENTERS)**

Аннотация: в статье освещается проблематика цифровизации избирательного процесса на примере внедрения видеонаблюдения за выборами, особое внимание уделено вопросам организации работы центров общественного наблюдения.

Ключевые слова: выборы, избирательный процесс, видеонаблюдение, центры общественного наблюдения.

Abstract: the article highlights the digitalization of the electoral process using the example of the introduction of video surveillance of elections, with special attention paid to the organization of the work of public observation centers.

Keywords: elections, electoral process, video surveillance, public observation centers.

В правовом демократическом государстве проведение выборов и референдумов не может происходить без участия институтов гражданского общества и осуществления общественного контроля. Одним из инструментов, позволяющих реализовать данное положение на практике, является внедрение системы видеонаблюдения за процессом голосования.

Введение видеонаблюдения при организации голосования впервые произошло в связи с выборами Президента Российской Федерации. В декабре 2011 г. В.В. Путин предложил Центральной избирательной комиссии Российской Федерации (далее по тексту – ЦИК РФ) и Министерству связи и массовых коммуникаций Российской Федерации обеспечить видеонаблюдение процедур голосования и подсчёта голосов избирателей на предстоящих выборах Президента Российской Федерации в 2012 г¹.

По вопросу цифровизации избирательного процесса и, в частности, процесса наблюдения Россия занимает лидирующие позиции. Например, по данным на 2021 г., в таких развитых государствах как Великобритания, Франция, Италия, Испания, Австрия, Нидерланды, Канада, Австралия видеонаблюдение за выборами не применяется².

Изначально предполагалось, что к 2021 г. видеонаблюдение должно было охватить около пятидесяти тысяч участков, где могли голосовать более восьмидесяти процентов избирателей. Однако непосредственно перед выборами председатель ЦИК РФ Э.А. Памфилова сообщила, что в общей сложности видеонаблюдением охвачены девяносто шесть процентов территориальных и участковых избирательных комиссий, где потенциально смогут проголосовать более девяноста восьми процентов избирателей³. Ранее она обращала внимание, что на выборах в Госдуму в 2016 г. видеонаблюдение охватывало только тридцать пять процентов избирателей⁴.

До 2021 г. трансляция в сети Интернет была доступна всем желающим, однако, в связи с кратным увеличением инфраструктуры и ростом продолжительности голосования, такое мероприятие потребовало бы существенных затрат. По сообщению Э.А. Памфиловой трансляция в сети Интернет с избирательных участков в течение трёх суток только по Москве стоила бы почти миллиард рублей, в то время как по всей стране она обошлась бы ещё дороже⁵. По словам главы рабочей группы Общественной палаты Российской Федерации по противодействию распространению недостоверной информации А.А. Малькевича открытая в течение трёх дней трансляция в сети Интернет потенциально может использоваться недобросовестными лицами посредством монтажа, склеек и создания недостоверных роликов о нарушении

ниях⁶. Тем не менее, кандидатам и политическим партиям предоставляется доступ к служебному portalу с онлайн-трансляцией с избирательных участков, а для граждан, желающих осуществлять наблюдение, есть возможность ознакомиться с ней в центрах наблюдения (видеонаблюдения) при общественных палатах субъектов Российской Федерации.

Впервые центры общественного наблюдения (далее по тексту – ЦОН, Центры) начали функционировать в 2021 г. Они были сформированы и работали на тот момент во всех 85 субъектах Российской Федерации и на федеральной территории «Сириус». В 18 субъектах Российской Федерации дополнительно были созданы филиалы таких Центров⁷. Стоит отметить, что Центры являются независимыми от Центральной избирательной комиссии Российской Федерации структурами, по словам заместителя председателя ЦИК РФ Н.И. Булаева Центры являются самостоятельными и независимыми структурами и единственная задача, которую ЦИК РФ ставит перед собой – обеспечение максимальных технических возможностей для эффективного и современного отображения происходящего на избирательных участках⁸. В этой связи в плане работы ЦИК РФ на 2023 г. особо выделены такие направления работы, как взаимодействие с Общественной палатой Российской Федерации, общественными палатами субъектов Российской Федерации, центрами общественного наблюдения за выборами и наблюдателями в целях обеспечения открытости и гласности избирательных процедур в Российской Федерации (п. 1.17 плана), а также анализ практики применения средств видеонаблюдения в помещениях для голосования, помещениях территориальных избирательных комиссий и трансляции изображения, в том числе в центрах общественного наблюдения (п.1.27 плана)⁹.

Организационное обеспечение деятельности ЦОН возложено на Общественную палату Российской Федерации. Техническое обеспечение видеотрансляции должно было осуществлять ПАО «Ростелеком».

Решением совета Общественной палаты Российской Федерации от 09 сентября 2021 г. № 112-С было утверждено Положение о Центре общественного наблюдения (видеонаблюдения) за ходом голосования при проведении выборов различного уровня в

Единый день голосования 19 сентября 2021 г.¹⁰. В соответствии с данным документом задачами Центра, особенно важными именно в отношении наблюдения на стадии голосования, являлись:

1) мониторинг ситуаций в участковых избирательных комиссиях и территориальных избирательных комиссиях, и в случае необходимости содействие оперативному реагированию наблюдателей при возникновении непредвиденных ситуаций;

2) организация просмотров видеотрансляции в случае поступления информации о возможных нарушениях требований избирательного законодательства и иных возникших на участках проблемах;

3) обеспечение взаимодействия с Общественными палатами субъектов Российской Федерации и муниципальных образований, наблюдателями и средствами массовой информации по вопросам видеонаблюдения.

7 сентября 2023 г. на базе Общественной палаты Воронежской области открылся Центр общественного наблюдения (видеонаблюдения) за ходом голосования, проводимого в 2023 г. В течение трёх дней – 8, 9 и 10 сентября – из Центра осуществлялось видеонаблюдение, с трансляцией изображения на восьми больших экранах и на персональных компьютерах¹¹. Организация работы Центра регулировалась в соответствии с Порядком, утверждённым Советом Общественной палаты Воронежской области¹². Аналогичные акты были приняты Общественными палатами других субъектов Российской Федерации. При подготовке данной публикации были изучены соответствующие акты Костромской, Новгородской и Псковской областей, Республики Алтай. По своему содержанию эти документы преимущественно дублируют Положение, утверждённое Решением совета Общественной палаты Российской Федерации от 09 сентября 2021 года № 112-С.

В соответствии с Порядком, утверждённым Советом Общественной палаты Воронежской области, право участвовать в работе Центра принадлежит совершеннолетним лицам, в частности, гражданами при предъявлении паспорта, за день до голосования направившим индивидуальную заявку по утверждённой Положением форме и согласие на обработку персональных данных. Для упорядочения и систематизации информации об участ-

никах видеонаблюдения в Центре ведётся журнал учёта лиц, принимающих участие в видеонаблюдении. Центр осуществляет свою работу круглосуточно, начиная с момента начала голосования и до составления протоколов о его итогах. Акцентируется внимание на том, что наблюдатели должны быть взаимовежливыми, не нарушать общественный порядок, а также не допускать использование и распространение ложной или непроверенной информации.

Несмотря на то, что не у всех общественных палат есть возможность размещения Центров в занимаемых ими помещениях, таковые всё равно организуются. Так, Общественная палата Орловской области дислоцировала Центр в Фундаментальной библиотеке ФГБОУ ВО "ОГУ им. И. С. Тургенева"¹³.

Видеонаблюдение является не только эффективным инструментом общественного контроля, но и защитой для членов избирательных комиссий от различного рода акций негативной направленности со стороны недобросовестных журналистов и лиц, осуществляющих действия провокационного характера¹⁴.

К сожалению, существует правовой пробел в сфере регулирования деятельности Центров общественного наблюдения (видеонаблюдения). Их статус пока что не закреплён в избирательном законодательстве. Как следствие, не определен статус граждан, пришедших в Центр по своей инициативе и осуществляющих в нём видеонаблюдение. Возникают вопросы о том, каким образом должны быть удостоверены полномочия гражданина, пришедшего в ЦОН, какие это полномочия, так как само присутствие в ЦОН в режиме видеонаблюдения делает невозможным использовать целый ряд прав, которыми, как правило, могут воспользоваться наблюдатели. Проблемой является то, что право на инициативное участие в видеонаблюдении из Центра общественного наблюдения не гарантируется с позиции трудового законодательства, так как по ст. 170 Трудового кодекса РФ работодатель обязан освободить работника только на время выполнения «государственных или общественных обязанностей», а гражданин реализует не обязанность, а своё право на видеонаблюдение за процессом голосования.

Таким образом, Центры общественного наблюдения (видеонаблюдения) – новый перспективный инструмент реализации

права граждан осуществлять наблюдение за проведением голосования и подведением его итогов. Центры популяризируют институт общественного наблюдения за выборами и Общественные палаты, так как демонстрируют ещё одну сферу их деятельности. Внедрение такого направления цифровизации как видеонаблюдение за процессом голосования позволяет существенно сократить число нарушений и повысить доверие к выборам и избирательным комиссиям у граждан.

¹ См.: РИА «Новости». URL: <https://ria.ru/20111215/517214531.html> (дата обращения: 18.10.2023).

² Презентация ЦИК о видеонаблюдении на выборах (21.07.2021) // URL: <https://telegra.ph/CIK-Rossii-prinyala-poryadok-videonablyudeniya-na-uchastkah-07-14> (дата обращения: 17.10.2023).

³ См. об этом: Ходыкин М. Всеобщее око: кто сможет следить за видеотрансляцией выборов и какие проблемы решает новая система // Известия. 2021. 10 авг. URL: <https://iz.ru/1214464/maksim-khodykin/vseobshchee-okto-smozhet-sledit-za-videotranslatsiei-vyborov> (дата обращения: 18.10.2023).

⁴ См.: Гулалиева М. Центры общественного наблюдения за выборами появятся в каждом регионе // Парламентская газета. 2021. 5 авг. URL: <https://www.pnp.ru/politics/centry-obshhestvennogo-nablyudeniya-za-vyborami-poyavyatsya-v-kazhdom-regione.html?ysclid=lnrtjcw4a2246148326https://www.pnp.ru/politics/centry-obshhestvennogo-nablyudeniya-za-vyborami-poyavyatsya-v-kazhdom-regione.html?ysclid=lnrtjcw4a2246148326> (дата обращения: 17.10.2023).

⁵ См.: Сайт Сетевого издания "ТВ Центр-Москва" (новость от 21.07.2021). URL: <http://www.tvc.ru/news/show/id/216154> (дата обращения: 17.10.2023).

⁶ См. об этом: Ходыкин М. Всеобщее око: кто сможет следить за видеотрансляцией выборов и какие проблемы решает новая система // Известия. 2021. 10 авг. URL: <https://iz.ru/1214464/maksim-khodykin/vseobshchee-okto-smozhet-sledit-za-videotranslatsiei-vyborov> (дата обращения: 18.10.2023).

⁷ См.: Маркина Л. Практика организации видеонаблюдения на выборах, прошедших в единый день голосования 19 сентября 2021 года: *Из выступления на совещании Комитета Совета Федерации по Регламенту и организации парламентской деятельности 29.11.2021 г.* // *Официальное сетевое издание «Вестник Центральной избирательной комиссии Российской Федерации»*. URL: <http://vestnik.cikrf.ru/vestnik/publications/opinions/51133.html> (дата обращения: 18.10.2023).

⁸ См.: Сайт сетевого издания "ТВ Центр-Москва" (новость от 21.07.2021). <https://www.tvc.ru/news/show/id/216195?ysclid=lnrt76p4rj784111812> (дата обращения: 18.10.2023).

⁹ См.: Постановление ЦИК России от 21.12.2022 г. № 104/817-8 "О Плане работы Центральной избирательной комиссии Российской Федерации на 2023 год" // СПС «КонсультантПлюс».

¹⁰ См.: Сайт Общественной палаты Волгоградской области // URL: <https://opvo.volganet.ru/2-obshchestvennoe-nablyudenie-za-provedeniem-vyborov-v-edinyy-den-golosovaniya-13-sentyabrya-2020-go/polozhenie-centr-vibori-oprf09092021%20%281%29.pdf> (дата обращения: 18.10.2023).

¹¹ См.: Сайт Общественной палаты Воронежской области // URL: https://opvo36.ru/news_detail/1741/?ysclid=lnrwl39rtv518730359 (дата обращения: 18.10.2023).

¹² См.: Порядок организации работы центра общественного наблюдения (видеонаблюдения) за ходом голосования при проведении в единый день голосования 10 сентября 2023 года: утв. Советом Общественной палаты Воронежской области // Ссылка на текст документа опубликована в информации «В Общественной палате Воронежской области открылся Центр общественного наблюдения. URL: https://opvo36.ru/news_detail/1741/?ysclid=lnrwl39rtv518730359 (дата обращения: 17.10.2023).

¹³ См.: Центр общественного наблюдения (видеонаблюдения) приглашает к сотрудничеству // Сайт Общественной палаты Орловской области. URL: [opo.o.ru/новости/центра-общественного-наблюдения-\(видеонаблюдения\)-приглашает-к-сотрудничеству](https://opo.o.ru/news/centra-obshchestvennogo-nablyudeniya-videonablyudeniya-priglasenie-k-sotrudnichestvu) (дата обращения: 17.10.2023).

¹⁴ См.: Юхин С. Видеонаблюдение – ключевой инструмент общественного контроля и защита от провокаторов // Сайт «Независимый общественный мониторинг». URL: <https://nom24.ru/info/events/sergey-yukhin-videonablyudenie-klyuchevoy-instrument-obshchestvennogo-kontrolya-i-zashchita-ot-provo/?ysclid=lnrv3kckxc172042301> (дата обращения: 17.10.2023).

*Воронежский государственный
университет
Кожемяко Иван Александрович
E-mail: Iwank01@mail.ru*

*Voronezh State University
Kozhemyako Ivan Alexandrovich
E-mail: Iwank01@mail.ru*

Курлянчик Владислав Сергеевич

*Гродненский государственный
университет имени Янки Купалы*

**ПРАКТИКА ПРИМЕНЕНИЯ
ЭЛЕКТРОННЫХ НАВИГАЦИОННЫХ ПЛОМБ
В ЕВРАЗИЙСКОМ ЭКОНОМИЧЕСКОМ СОЮЗЕ**

Kurlyanchik Vladislav Sergeyevich

Yanka Kupala State University of Grodno

**USE OF ELECTRONIC NAVIGATION SEALS
IN THE EURASIAN ECONOMIC UNION**

Аннотация: цель исследования заключается в определении эффективности использования навигационных пломб в ЕАЭС. Проводится анализ положений Соглашения о применении в Евразийском экономическом союзе навигационных пломб для отслеживания перевозок 2022 года. В статье определены национальные операторы, осуществляющие контроль за передвижение грузов на территории государств-членов ЕАЭС. Автор уделяет внимание информационному взаимодействию по применению навигационных пломб между государствами-членами ЕАЭС и подробно рассматривает статью 9 Соглашения.

Abstract: the purpose of the study is to determine the effectiveness of the use of navigation seals in the EAEU. The analysis of the provisions of the Agreement on the Use of Navigation Seals in the Eurasian Economic Union for Tracking Traffic in 2022 is carried out. The article defines the national operators that control the movement of goods on the territory of the EAEU member states. The author pays attention to information interaction on the use of navigation seals between the EAEU member states and examines in detail Article 9 of the Agreement.

Ключевые слова: электронная навигационная пломба, перемещение товаров, Евразийский экономический союз (ЕАЭС), национальный оператор, контролирующий орган.

Keywords: *electronic navigation seal, movement of goods, the Eurasian Economic Union (EAEU), the national operator, the supervisory authority.*

Актуальность темы исследования заключается в том, что таможенное регулирование всегда находится на стыке интересов государства и бизнеса. Государственным органам необходимо обеспечить экономическую безопасность. Бизнесу нужно простое и понятное таможенное регулирование, выборочный и прогнозируемый таможенный контроль, отсутствие неоправданных затрат. Дальнейшее развитие таможенного регулирования связано с внедрением современных электронных технологий, вытеснением бумажного документооборота, максимальной цифровизацией всех процессов.

Так, одним из механизмов отслеживания перевозок по территории Евразийского экономического союза (далее – ЕАЭС) является использование электронных навигационных пломб (далее – навигационная пломба).

Навигационная пломба – это специальное устройство, с помощью которого можно отслеживать передвижение грузов по территории ЕАЭС.

Эффективность использования навигационных пломб заключается в том, что их использование позволяет осуществлять дистанционный цифровой контроль при трансграничных перевозках грузов, гарантировать сохранность товаров и упростить процедуры их оформления на границе. Применение навигационных пломб повышает прозрачность перевозок по территории ЕАЭС. Для бизнеса преимущества также очевидны. Это гарантия безопасного транзита своих товаров на пространстве ЕАЭС, исключение дополнительных форм и мер контроля со стороны контролирующих органов союза, экономия денежных средств. Так, используя навигационные пломбы в Республике Беларусь, перевозчик тратит порядка 50 долларов США, а используя таможенное сопровождение 300 долларов США¹.

Первой страной на территории ЕАЭС, которая начала использовать навигационные пломбы и доказала эффективность их использования, является Республика Беларусь. В Республике Беларусь навигационные пломбы начали тестировать в

2019 году, в период обострения пандемии, чтобы отслеживать движение транспортных средств по установленному маршруту, а их использование началось в 2020 году на основании Постановления Совета Министров Республики Беларусь № 311 «О применении навигационных устройств (пломб)» от 25 мая 2020 года. Так, Владимир Орловский, председатель ГТК, отметил эффективность использования навигационных пломб и сказал, что «с марта по июнь 2020 года, когда использовали пломбу в рамках ограничения распространения коронавирусной инфекции, мы применили порядка 80 тыс. пломб. И если до применения пломб у нас было зафиксировано примерно 30 нарушений по отклонению от маршрута, после начала применения пломб – менее 1%»². На данный момент навигационные пломбы обеспечивают прозрачность перевозок и являются альтернативой таможенному сопровождению.

Опираясь на опыт использования навигационных пломб белорусскими коллегами, 19 апреля 2022 года в Москве было подписано «Соглашение о применении в Евразийском экономическом союзе навигационных пломб для отслеживания перевозок» (далее – Соглашение), а 3 апреля 2023 года оно вступило в силу. Настоящее Соглашение определяет основы регулирования применения в ЕАЭС навигационных пломб для отслеживания перевозок объектов отслеживания по территориям двух и более государств-членов ЕАЭС. Также в Соглашении отмечается, что использование навигационных пломб должно минимизировать количество досмотров и осмотров содержимого в грузовых емкостях транспортных средств. В Соглашении отмечается, что отслеживание перевозок по территориям государств-членов ЕАЭС обеспечивается национальными операторами с использованием информационных систем. В Республике Беларусь национальным оператором является – РУП «Белтаможсервис», Российской Федерации – ООО «Центр развития цифровых платформ», Республике Казахстан – ДТОО «Институт космической техники и технологий», Республике Армения – компания "АрмДжиПиЭс", Республике Киргизия – ассоциация «АМАП КР».

Член Коллегии, министр по таможенному сотрудничеству Евразийской экономической комиссии Эльдар Алишеров отметил, что «в Соглашении предусмотрено, что использование

навигационных пломб будет внедряться в три этапа. Первый — в январе 2024 года, когда должны начать применять пломбы по акцизным, санкционным и налоговым товарам, перевозимым автомобильным транспортом. Это алкоголь, табак, одежда, бытовая техника и прочее. Второй этап начнется с середины следующего года, когда с навигационными пломбами будут перемещать уже и другие товары, а также начнется применение этих технологий по железной дороге. На третьем этапе будет внедрена перевозка всех видов товаров по железной дороге с применением навигационной пломбы»³. Также правовой основой применения навигационных пломб в ЕАЭС является не только Соглашение, но и Решение Коллегии ЕЭК от 22.08.2023 № 128 «О некоторых вопросах применения навигационных пломб».

Следует отметить, что в рамках реализации Соглашения предусмотрено информационное взаимодействие по применению навигационных пломб между государствами-членами ЕАЭС.

На основании рисунка подробно рассмотрим статью 9 Соглашения.

1. Отслеживание перевозок по территориям государств-членов на всем пути следования (перевозки) объектов отслеживания осуществляет национальный оператор государства-члена, на территории которого начинается такое отслеживание. На рисунке показано, что отслеживание перевозки начинается в Республике Беларусь, поэтому отслеживать перевозку будет национальный оператор Республики Беларусь – РУП «Белтаможсервис».

2. Для обеспечения отслеживания перевозок по территориям государств-членов национальным оператором (в нашем случае РУП «Белтаможсервис»), отслеживающим перевозку по территориям государств-членов, в случае, если для отслеживания перевозок по территориям государств-членов применяется навигационная пломба (в нашем случае навигационная пломба Республики Казахстан), зарегистрированная в информационной системе национального оператора другого государства-члена (в нашем случае (ДТОО «Институт космической техники и технологий»)), используется программно-аппаратный комплекс, обеспечивающий возможность активации и деакти-

вации навигационной пломбы информационной системой указанного национального оператора (в нашем случае РУП «Белтаможсервис») и маршрутизацию информации, получаемой от такой навигационной пломбы, в его информационную систему (в нашем случае в ДТОО «Институт космической техники и технологий»). То есть РУП «Белтаможсервис», используя навигационную пломбу Республики Казахстан, предоставляет доступ ДТОО «Институт космической техники и технологий» для того, чтобы и в Республике Казахстан видели, где следует транспортное средство.

3. На рисунке видно, чтобы доставить товар из Республики Беларусь в Республику Казахстан перевозчик должен будет проехать территорию Российской Федерации. В связи с этим РУП «Белтаможсервис» обязан предоставить сведения в режиме реального времени национальному оператору Республики Казахстан (ДТОО «Институт космической техники и технологий») и Российской Федерации (ООО «Центр развития цифровых платформ»).

4. Национальный оператор Республики Казахстан (ДТОО «Институт космической техники и технологий») и Российской Федерации (ООО «Центр развития цифровых платформ»), Республики Беларусь («Белтаможсервис») осуществляют сбор, обработку, передачу информации о такой перевозке, включая передачу информации, в контролирующие органы (таможенные органы) своего государства-члена.

Таким образом, реализация положений Соглашения о применении в Евразийском экономическом союзе навигационных пломб для отслеживания перевозок 2022 года позволяет в online-режиме контролировать перемещение товаров и транспортных средств на территории Республики Беларусь и ЕАЭС; обеспечивает «прозрачность» перевозок; упрощает и ускоряет процедуру доставки грузов получателю; минимизирует количество досмотров и осмотров содержимого в грузовых емкостях транспортных средств; обеспечивает снижение в ЕАЭС доли теневого товарооборота, от которого страдают добросовестные производители и потребители. Также важным аспектом в применении навигационных пломб является информационное взаимодействие между государствами-членами ЕАЭС.

¹ Экономия или необходимость: для чего нужны навигационные пломбы [Электронный ресурс] // Sputnik Беларусь – последние новости и главные события. – URL: <https://sputnik.by/20210405/Ekonomiya-ili-neobkhodimost-dlya-chego-nuzhny-navigatsionnye-plomby-1047310321.html> (Дата обращения: 15.10.2023).

² ГТК Беларуси с 4 августа начнет применять навигационные пломбы при перевозках товаров вместо таможенного сопровождения [Электронный ресурс] // Агентство ПраймПресс. – URL: https://primepress.by/news/ekonomika/gtk_bearus_i_s_4_avgusta_nachnet_primenyat_navigatsionnye_plomby_pri_perevozkakh_tovarov_vmesto_tamo-23457/ (Дата обращения: 15.10.2023).

³ О трех этапах внедрения в ЕАЭС навигационных пломб рассказал министр ЕЭК [Электронный ресурс] // Новости Кыргызстана. – URL: <https://ru.sputnik.kg/20230929/eaes-navigatsionnye-plomby-alisherov-1079011769.html> (Дата обращения: 01.10.2023).

*Гродненский государственный
университет имени Янки Купа
Курляничик Владислав Сергеевич
E-mail: kurlyanchik2310@mail.ru*

*Yanka Kupala State University
of Grodno
Kurlyanchik Vladislav Sergeyevich
E-mail: kurlyanchik2310@mail.ru*

Малыхина Валерия Викторовна

Воронежский государственный университет

**ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
В ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРАВА**

Malykhina Valeria Viktorovna

Voronezh State University

**ARTIFICIAL INTELLIGENCE
IN THE DIGITAL TRANSFORMATION OF LAW**

Аннотация: в статье поднимается проблема правового регулирования общественных отношений, связанных с использованием искусственного интеллекта. Актуальность исследования обусловлена увеличением количества сфер, внедряющих инновационные механизмы. В рамках анализа категории правосубъектности рассматривается аспект соотношения конструкции искусственного интеллекта и юридического лица. Несмотря на то, что современном этапе невозможно провести абсолютную аналогию, в перспективе традиционная модель правосубъектности может быть расширена, в связи с чем необходимо предварительное осмысление данного вопроса с позиции как теории права, так и практики его применения.

Abstract: the article raises the problem of legal regulation of public relations related to the use of artificial intelligence. The relevance of the study is due to the increase in the number of areas introducing innovative mechanisms. Within the framework of the analysis of the category of legal personality, the aspect of the relationship between the construction of artificial intelligence and a legal entity is considered. Despite the fact that it is impossible to draw an absolute analogy at the present stage, in the future the traditional model of legal personality can be expanded, and therefore a preliminary understanding of this issue is necessary from the standpoint of both the theory of law and the practice of its application.

Ключевые слова: правосубъектность, трансформация права, искусственный интеллект, электронное лицо, юридическая ответственность.

Keywords: legal personality, transformation of law, artificial intelligence, electronic person, legal responsibility.

Трансформация правовых институтов, свойственная современному этапу развития общества, неизбежно влечет возникновение ранее неизвестных категорий и постановку новых вопросов, связанных с опережающим законодательством развитием общественных отношений. Цифровизация общественных отношений предопределила возникновение беспилотных летательных аппаратов, самоуправляемых транспортных средств и компьютеров с системой искусственного интеллекта (далее – ИИ), способных генерировать определенные решения за человека.

Область применения технологий ИИ расширяется с каждым годом, включая в себя как традиционные сферы использования – производство расчетов, анализ данных, так и иные – тесно связанные с жизнедеятельностью человека. Это порождает множество вопросов о последствиях таких решений¹, а также – о распределении бремени ответственности за них, и, как следствие, заставляет пересматривать традиционные правовые представления о правосубъектности в контексте использования искусственного интеллекта.

В 2017 году Европейский парламент озвучил инициативу разработки правовых норм, определяющих процесс создания и использования ИИ, что нашло отражение в Резолюции от 16.02.2017 г., в которой выделено две модели ответственности за вред, причиненный робототехникой: ответственность независимо от вины и иная модель ответственности, согласно которой ответственным признается лицо, способное минимизировать риски. В Резолюции подчеркивается, что необходимо учитывать уровень самостоятельности робота, отличать навыки, которыми его обучили в рамках тренировок, от навыков, которые робот приобрел в процессе самостоятельного обучения.

Резолюция от 16.02.2017 г. в долгосрочной перспективе предусматривает разработку специального правового статуса «электронных лиц» (electronic persons), которые могут иметь

права и обязанности в случае вступления в равноправные отношения с третьими лицами, а также способных нести самостоятельную ответственность за любой причиненный вред.

Важно отметить, что в Резолюции указана перспектива наделения статусом «электронных лиц» «продвинутых» автономных роботов – сильного искусственного интеллекта. Современные технологии моделируют образ «слабого» искусственного интеллекта, основанного на математических вычислениях и не способного к многоаспектному анализу ситуации, более того, соотносению действий с морально-этическими постулатами.

Активное развитие технологического процесса обуславливает вопрос: сможет ли искусственный интеллект стать самостоятельной личностью, способной к усвоению чувственного опыта, самоопределению наравне с человеком?

Как отмечают исследователи, определение личности подвергалось изменениям с течением времени. Многие современные дискуссии о личности базируются на определениях, выдвинутых мыслителями эпохи Просвещения. Так, Джон Локк в «Эссе о человеческом понимании»² описывает «личность» как «судебно-медицинский термин», который «принадлежит только разумным агентам, способным соблюдать закон, а также счастье и несчастье». Позднее Д. К. Грей проводит различие между общим и техническим юридическими значениями понятия «личность», отмечая, что последнее относится к «субъекту юридических прав и обязанностей»³.

Исследователи все чаще обращают внимание на применение юридической индивидуальности к технологическим объектам, в частности, технологиям искусственного интеллекта. Основные аргументы сосредоточены вокруг степени, в которой формы технологии демонстрируют способности, подобные человеческим. В своих трудах Л. Б. Солум⁴ выдвигает три возражения против предоставления ИИ статуса юридического лица: (1) личность должна предоставляться только физическим лицам; (2) ИИ не обладает некоторыми свойствами, необходимыми для получения статуса юридического лица (в частности, сознанием, душой); и (3) человеческие артефакты никогда не могут быть чем-то большим, чем человеческая собственность. Можно проследить три эволюционные стадии правовой адаптации – «кра-

ткосрочная: толкование и расширение существующего законодательства», «среднесрочная: ограниченная индивидуальность со строгой ответственностью» и «долгосрочная: полная индивидуальность с «постчеловеческими» правами».

В рамках исследований выдвигаются идеи о создании поведенческих тестов, с помощью которых сущность может претендовать на статус личности. Так, Ф. П. Хаббард⁵ предлагает следующие критерии: (1) способность взаимодействовать со своим окружением и участвовать в сложном мышлении и общении, (2) ощущение себя самим собой с заботой о достижении своего плана или цели в жизни и (3) способность жить в сообществе, основанном на взаимных личных интересах с другими людьми. Указанные способности зависят от обладания такими свойствами, как рациональность, интеллект, самосознание.

В рамках национального правового поля попытка легального определения ИИ была предпринята путем принятия Указа Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». В документе обозначено, что ИИ есть комплекс технологических решений, позволяющий *имитировать когнитивные функции человека* (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека.⁶

Анализ данной дефиниции показывает, что ИИ – это не просто набор технологий, специальных методов и алгоритмов, но те из них, которые, во-первых, воспроизводят когницию, особый психологический механизм, направленный на обработку человеческим сознанием определенной информации, и, во-вторых, приводят к появлению интеллектуального продукта.

В 2008 г. впервые была апробирована новая технология действия мемристора, которая по образу своей работы схожа с коммуникационным предназначением нейронного синапса, отвечающего за передачу нервного импульса между клетками живого организма с участием комплекса нейромедиаторов, что позволило сделать шаг к построению нейроморфной архитектуры ИИ, которая эффективно подражает деятельности *encephalon*.

Очерченное создает предпосылки для перехода от слабого ИИ или ИИ с ограниченной памятью, которые в целом фрагментарно запоминают различные сведения, к сильному ИИ, действительно имитирующему базовые когнитивные способности *homo sapiens* в целях достижения результатов, аналогичных итогам интеллектуальной деятельности. Переход может быть сопряжен с реализацией таких познавательных элементов, как восприятие, память, мышление.

В этой связи исследователи предопределяют возникновение правового явления Smart Law Doctrine – условной «отрасли права», содержащей общие направления правового регулирования новой сферы общественных отношений. Среди принципов робототехники выдвигаются такие, как «Роботы не должны играть на эмоциях чувствительных людей», «ИИ должен быть прозрачен: всегда должна иметься возможность выяснить, как он работает». Формирование способности моделировать когнитивные функции человека предопределяют наложение определенных обязанностей на роботизированные системы, в частности – технологии ИИ. Однако наравне с этим предлагается закрепление за ИИ права на развитие и самоопределение, что неразрывно связано с концепцией свободы воли.

В этой связи дискуссия о целесообразности придания ИИ статуса субъекта права обретает практическое значение. В долгосрочной перспективе вопрос о расширении правосубъектности может быть поставлен, поэтому он нуждается в предварительном осмыслении с позиции как теории права, так и практики его применения.

¹ Архипов, В. В. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике / В. В. Архипов, В. Б. Наймов // – 2017. – № 6(55). – С. 46-62.

² Locke J. An Essay Concerning Human Understanding (27th ed.). T. Tegg and Son – 1836. – P. 234.

³ Gray J. C. The Nature and Sources of the Law. Columbia University Press. – 1909. – P. 27.

⁴ Solum L. B. Legal Personhood for Artificial Intelligences. North Carolina Law Review, 70(4). – 1992. – 1231–1288 p.

⁵ Hubbard F. P. “Do Androids Dream?”: Personhood and Intelligent Artifacts. Temple Law Review, 83, 405–474. -2011. – P. 419.

⁶ Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года").

*Воронежский государственный
университет
Мальхина Валерия Викторовна
E- mail: lera.malyhina@mail.ru*

*Voronezh State University
Malykhina Valeria Viktorovna
E- mail: lera.malyhina@mail.ru*

Пономарева Лилия Александровна

Воронежский государственный университет

ЗАКЛЮЧЕНИЕ И ИСПОЛНЕНИЕ СМАРТ-КОНТРАКТОВ В СОВРЕМЕННОМ ГРАЖДАНСКОМ ПРАВЕ

Ponomareva Lilia Alexandrovna

Voronezh State University

CONCLUSION AND EXECUTION OF SMART CONTRACTS IN MODERN CIVIL LAW

Аннотация: в статье рассматривается понятие «смарт-контакта», в том числе с опорой на зарубежный опыт, предпринимается попытка раскрыть правовую природу смарт-контрактов. В статье также поднимаются проблемы, связанные с применением смарт-контрактов в гражданском обороте.

Abstract: the article discusses the concept of "smart contact", including relying on foreign experience, explains the legal nature of smart contracts. The article also raises issues related to the use of smart contracts.

Ключевые слова: смарт-контакт, автоматизированность контракта, электронная форма сделки, блокчейн

Keywords: smart contact, contract automation, electronic transaction form, blockchain.

Развитие IT-технологий в современном мире обусловило появление и широкое распространение в юриспруденции понятия «смарт-контракт». Так как раньше в законах не было подобия «умному договору», то на сегодняшний день возникла необходимость создания правовых мер, обеспечивающих его заключение и исполнение с учетом защиты интересов сторон.

В отечественном законодательстве термин «смарт-контракт» в настоящее время не выделяется, поэтому обратимся к науке и практике зарубежных стран.

Термин «смарт-контракт» (smartcontract) ввел в употребление в 1994 г. американский ученый в области информатики, криптографии и права Ник Сабо. Он утверждал, что описание всех условий «умного контракта» должно совершаться с помощью математических инструментов и языков программирования. Смарт-контракт ученый описывал в своих работах как электронный алгоритм, рассчитанный для автоматизации процесса исполнения контрактов в блокчейне¹.

Российские ученые О. С. Гринь, Е. С. Гринь и А. В. Соловьев, отмечают несколько трактовок термина смарт-контракт²:

– «*smartcontract*» как компьютерный код. Здесь имеется в виду, что обязательство создается с использованием электронных средств, являющееся разновидностью письменной формы сделки (статья 309 ГК РФ).

– «*legalsmartcontract*» – условия договора, обеспеченные программным кодом. Всегда достигается исполнение соглашения, так как происходит автоматическое исполнение обязательства по заранее заданным сторонами условиям на платформе блокчейн при помощи программной кодировки, но без участия его сторон.

В настоящее время в действующем законодательстве РФ определение смарт-контрактов отсутствует. Общепринятой в российской теории гражданского права стала формулировка, предложенная А. И. Савельевым. Он трактует этот термин как «соглашение сторон, существующее в виде программного кода, действующего в распределенном реестре данных, обеспечивающего выполнение условий такого договора при наступлении заранее определенных в нем обстоятельств»³.

В Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» было принято решение отказаться от использования этого понятия. Возможность использования смарт-контрактов в части 2 статьи 309 ГК РФ изложена так: «Условиями сделки может быть предусмотрено исполнение ее сторонами возникающих из нее обязательств при наступлении определенных обстоятельств без направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления его сторон путем применения информационных технологий, определенных условиями сделки»⁴.

Основные характеристики смарт- контракта:

1) смарт-контракт является цифровой формой гражданско-правового договора или сразу нескольких договоров. При этом:

а) условия соглашения выражены в виде программного кода,
б) автоматическое исполнение встречного обязательства по типу «если – то» (*if – then*) – по заранее заданным сторонами условиям в информационной системе блокчейн,

в) невозможность его изменения, в том числе по соглашению сторон после того, как он был размещен в сети блокчейн;

2) смарт-контракт гарантирует точность фиксации и удер- живания информации о нем в информационном поле блокчейн.

3) при расчетах применяются цифровые финансовые активы и виртуальная валюта, представляющие собой записи в информационной системе блокчейн, подтверждающие имущественные и иные права.

С учетом юридической природы следует отметить, что, яв- ляясь на сегодняшний день особым способом заключения до- говора, смарт-контракт стал особой разновидностью договора присоединения и может быть представлен в виде сделки под ус- ловием (в рамках статьи 157 ГК РФ) либо выступать в качестве договора с ограниченным исполнением обязательства (статья 327.1 ГК РФ). Это обусловлено тем, что «умный» контракт само- стоятельно исполняется только при наступлении определенного события, которое было согласовано в договоре.

Для того чтобы заключить договор в форме смарт-контракта, необходимо использовать специальные электронные платфор- мы, функционирующие на принципах системы блокчейн, то есть на основе децентрализованных баз данных, хранящие в себе ма- тематические алгоритмы, закрепляющие условия заключенных сделок.

Момент заключения смарт-контракта может быть точно определен, так как программный код функционирует только во время внесения записи об акцепте оферты в очередной блок за- писей распределенного реестра.

Выделяется несколько способов внесения изменений:

– прекратить или расторгнуть действующий смарт-контракт и заключить новый с измененными условиями;

– внести изменения в программный код смарт-контракта без его прекращения (в случае, если устройство платформы, на которой реализован смарт-контракт, допускает такие изменения).

Исполнение смарт-контракта реализуется как в полном объеме, так и по частям, что фиксируется в распределенном реестре, где развернут смарт-контракт.

Так, срок выполнения строго контролируется программным кодом, просрочка и исполнение помечаются в распределенном реестре.

В то же время применение на практике смарт-контрактов имеет ряд трудностей:

1. Дефицит IT-специалистов для создания данного продукта. Обусловлен нехваткой на рынке труда специалистов достаточно высокой квалификации, способных создать программный код без уязвимостей⁵.

2. Трудности понимания кода для рядового участника. Документ содержит условия договора, которые могут быть прописаны в самом контракте и компьютерном коде. Для понимания договора в простой письменной форме не требуется особых знаний, однако для проверки записанных в компьютерном коде условий с целью удостоверения в правильности и полноте записи условий сделки требуется специальное образование, поскольку компьютерный код составляется на языке программирования. Для анализа кода требуется привлечение третьего лица⁶.

3. Зависимость смарт-контрактов от offchain ресурсов. Для реализации условий необходимы сведения, поступающие от расположенных не в блокчейне внешних источников, называемых оракулами – доверенных третьих сторон, получающих данные из внешних систем и передающих их в блокчейн по расписанию.

4. Невозможность изменения и расторжения смарт-контрактов. Отсутствие гибкости отвечает принципам блокчейна, но усложняет взаимодействие между заинтересованными сторонами.

5. Обнаруживается крайне низкий уровень распространенности в России системы смарт-контрактов, поскольку, согласно внутреннему регулированию, они должны дублироваться на бумажном носителе, что противоречит природе смарт-контрактов, ориентированной на замену бумажного документооборота цифровым.

Итак, возрастающий интерес мирового правового сообщества, специфические признаки смарт-контрактов, выделяющие их из всего многообразия других договорных конструкций, подтверждают безусловную потребность утверждения понятия «смарт-контракт» на уровне федеральных законов, а не просто упоминание данного термина на уровне специальных узконаправленных нормативных правовых актов.

Существенной проблемой является отсутствие закрепления смарт-контрактов на законодательном уровне как формы заключения гражданско-правовых соглашений. К недостаткам их использования можно также отнести: смарт-контракты – это программный код, который опосредует возможность ошибок и сбоев в программе, что подразумевает необходимость привлечения специалиста по IT-технологиям и оплату его услуг.

Преимуществами же смарт-контрактов являются их самоисполняемость, защита от изменений, которые не утверждены сторонами, прозрачность исполняемой сделки.

Из вышесказанного следует, что одной из первоочередных задач является закрепление понятия смарт-контракта на уровне федерального закона.

¹ Мамаева, Н. В. Смарт-контракты / Н. В. Мамаев // Наука и образование. – 2018. – № 4 (27). – С. 11–12.

² Гринь О. С. и др. Правовая конструкция смарт-контракта: юридическая природа и сфера применения / О. С. Гринь, Е. С. Гринь, А. В. Соловьев // Lexrussica. – 2019. – № 8. – С. 51–62.

³ Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права / Вестник гражданского права. – 2016. – № 3. – С. 32–60.

⁴ Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51ФЗ (ред. от 31.07.2020) // СЗ РФ. 1994. № 32. Ст. 3301.

⁵ Шайхутдинов Р.Р. Понятие и проблемы внедрения смарт-контрактов // Мавлютовские чтения: материалы XIV Всероссийской молодёжной научной конференции. – Уфа, 2020. – С. 27–32.

⁶ Душаева А.А. Проблемы применения смарт-контрактов в деятельности компании // Имущественные отношения в Российской Федерации. – 2019. – № 10 (217). – С. 58–64.

*Воронежский государственный
университет
Пономарева Лилия Александровна
E-mail: lilia.lilia30@yandex.ru*

*Voronezh State University
Ponomareva Lilia Alexandrovna
E-mail: lilia.lilia30@yandex.ru*

Попова Виктория Павловна

Воронежский государственный университет

ЭЛЕКТРОННЫЕ РЕСУРСЫ В СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Popova Victoria Pavlovna

Voronezh State University

ELECTRONIC RESOURCES IN THE PUBLIC ADMINISTRATION SYSTEM

Аннотация: последние несколько десятилетий характеризуются широким распространением информационных технологий во всех сферах жизни общества в России, и государственное управление не является исключением. В данной статье рассматриваются самые востребованные электронные ресурсы в системе управления государством на современном этапе его развития, а также возникающие проблемы в данной области общественных отношений.

Abstract: the last few decades have been characterized by the widespread use of information technologies in all spheres of society in Russia, and public administration is no exception. This article examines the most in-demand electronic resources in the system of government at the present stage of its development, as well as emerging problems in this area of public relations.

Ключевые слова: государственное управление, электронные ресурсы, информационные технологии, искусственный интеллект.

Keywords: public administration, electronic resources, information technology, artificial intelligence.

Государственная информационная политика – это относительно обособленная и независимая деятельность государства по применению информации в процессах информационного обмена, установления и реализации целей, задач, принципов, приоритетов и условия развития информационной сферы. Какие же

задачи стоят перед государством для развития информационной сферы? Прежде всего, это управленческая задача – информационное обеспечение принятия решений в области государственного управления и доведение их до нижестоящих руководителей, подчиненных, граждан; задача по обеспечению безопасности – защита государственной информации с ограниченным доступом и секретных данных; защита прав и свобод граждан при использовании информационных систем, защита граждан от деструктивной информации, а также государственный контроль. Политика информатизации заключается в создании технических, технологических и экономических условий развития информационных технологий.

В последнее время электронные ресурсы стали занимать особое место в системе государственного управления. К ним относят Единый портал государственных услуг Российской Федерации, систему электронного документооборота для государственных и муниципальных ведомств и организаций, портал открытых данных Российской Федерации, возможность проведения судебных заседаний в режиме онлайн и не только.

Стоит отметить, что Правительство РФ активно внедряет электронные ресурсы в систему работы государственных органов¹.

Так, было утверждено Положение о новой системе электронного документооборота для государственных и муниципальных ведомств и организаций. Данное Постановление (от 15 февраля 2022 года №172) устанавливает рекомендации органам государственной власти, органам местного самоуправления, государственным и муниципальным учреждениям использовать государственную информационную систему «Типовое облачное решение системы электронного документооборота»².

Такие системы электронного документооборота дают возможность создавать, пересылать, подвергать обработке, сохранять и подписывать документы в цифровой форме с соблюдением важных норм и требований безопасности, в отсутствии использования электронных носителей. Благодаря такому решению большое количество рутинных процессов удастся автоматизировать. Систему электронного документооборота широко используют как федеральные, так и региональные органы госу-

дарственной власти, но, следует отметить, что на муниципальном уровне и в бюджетных организациях такие решения еще не установлены. Помимо обеспечения увеличения качества и скорости оказания государственных услуг «типовое облачное решение» будет способно уменьшать трудовые, материальные и временные затраты организаций-участников и ведомств.

Широкое распространение получила тенденция проведения судебных заседаний в Арбитражном суде в онлайн-режиме. Этому способствовала прошедшая пандемия. Впервые предложение о проведении судебных заседаний в онлайн-режиме была указана в п. 5 Постановления Президиума Верховного Суда Российской Федерации и Президиума Совета судей Российской Федерации от 8 апреля 2020 г. №821³. Следует отметить, что введение данного положения способствовало улучшению качества российского судопроизводства, ведь развитие современного правосудия невозможно рассматривать в отрыве от информационных технологий, но и следует не забывать о том, что проведение судебных заседаний в онлайн-режиме никак не сможет в полной мере заменить очное проведение заседания, потому что технические неполадки, перебои с интернет-питанием могут оказаться причиной уклона лица от участия в судебном онлайн-заседании, также, с точки зрения психологии, в режиме онлайн, убедительность выступающего представителя снижается, тем самым, снижается возможность убедить суд в своей позиции⁴.

Кроме того, одними из самых востребованных систем государственного электронного управления являются следующие:

1) Big Data – большие данные. Такая система применяется для принятия решений и установления последствий их принятия, в том числе в государственном управлении. Основной метод работы данной системы – метод анализа данных. Так, например, нас предупреждают о природных и техногенных катастрофах, максимально точный прогноз спасает жизни тысячи людей. Работает это следующим образом: система обрабатывает большое количество показаний датчиков и на основании этой информации помогает установить дату и место возможного катаклизма. Касаемо юриспруденции, Big data также является полезной: технология способна анализировать десятки тысяч похожих судебных дел, по ключевым словам, и давать

прогнозы даже с учетом личности судьи. Это позволяет экономить колоссальное количество времени у практикующих юристов, ведь они заранее понимают перспективы рассмотрения судебного дела.

2) Искусственный интеллект. Эта система является инструментом работы с большими данными – это нейронные сети, методы машинного обучения; кроме того, способствует эффективной работе правоохранительных органов, ведь в настоящих правовых реалиях расследование и раскрытие преступлений осуществляется путем справочных и информационно-поисковых систем, с помощью нейросети и искусственного интеллекта сотрудники правоохранительных органов могут идентифицировать преступников⁵. Так нейросети могут анализировать записи с камер видеонаблюдения и помогают в определении личности преступника по его лицу. Это значительно ускоряет и упрощает работу правоохранительных органов.

3) Система распределенного реестра – эта технология представляет собой новый подход к созданию баз данных, ключевой особенностью которого является отсутствие единого центра управления. Каждый узел составляет и записывает обновления реестра независимо от других узлов⁶. Она существенно помогает государственному управлению информацией об организациях, активах и физических лицах, также повышает защиту государственной базы данных и систем государственных услуг, снижает риск коррупции и ускоряет взаимодействие граждан с органами власти и межведомственными организациями⁷;

4) Интернет вещей (Internet of Things, IoT). Интернет вещей позволяет выявлять нарушения и контролировать условия работы в системе государственного управления. Данная система также применяется для сбора данных и мониторинга работы госорганов. Применение данной программы включает в себя и гражданско-правовые отношения. Например, различные соглашения и договоры между пользователями IoT-устройств и их операторами. В таком контексте следует обращать внимание не только на правовые требования к заключению договоров и их исполнения, но и на разрешение и регулирование самих споров, связанных с использованием «интернет вещей». Правовые особенности и характерные черты использования данных устройств

в различны, они могут зависеть как от конкретной ситуации, так и от контекста в целом. Операторы таких IoT-устройств обязаны учитывать установки и рекомендации, связанные с их деятельностью, должны соблюдать все нормативно-правовые требования для обеспечения гарантий безопасного пользования IoT-устройств в Российской Федерации и для обеспечения защиты прав пользователей.

Все указанные системы позволяют активно расширять возможности государственного управления, эффективно принимать решения, разрабатывать машиночитаемые законы и обеспечивать «прозрачность» системы органов государственного управления.

Введение новых технологий и систем для госуправления, безусловно, является фактором, обеспечивающим повышение уровня эффективности работы государственных органов. Но наряду с преимуществами возникают следующие проблемы:

1) Увеличение IT-преступлений. Технологии искусственного интеллекта позволяют злоумышленникам выдавать себя за других людей, имитируя их голос, почерк и манеру общения, что может быть использовано противоправных деяниях;

2) Проблема безработицы, снижение производительности труда и мотивации работников. С увеличением подобных систем человеческий труд может быть менее востребованным. Однако полагаем, что названные технологии еще длительное время не смогут полностью заменить человека;

3) Недостаток финансовых ресурсов для внедрения высокотехнологичных решений;

4) Слабая научно-техническая инфраструктура в Российской Федерации, которая требует серьезной модернизации и средств;

5) Отсутствие соответствующе подготовленных специалистов; слабая нормативно-правовая база для внедрения, например, технологий искусственного интеллекта.

В заключение стоит сказать, что в настоящее время российское государство активно проводит политику информатизации, повышает уровень своих технологических и информационных ресурсов, а также обеспечивает эффективную и результативную деятельность органов власти, что, в большей части способствует повышению качества жизни граждан нашей страны.

¹ Более подробно можно ознакомиться на сайте Правительства России // <http://government.ru/news/44582/>

² Постановление Правительства Российской Федерации от 15.02.2022 № 172 // Собрание законодательства РФ. – 2022. – N 8. – Ст. 1178.

³ Постановление Президиума Верховного Суда РФ, Президиума Совета судей РФ от 08.04.2020 N 821 (ред. от 29.04.2020) <О приостановлении личного приема граждан в судах> [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 15.02.2022). В настоящее время документ утратил силу с 12 мая 2020 года в связи с истечением срока действия, установленного пунктом 9 данного документа.

⁴ Савченкова Е.Н., Юлбердина Л.Р., Фадеев А.В. Онлайн-заседания в Арбитражном суде: уроки пандемии // Право и государство: теория и практика. – 2021. – №8. – С. 110-112

⁵ Степаненко Д.А., Бахтеев Д.В., Евстратова Ю.А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. – 2020. – №2. – С. 206-213.

⁶ Связанные одной цепью: как блокчейн защищает данные [Электронный ресурс] // Яндекс Практикум URL: <https://practicum.yandex.ru/> (дата обращения: 18.11.2023).

⁷ Дорожная карта развития «Сквозной» цифровой технологии «Система распределенного реестра» [Электронный ресурс] // digital.gov.ru/uploaded/files/07102019srr.pdf

*Воронежский государственный
университет
Попова Виктория Павловна
E-mail: [popovaviktoria8685@
gmail.com](mailto:popovaviktoria8685@gmail.com)*

*Voronezh State University
Popova Victoria Pavlovna
E-mail: [popovaviktoria8685@
gmail.com](mailto:popovaviktoria8685@gmail.com)*

Проценко Евгения Олеговна

Воронежский государственный университет

**РЕАЛИЗАЦИЯ ПРИНЦИПА ГЛАСНОСТИ
И ОТКРЫТОСТИ СУДЕБНОГО РАЗБИРАТЕЛЬСТВА
В УСЛОВИЯХ ЦИФРОВИЗАЦИИ
АДМИНИСТРАТИВНОГО СУДОПРОИЗВОДСТВА**

Procenko Evgeniya Olegovna

Voronezh State University

**IMPLEMENTATION OF THE PRINCIPLE
OF TRANSPARENCY AND OPENNESS
OF JUDICIAL PROCEEDINGS IN THE CONTEXT
OF DIGITALIZATION OF ADMINISTRATIVE
PROCEEDINGS**

Аннотация: статья посвящена нормативного закреплению применения новых цифровых достижений, в рамках реализации принципа гласности и открытости судебного разбирательства в административном судопроизводстве.

Abstract: the article is devoted to the normative consolidation of the application of new digital achievements, within the framework of the implementation of the principle of transparency and openness of judicial proceedings in administrative proceedings.

Ключевые слова: принципы судебного разбирательства, гласность, открытое рассмотрение дела, состязательность, административное судопроизводство, цифровой процесс.

Keywords: principles of judicial proceedings, transparency, open consideration of the case, adversarial, administrative proceedings, digital process.

В статье 6 Кодекса административного судопроизводства Российской Федерации, в перечень принципов административного судопроизводства, включен принцип открытости судебного

разбирательства, а в ч. 3, 4 ст. 11 указывается, что лица, участвующие в деле, и лица, не участвующие в деле, вопрос о правах и об обязанностях которых разрешен судом, не могут быть ограничены в праве на получение информации о дате, времени и месте рассмотрения административного дела, устной и письменной информации о результатах рассмотрения административного дела и принятых по нему судебных актах. Каждый имеет право знакомиться в установленном порядке со вступившим в законную силу судебным решением по рассмотренному в открытом судебном заседании административному делу, за исключением случаев ограничения этого права в соответствии с законом¹.

По мнению Е.Г. Стрельцовой к элементам данного принципа, как представляется, следует относить:

- право получать информацию о том, какой судья будет рассматривать дело, в том числе о замене судьи и причинах замены;
- право быть извещенным о начале процесса и его движении;
- право иметь равный и беспрепятственный доступ к материалам дела (в бумажном и электронном виде);
- право быть извещенным о вынесенных по делу судебных актах².

С указанным мнением можно согласиться, поэтому будем рассматривать данные принципы, через раскрытие составных частей.

Уже в настоящее время используется такие современные достижения, как возможность участия в судебном заседании в формате видеоконференцсвязи, оповещения сторон с помощью СМС-уведомлений, электронный документооборот³.

Однако достижения в информационной среде не стоят на месте и многие средства уже можно применять в административном судопроизводстве.

Так на XII Международном юридическом форуме стран Азиатско-тихоокеанского региона председатель Верховного суда Вячеслав Лебедев рассказал о справочном центре, разработанном с использованием искусственного интеллекта. Он работает в столичных судах общей юрисдикции. Сервис позволяет обрабатывать все телефонные обращения граждан.

Цифровые технологии помогают расширить доступ к правосудию, обратил внимание Вячеслав Лебедев, глава Верховного

суда. Он рассказал, что в 2023-м в российские суды подали более 7 млн электронных документов. По видео-конференц-связи провели более 400 000 судебных заседаний, а с применением веб-конференции – свыше 500 000.

Еще Лебедев рассказал о системе «Горячая линия Московского городского суда»: в московских судах общей юрисдикции с помощью искусственного интеллекта разработали единый справочный центр. Его сотрудники отвечают на звонки граждан, сообщают им о стадиях, на которых находится их дела, деталях заседания, составляют списки кандидатов в присяжные. Технологии позволяют отвечать на каждое обращение. Благодаря им телефон не бывает занят, объяснил глава ВС.

Однако, указанные изменения еще нормативно не закреплены в федеральных нормативно-правовых актах, а также не применяются повсеместно, в связи с недостаточной материально-технической базой в региональных судебных департаментах.

Первая проблема реализации принципа открытости судебных заседаний – это отсутствие единой цифровой платформы, транслирующей судебные заседания. В настоящее время обычным гражданам, а также лицам, участвующим деле проблематично присутствовать на открытых судебных заседаниях без посещения здания суда. Кроме того, принять участие в режиме видеоконференцсвязи возможно только в случае удовлетворения заявленного ходатайства судьей, рассматривающим дело в порядке административного судопроизводства.

Мало распространена информация о том, что в Белгородском областном суде организована регулярная онлайн-трансляция судебных заседаний апелляционной инстанции по уголовным делам с июля 2015 г. Подчеркивается, что функционирование проекта основывается на принципах соблюдения прав граждан на неприкосновенность частной жизни, личную и семейную тайну, прав и законных интересов участников судебного процесса, их безопасности. Вместе с тем выражено и стремление к сохранению баланса частных и публичных интересов, а также интересов правосудия. Для трансляции через сеть Интернет отбирается далеко не каждое дело. В этом процессе суд сам решает, какое заседание допустимо широко обнародовать, «поскольку открытое рассмотрение дел и освеще-

ние судебного разбирательства в ряде случаев может повлечь неправильное формирование общественного мнения о ходе процесса, его результатах»⁴. Китайский ученый М. Чжан провел весьма существенное исследование проблемы сетевых трансляций. По его справедливому мнению, если интернет-трансляция судебных процессов зависит только от выбора судебной администрации и используется просто как инструмент политического влияния, то она не может быть действительно индикатором открытости судебной системы, это просто новый «формализм» во главе с судом⁵.

На мой взгляд, решением проблемы будет являться дополнение платформы «Госуслуги» возможностью участвовать или присутствовать на открытых судебных заседаниях, так как данным сервисом пользуется большое количество граждан, оно удобно в использовании и подключиться можно из любого региона.

Следующая проблемой является опубликование судебных решений. И здесь снова необходимо обратить внимание на то, что все судебные решения публикуются на различных официальных сайтах судебных органов, что создает дополнительные проблемы для их поиска, а система ГАС «Правосудие» часто работает некорректно. В настоящее время в арбитражном процессе успешно используется платформа «Мой арбитр». Однако для граждан существует единая платформа «Госуслуги», на которой каждый гражданин может обратиться с заявлением о получении всех видов государственных услуг, добавление на указанную платформу опубликование всех судебных решений также упростит возможность гражданам знакомиться с судебными актами, раскроет принцип гласности, а также другие принципы административного судопроизводства.

Еще необходимо выделить проблему приобщения доказательств в ходе судебного заседания. В настоящее время стороны заблаговременно приобщают доказательства или во время судебного заседания, при этом существует большая проблема приобщения материалов сторонами, участвующими в деле с помощью системы видеоконференцсвязи.

Решением указанной проблемы, на мой взгляд будет являться дополнение приложения «Госуслуги» возможностью приобщить к материалам дела различные доказательства, пояснения и

документы, а также возможностью ознакомиться в ходе судебного заседания или во время перерыва.

Также в настоящее время административным законодательством не регламентирован точный последовательный порядок участия средств массовой информации в ходе рассмотрения дела об административном правонарушении в открытом судебном процессе.

Учитывая, что суду запрещается безосновательно препятствовать участию в судебном заседании представителей общественности, средств массовой информации, ведению ими письменных записей, а также использованию портативных аудиотехнических устройств, по мнению автора Шевченко О.А., с которым можно согласиться, необходимо детально закрепить в кодекса административного судопроизводства Российской Федерации основания для отказа средствам массовой информации в применении в зале судебного заседания фото- и видеозаписи с применением стационарной аппаратуры, а также трансляции судебного заседания по радио и телевидению. С целью реализации возможности участия в судебном процессе представителям средств массовой информации необходимо ставить суд в известность о намерении любого рода фиксации судебного процесса заблаговременно в письменном виде. При этом следует иметь в виду, что представители средств массовой информации могут быть не допущены судом на судебные заседания из соображений морали, обеспечения общественного порядка или национальной безопасности либо при рассмотрении дел на предмет, касающийся несовершеннолетних детей, поскольку гласность судебного разбирательства может нарушить интересы правосудия. Следовательно, реализация открытого судебного разбирательства и одновременно в некоторых случаях законные основания для ограничения распространения информации о некоторых деталях процесса имеют существенное значение для справедливого правосудия, так как дают возможность осмыслить суть судебного процесса, укрепить доверие к суду и повысить авторитет судебной власти⁶.

Таким образом, органами государственной власти Российской Федерации проводится большой объем мероприятий, направленный на цифровизацию всех органов власти, которые

необходимо как можно быстрее применять и закреплять в различных нормативных актах.

¹ Кодекс административного судопроизводства Российской Федерации от 08 марта 2015 года № 21-ФЗ (ред. от 24.07.2023 № 351-ФЗ)

² М.В. Самсонова, Е.Г. Стрельцова, А.В. Чайкина и др. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы // Изд.. Инфотропик Медиа, 2022. СМ.: 336 с.

³ Федеральный закон от 24.07.2023 № 349-ФЗ «О внесении изменений в Кодекс административного судопроизводства Российской Федерации»

⁴ Тонков В.Е., Сазонова И.А. Интернет-трансляция судебных заседаний: обеспечение сбалансированности принципов гласности и открытости судопроизводства и иных принципов, действующих в стадии судебного разбирательства // Вестник судейского сообщества Белгородской области. 2016. N 5

⁵ Чжан М. Активно или осторожно? Ограничения судебных слушаний в прямом эфире.

⁶ Шевченко О.А., Труфанов В.А. Реализация принципов гласности и состязательности в ходе судебного разбирательства при рассмотрении дела об административном правонарушении // Административное право и процесс. 2022. N 12. С. 49–51.

*Воронежский государственный
университет
Проценко Евгения Олеговна
E-mail: lukashevich333@mail.ru*

*Voronezh State University
Procenko Evgeniya Olegovna
E-mail: lukashevich333@mail.ru*

Садкеева Дарья Дмитриевна

Саратовская государственная юридическая академия

**ПРАВОВАЯ ОХРАНА
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
В СФЕРЕ ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА**

Sadkeeva Darya Dmitrievna

Saratov State Law Academy

**LEGAL PROTECTION
OF INTELLECTUAL PROPERTY IN THE FIELD
OF PHYSICAL CULTURE AND SPORTS**

Аннотация: в статье рассмотрена актуальность и роль интеллектуальной собственности в условиях развития цифровой экономики. Авторами приведены основные правовые институты защиты прав на объекты интеллектуальной собственности, выявлены основные пробелы правового регулирования данной области правоотношений. В завершение, сформулированы направления совершенствования законодательной базы.

Abstract: the article examines the relevance and role of intellectual property in the context of the development of the digital economy. The authors present the main legal institutions for the protection of intellectual property rights, identify the main gaps in the legal regulation of this area of legal relations. Finally, the directions for improving the legislative framework are formulated.

Ключевые слова: интеллектуальная собственность, спорт, ноу-хау, имидж, спортсмены.

Keywords: intellectual property, sport, know-how, image, athletes.

Развитие цифровой экономики способствует трансформации уже существующих и появлению новых институтов права. Одним из драйверов научно-технического прогресса на современном этапе выступает интеллектуальная собственность.

Правовая регламентация и защита объектов интеллектуальной собственности являются важнейшими направлениями работы правоведов. В современном мире полным ходом идет коммерциализация отраслей общественной жизни, исключением не стала сфера физической культуры и спорта. На сегодняшний день в Российской Федерации нормативное регулирование прав на объекты интеллектуальной собственности в области спорта не совершенно.

Концептуальной основой работы является понятие интеллектуальной собственности, закрепленное в ст. 138 ГК РФ¹. На национальном уровне защита и охрана объектов интеллектуальной собственности регламентируется Конституцией РФ², а именно статьями 44 и 71, ч. 4 Гражданского кодекса Российской Федерации, федеральными законами и специализированными нормативно-правовыми актами об отдельных видах объектов интеллектуальной деятельности.

На международном уровне основными источниками прав на интеллектуальную собственность в сфере спорта являются Всемирная (Женевская) конвенция об авторских правах, Соглашение о международной классификации товаров и услуг для регистрации знаков, Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций и другие³.

Гражданский кодекс регулирует правоотношения в сфере интеллектуальной собственности посредством института авторского права и смежных прав; института патентного права; института средств индивидуализации участников гражданского оборота и производимой ими продукции; института особых объектов права интеллектуальной собственности⁴.

Все эти институты в той или иной мере имеют проявление и в спортивной сфере, в рамках которой либо непосредственно создаются, либо привлекаются извне в качестве уже созданных объекты интеллектуальной собственности (произведения, изобретения, товарные знаки). Информатизация внесла свои коррективы в правовое регулирование данных институтов.

К числу объектов авторских и смежных прав в области спорта относятся хореографические произведения. В качестве самостоятельного объекта правовой охраны авторских прав могут

выступать хореографические номера, спортивные номера, танцевальные композиции в фигурном катании, художественной гимнастике и синхронном плавании.

Во избежание неправомерного использования авторских произведений прибегают к детальному описанию хореографического произведения с помощью фото и видео-регистрации.

В отдельных случаях права на использования музыкально-го произведения передаются от его автора спортивной организации на основе договора или соглашения. Так же под защиту авторских прав согласно письму Министерства спорта РФ от 27.07.2017 N ПН-05-10/5493⁵ попадают аудиовизуальные произведения, произведения графики и дизайна. Защита и охрана первых в основном связана с их использованием в рекламных целях. Дизайн и графика выступают сопровождающим элементом любых крупных спортивных мероприятий.

Объекты патентного права активно задействованы в области спорта. К ним в частности относятся изобретения, промышленные образцы и полезные модели. В качестве изобретения рассматривается новое решение творческого характера, содержащее в себе новизну и изобретательскую составляющую. К ним можно отнести Очки «Reson Jet» – умные очки с виртуальным экраном или лазерную футбольную площадку от NIKE. Полезной моделью называют объекты нематериального мира, которые несут собой техническое решение. Полезной моделью можно считать разработанные модели лыжных палок обтекаемой формы, гольфийских клюшек из секретного практически невесомого материала и другие.

Определение промышленного образца дается в ст. 1132 ГК РФ. На сегодняшний день, благодаря патентованию в качестве промышленного образца фирменной символики и атрибутики спортивных клубов и мероприятий, можно не боясь конкуренции производить и продавать спортивную одежду и сувениры с запатентованными объектами.

Объектами защиты посредством института средств индивидуализации участников гражданского оборота и производимой ими продукции являются товарные знаки и фирменные названия. Законодатель раскрывает понятие товарного знака в статье 1477 ГК РФ. Самыми часто нарушаемыми в области спорта являются

права на товарные знаки. В основном партии с контрафактной продукцией поступают в Россию из стран Средней Азии и Ближнего Востока и реализуются на территории РФ по более низкой цене, чем оригинал или в качестве оригинала. Наиболее копируемыми являются такие бренды как «Reebok», «Adidas», «Nike».

Важнейшим институтом в области спорта, в условиях цифровизации, по праву, можно считать особые объекты права интеллектуальной собственности. Ноу-хау или секретом производства может быть любая информация о результатах научно-интеллектуальной технической деятельности о методах осуществления профессиональной деятельности, обладающей коммерческой стоимостью или ценностью. К примеру, многие спортивные клубы запрещают журналистам и вообще посторонним людям наблюдать за процессом тренировок спортсменов, опасаясь распространения информации и раскрытия особых методик, которые применяют тренеры команд. Так было в 2018 году на Олимпийских играх в Пхенчхане, когда руководство одной из хоккейных команд не пустило сотрудников СМИ снять репортаж о тренировках канадских спортсменов.

Несовершенство законодательства регулирования интеллектуальной собственности в области спорта наблюдается во всех странах мира. Одним из ярких пробелов в Российском законодательстве можно считать отсутствие в нем закрепленных понятий "имиджевых прав" или "имиджа". В современном мире спортсмены давно стали частью маркетинговых компаний, в связи с этим приобретают большую важность в сфере регулирования отношений по поводу интеллектуальной собственности так называемые «имиджевые права».

"Имиджевые права" спортсменов включают в себя, права на коммерческое использование облика, образа, имени и иных аспектов личной идентичности спортсмена. В общемировой практике указанные элементы "имиджа" спортсмена регистрируются в качестве товарных знаков. Имиджевые права подразумевают под собой права, которые спортсмен приобрел в результате профессиональной деятельности и которые направлены на защиту его деловой репутации, имени, неприкосновенности частной жизни и других благ нематериального характера и результатов творческой и интеллектуальной деятельности.

Продвижение средств индивидуализации спортсменов связано с их коммерческой выгодой от сотрудничества в рамках рекламных кампаний спортивных мероприятий. Обычно такие права спортсменов контролируются на договорной основе профессиональными спортивными организациями, в которых спортсмены осуществляют свою деятельность.

Одним из наиболее эффективных способов использования имиджевых прав спортсменов является продвижение с их помощью какой-либо продукции (например, позитивная реклама одобрения и продукции спортсменами)⁶.

В заключение вышесказанного отметим, что в связи с коммерциализацией объектов интеллектуальной собственности в спортивной сфере и быстрого развития цифровой экономики возникает множество правовых проблем, для решения которых необходимо усовершенствование законодательной базы, регулирующей отношения участников спортивной деятельности, в процессе которой могут возникать интеллектуальные права создателей и исполнителей спортивных произведений. Необходимо добавить в часть IV ГК РФ статью, посвященную правовой охране и защите объектов интеллектуальной собственности в спорте, или издать НПА, регулирующий данный вопрос более подробно, решить иные связанные с рассмотренным предметом вопросы законодательного и правоприменительного характера.

¹ Гражданский кодекс Российской Федерации // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 15.10.2023).

² Конституция Российской Федерации // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 15.10.2023).

³ Агамагомедова, С. А. Развитие института интеллектуальной собственности в условиях цифровизации экономики / С. А. Агамагомедова, Н. А. Надькина // Известия высших учебных заведений. Поволжский регион. Экономические науки. – 2019. – № 1(9). – С. 4-16. – DOI 10.21685/2309-2874-2019-1-1. – EDN KGBVYX. / (дата обращения: 15.10.2023).

⁴ Воеводина, С. С. Интеллектуальная деятельность в условиях глобализации спортивных отношений / С. С. Воеводина, И. А. Бушин // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2020. – № 3. – С. 806-810. – EDN LABOTU. / (дата обращения: 15.10.2023).

⁵ Министерство спорта Российской Федерации. Письмо от 27 июля 2017 г. N ПН-05-10/5493 // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_278359/ (дата обращения: 15.10.2023).

⁶ Рахимов, А. А. Коммерциализация интеллектуальной собственности в сфере физической культуры и спорта / А. А. Рахимов // Физическое воспитание и студенческий спорт глазами студентов : Материалы VI Международной научно-практической конференции, Казань, 13–14 ноября 2020 года / Под редакцией Р.А. Юсупова, Б.А. Акишина. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2020. – С. 605-607. – EDN MLEHEY. / (дата обращения: 15.10.2023).

*Саратовская государственная
юридическая академия
Садкеева Дарья Дмитриевна
E-mail: sadkeeva.03@mail.ru*

*Saratov State Law Academy
Sadkeeva Darya Dmitrievna
E-mail: sadkeeva.03@mail.ru*

Сарычева Александра Сергеевна

Воронежский государственный университет

ЦИФРОВЫЕ СЛЕДЫ ПРЕСТУПЛЕНИЯ

Saricheva Alexandra Segeevna

Voronezh State University

DIGITAL TRACES OF CRIME

Аннотация: многофункциональность и постоянное совершенствование цифровых устройств только расширяют пользовательские и криминалистические возможности. В статье рассматривается понятие цифровых следов, а также проводится исследование возможных способов работы со следами при раскрытии преступлений. Кроме того, в работе анализируется классификация цифровых следов, для полного понимания природы и сущности объекта.

Abstract: the versatility and continuous improvement of digital devices only expand user and forensic capabilities. The article examines the concept of forensic traces, as well as analyzes possible ways to work with traces in solving crimes. In addition, the paper analyzes the classification of digital footprints for a complete understanding of the nature and essence of the object.

Ключевые слова: цифровые следы, нахождение и преобразование данных, информация.

Keywords: digital traces, finding and converting data, information.

Человек на протяжении всей своей жизни при взаимодействии с окружающим миром оставляет различные следы: рук, ног, обуви, зубов, одежды. Как отпечатки пальцев рук помогают в идентификации преступника, так и цифровой след помогает определить потенциального преступника и изобличить его в совершении правонарушений.

Компьютерными технологиями пронизаны все сферы человеческой деятельности. Каждый пользователь сети, оставляя

следы своих действий, потенциально находится в опасной зоне деятельности преступников.

Исходя из криминалистического понимания цифровых следов, наиболее подходящее определение, на наш взгляд, дано Е.Р. Россинской и И.А. Рядовским, по мнению которых "цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи"¹. Сходное определение выведено в монографии А.М. Багмета, В.В. Бычкова, С.Ю. Скобелина, Н.Н. Ильина: "Цифровой след – любая криминалистически значимая компьютерная информация, представленная в форме электрических сигналов, независимо от средств их хранения, обработки и передачи"². Следует заметить, что в указанных определениях авторы описывают цифровой след как некую информацию, существующую в материальной среде. Однако для точного определения цифрового следа, следует ввести более конкретизированное понятие. Под цифровым следом, на наш взгляд, следует понимать результаты уникальных действий пользователей, произведенных в информационной среде, при помощи которых можно определить обстоятельства совершенных преступлений и выявить связь с субъектом преступного посягательства.

Для полного понимания сущности цифрового следа, представляется возможным проанализировать автореферат Красновой Л.Б., где представлена классификация следов преступлений, совершаемых с помощью компьютерной техники. Автор приходит к выводу о возможности деления следов на первичные и вторичные.

Под первичными следами понимаются следы, образующиеся непосредственно при воздействии на предмет посягательства – компьютерную информацию. Это может быть модификация, удаление или копирование данных или программ. К примеру, создание вредоносной программы для изобличения данных пользователей сайта, с возможностью последующего использования этих данных в корыстных целях.

Под вторичными следами понимаются следы, образующиеся не на предмете посягательства, а возникающие на других, не являющихся предметами посягательства объектах, вследствие это-

го воздействия. К вторичным следам относятся изменения файловых характеристик при изменении его содержимого. Простым примером может являться изменение содержания некоего файла для сокрытия первоначальной информации.

Принципиальное различие этих групп следов состоит в механизме следообразования. Первичные следы являются следствием непосредственного воздействия пользователя, с использованием какой-либо информационной технологии, а вторичные являются следствием воздействия технологических процессов без участия человека и вне его желания³.

На наш взгляд такая классификация полностью оправдана, в связи со сложными процессами, происходящими при возникновении следов, а также с последующей трансформацией данных на различных носителях.

Для работы с такими следами криминалистам следует понимать, что цифровые следы являются следами материальными, так как, будучи оставленными в результате определенных событий, отражаются на материальных объектах, хотя в некоторых случаях период их существования весьма невелик. Проблема временного сохранения следов стоит очень остро, ведь с развитием технологий у злоумышленников появляются новые варианты сокрытия и переброса информации на другие носители, а также на носители с удаленным доступом, что, несомненно, считается осложнением в ходе расследования преступлений.

По происхождению цифровые следы являются технологическими, поскольку формирование данных следов обусловлено спецификой реализации информационных технологий. Информационная составляющая становится доступной для восприятия только после их интерпретации с помощью прикладного программного обеспечения и с использованием средств вывода⁴.

Обнаружение и фиксация цифровых следов является основной задачей криминалистов. Вне зависимости от вида расследуемого преступления, наиболее значимыми мероприятиями по обнаружению, сбору и фиксации таких следов связаны с осмотром места происшествия и с осуществлением выемки материалов, содержащих нужную для расследования информацию⁵.

В связи с произведенным анализом можно говорить о специфических неотложных действиях. Таковыми они считаются по-

сколько используются в интересах раскрытия, расследования преступления и установления истины по делу. Как правило, необходимо производство следственных действий, направленных на выявление следов в оперативной памяти компьютера, на носителях информации различных типов. Особенность таких следов заключается в том, что они имеют высокую скорость преобразования, легко уничтожаются и модифицируются, могут быть представлены многочисленными копиями.

Для обнаружения, сбора и фиксации данных, в том числе на месте происшествия, имеются специальные программы, способные исследовать и фиксировать цифровые следы. Среди таких программных комплексов широко используются UFED, XRY, «Мобильный криминалист»⁶.

Функционал первых двух направлен на извлечение, восстановление и декодирование информации с различных устройств. Анализ полученных данных, возможность дешифровки мессенджеров, а также извлечение нужных сведений из облачных хранилищ. Указанные программы в применении у следователей используются для ускорения процесса обработки данных и упрощения работы криминалистов.

В статье была совершена попытка формулирования более конкретного понятия цифровых следов, в отличие от общеизвестных, что на наш взгляд может помочь в более точном толковании термина, а соответственно и в понимании процессов образования таковых следов. Как мы уже выяснили, следовая картина преступлений имеет свою уникальную специфику. Для работы криминалистов с такого рода следами требуется тщательный анализ большого количества данных для улучшения понимания мотивов преступника, а также учитывать растущий объем информации, собираемой в ходе цифровых расследований. В конечном счете, единые усилия по решению задач цифрового расследования создают большие возможности для поддержания безопасного и стабильного общества.

¹ Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы: Республикасы ИИМ М. Есболатов Алматы. 2019. С. 7.

² Бояркина Л.А., Бояркин В.В. Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ "Социосфера". 2016. N 62. С. 79.

³ Краснова Л.Б. Электронный документ как объект криминалистических исследований/ Л.Б. Краснова, Т.Э. Кукарникова// Юридические записки. – Воронеж: Изд-во Воронеж, гос ун-та, 1999. – Вып. 10: Криминалистические средства и методы исследования преступлений. – С. 199-206.

⁴ Багмет А.М., Бычков В.В., Скобелин С.Ю., Ильин Н.Н. Цифровые следы преступлений: монография. М.: Проспект, 2021. 168 с.

⁵ Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. N 4. С. 42–44.

⁶ Рогава И.Г., Асулян Н.М. Особенности обнаружения цифровых следов при расследовании преступлений, совершаемых с использованием цифровых технологий.

*Воронежский государственный
университет
Сарычева Александра Сергеевна
E-mail: as21072002@gmail.com*

*Voronezh State University
Sarycheva Aleksandra Sergeevna
E-mail: as21072002@gmail.com*

Сульдина Елизавета Дмитриевна

Саратовская государственная юридическая академия

**ПОНЯТИЕ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ
КИБЕРТЕХНИЧЕСКИХ ПРЕСТУПЛЕНИЙ
В УГОЛОВНОМ ПРАВЕ РФ**

Suldina Elizaveta Dmitrievna

Saratov State Law Academy

DIGITAL TRACES OF CRIME

Аннотация: в данной статье даётся характеристика состояния и возможных направлений совершенствования уголовного законодательства в сфере борьбы со специфическим видом преступлений – киберпреступлениями. Особое внимание уделено различной направленности данных преступлений, так же была проанализирована входящая в данную категорию дел, преступления, связанные с использованием компьютерных технологий. И в конечном итоге был сделан вывод о том, что уголовный кодекс РФ требует совершенствования в данной сфере.

Abstract: this article describes the state and possible directions for improving criminal legislation in the field of combating a specific type of crime – cybercrime. Special attention is paid to the various directions of these crimes, as well as the crimes related to the use of computer technologies included in this category of cases were analyzed. And in the end, it was concluded that the Criminal Code of the Russian Federation requires improvement in this area.

Ключевые слова: кибертехническое преступление, кибертехнологии, сеть «Интернет», киберпространство.

Keywords: cybertechnical crime, cybertechnology, the Internet, cyberspace.

Исходя из современного понимания кибернетики, применение кибернетических технологий можно представить как сложную систему, включающую социальные и технические па-

раметры, наиболее важные из которых, соответствуют основным областям глобальных систем управления. В частности это возможность эффективного управления, передачи и обработки информации, использование компьютерных систем и комплексов, тесная связь кибертехнологий с человеческим интеллектом и неограниченные возможности развития и технологической трансформации.

К сожалению, понятие "кибер" нельзя найти в статьях Уголовного кодекса РФ, а существующие положения уголовного законодательства касаются только малой части такого объемного понятия, то есть вопросов информационных технологий или использования компьютерной техники, что не придает этой сфере значимости в реализации уголовной политики.

Для начала рассмотрим подробнее блок преступлений, связанных с использованием компьютерных технологий, которые, конечно же, включают широкий спектр действий, но не являются исчерпывающими. Некоторые из них могут быть связаны с компьютерными системами, такими как кража или мошенничество, в то время как другие могут использовать компьютеры только в качестве средства передачи или приема информации при передвижении по интернет-сетям. В эту категорию также входят вредоносные действия, напрямую связанные с компьютерами, например, взлом устройства или пользовательских данных на конкретном устройстве. Данные запреты, содержащиеся в законодательстве, а точнее в главе 28 УК РФ¹, направлены на предотвращение общественно опасных действий, которые могут угрожать безопасности компьютерной информации и систем ее обработки.

Законы, посвящённые регулированию правонарушений с использованием компьютерных средств, наиболее часто содержат следующий перечень ограничения действий пользователя: запрет на неправомерный доступ к компьютеру, системе или Сети; изменение повреждение, использование, раскрытие, копирование или получение программ, или данных; введение вируса или другого загрязнителя в компьютерную систему; использование компьютера в схеме мошенничества; вмешательство в систему чужого компьютерного устройства или его использование; использование шифрования для совершения преступления; фаль-

сификация информации об источнике электронной почты; кража услуг сети-провайдера.

Выделим предмет данной группы преступлений, как не странно им выступает сама компьютерная информация, что вытекает из сути противоправных деяний, установленных в ст. 272, 273 и 274 УК РФ. Во вторую же группу преступлений следует определить те преступления, где компьютерная информация служит средством совершения преступления. К преступлениям, составы которых находятся в других разделах уголовного закона, можно отнести преступления: в форме мошенничества, совершенные в области компьютерной информации (ст. 159.6 УК РФ); связанные с незаконной организацией и проведением азартных игр, использующих информационно-коммуникационные сети, включая «Интернет» (ст. 171.2 УК РФ); преступления, связанные с манипулированием рынком, в том числе с использованием электронных, информационно-коммуникационных сетей (включая «Интернет») посредством распространения заведомо ложной информации; вопросы квалификации хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств информации или совершения операций с иностранной валютой, финансовыми инструментами или товарами (ст. 185.3 УК РФ); связанные со сбытом наркотических средств, психотропных веществ или их аналогов, совершенные с использованием электронных или информационно-коммуникационных сетей (включая «Интернет») (ч. 2 ст. 228.1 УК РФ); связанные с изготовлением или распространением порнографических материалов с использованием информационно-коммуникационных сетей (включая «Интернет») (ч. 2 ст. 242.2 УК РФ), а также ряд иных составов.

Мы рассмотрели небольшой блок деяний, входящий в кибертехнические преступления, но в связи с развитием кибертехнологий, возникает все больше преступлений, связанных с использованием компьютерной информации, которые не попадают под составы, находящиеся в главе 28 УК РФ. В таких случаях, компьютерная информация не является объектом преступления, а используется для достижения целей преступника. Примерами таких преступлений могут быть незаконный доступ к компью-

терным системам, распространение вредоносного программного обеспечения, хакерские атаки и другие подобные действия.

Так же стоит заметить некий недочет со стороны законодательства. На данный момент уже существует ряд преступлений, которые сейчас можно отнести к преступлениям в сфере компьютерной информации, хотя они не предусматривают использование компьютеров или информационно-коммуникационных сетей (включая «Интернет»). Такие преступления могут иметь негативное информационное воздействие, но не направлены на хищение, уничтожение или изменение определенной информации. В результате, количество преступлений, которые могут быть совершены с использованием кибернетических технологий, значительно больше, чем представлено в действующем Уголовном кодексе РФ, даже если использование таких технологий явно оговорено законом. Таким образом, кибертехнологичная криминальная активность имеет разнообразную направленность и затрагивает большинство групп охраняемых уголовным законом общественных отношений. Она также повышает уровень общественной опасности по сравнению с аналогичными некомпьютерными преступлениями, так как затрагивает безопасность информационно-коммуникационных систем.

Раскрывая сущность кибернетической преступности в Российской Федерации, следует отметить несколько ключевых аспектов, которые полностью характеризуют ее как явление социальной действительности. Кибернетическая преступность представляет собой особую форму преступности в России, которая существует наравне с другими видами преступности. Так же данная категория дел тесно связана с иными видами преступлений в России, поскольку кибернетические преступления часто включают в себя использование методов совершения других уголовно наказуемых действий. Одним из основных отличительных признаков этого вида преступлений является его высокотехнологичный характер, который определяется использованием современных кибертехнологий, информационно-коммуникационных сетей, различных компьютерных устройств и носителей компьютерной информации и т.д., которые обычно используются в качестве средств для совершения таких преступлений².

Высокая степень скрытности различных видов киберпреступлений является серьезным фактором, затрудняющим как предотвращение, так и борьбу с ними. Это в значительной степени обусловлено объективными факторами, такими как нежелание жертв обращаться за защитой к правоохранительным органам, незаметность компьютерных преступлений для большинства населения из-за их совершения в киберпространстве, а также сложность выявления таких преступлений и т.д.

Еще одним отягощающим фактором является, что Кибернетическая преступность развивается благодаря ее высокой организованности и связи с организованной преступностью. Множество киберпреступлений, таких как DDoS-атаки, банкинг, фишинг и создание ботнетов, совершаются организованными преступными группами, члены которых являются профессиональными специалистами. Это происходит потому, что лица, занимающиеся киберпреступлениями, имеют специализацию в компьютерных преступлениях и не совершают других видов преступлений. Они получают доход только от этого вида преступной деятельности, обладают необходимыми знаниями, навыками и умениями в области компьютерных технологий. Они также устанавливают понятия, терминологию, правила поведения и специфические законы, чтобы общаться, обмениваться опытом и находить соответствующих единомышленников.

Так же стоит отметить, что киберпространство существует за пределами государственных границ и, будучи общедоступным, позволяет преступникам, находящимся на территории одной страны, совершать преступления в отношении граждан других стран. Таким образом, киберпреступность имеет транснациональный характер, поскольку компьютерные преступники, чтобы получить преступные доходы и облегчить совершение преступлений на территории нескольких стран, вынуждены объединяться в международные преступные группировки, независимо от своей национальности.

Такие свойства киберпреступности указывают на сложность системы ее реализации, которая постоянно развивается и совершенствуется благодаря постоянному улучшению существующих и созданию новых кибертехнологий, привлечению новых участников в информационные сообщества, расширению структуры

киберпространства за счет увеличения числа пользователей в Интернете, развитию сети мобильных устройств и систем электронного документооборота в организациях и предприятиях. Кроме того, киберпреступность приобрела черты экономической преступности, так как преступления совершаются в финансовой, банковской или корпоративной сферах (интернет-банкинг, кибервымогательство, банковский фишинг и т.д.), а главной целью стала извлечение прибыли.

Особая опасность киберпреступности заключается в том, что она может превратиться в политическую преступность. Это связано с растущей активностью хакерских групп, спецслужб и военных структур из других стран, международных экстремистских и террористических организаций. Они осуществляют DDoS-атаки на правительственные сайты, кибершпионаж в отношении информационных систем государственных органов, оборонно-промышленных предприятий и российских дипломатических представительств. Они также распространяют экстремистскую информацию в Интернете и вербуют новых членов в террористические организации и т.д.³.

Хотя российское уголовное законодательство не всегда гибкое, оно стремится заполнить пробелы в правовом регулировании. В конце 2011 года – начале 2012 года были внесены поправки в уголовное законодательство России, чтобы устранить противоречия и привести правовые нормы в соответствие с практическими требованиями. Федеральным законом от 7 декабря 2011 года № 420 "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" были существенно изменены положения главы 28 УК РФ "Преступления в сфере компьютерной информации". Кроме того, Федеральный закон от 29 февраля 2012 года № 14 "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации в целях усиления ответственности за преступления сексуального характера, совершенные в отношении несовершеннолетних" добавил новый квалифицирующий признак в статью 242.1 УК РФ – "совершение преступления с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть "Интернет")".

Важным моментом в преступлении, связанном с использованием кибернетических технологий, стало вступление в силу Федерального закона от 29 ноября 2012 года № 207 "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации", который включал ряд новых составов преступлений, таких как мошенничество с использованием платежных карт (ст. 159.3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Примером адекватной реакции на развивающуюся преступную практику в этой области стало появление новых норм в Уголовном кодексе РФ, которые включали квалифицирующий признак использования электронных или информационно-телекоммуникационных сетей (включая Интернет) в ряде статей уголовного законодательства⁴.

Таким образом, подводя итоги и основываясь на вышесказанном, в первую очередь считаю важным дать понятие кибертехнических преступлений – это противозаконная деятельность, связанная с информационными ресурсами, при которой кибертехнические средства выступают либо как объект совершения преступления, либо как субъект непосредственного воздействия.

Так как в данное понятие входят и компьютерные технологии, стоит предположить, что будет уместно переименовать главу 28 УК РФ и ввести новые понятия, связанные уже с кибертехнологиями. В частности стоит обратить внимание на преступления с использованием искусственного интеллекта. Но сложность состоим в том, что в данном случае отсутствует комплексное представление о возможных средствах, способных обеспечить достижение преступной цели, и недостаточное правовое закрепление терминологического аппарата в российском уголовном законодательстве.

Поэтому при дальнейшем совершенствовании положений Уголовного кодекса РФ, касающихся ответственности за киберпреступления, необходимо тщательно мониторить киберпространство для определения реальной ситуации с использованием кибертехнологий и выявления потенциально опасных направлений их применения в общественной жизни. Это позволит разрабатывать эффективные меры контроля киберпространства с учетом возможных законодательных изменений и максимально

использовать потенциал уголовного законодательства для борьбы с преступлениями, связанными с использованием кибернетических технологий и защиты интересов государства, общества и граждан

¹ "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 30.12.2023)

² См.: Д.В. Пучков, Состояние уголовно-правового регулирования киберпреступлений в уголовном законодательстве Российской Федерации

³ Скларов Сергей Валерьевич, Евдокимов Константин Николаевич Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. №2.

⁴ Рарог А. И. Пробелы в уголовном законодательстве России // Пробелы в российском законодательстве. 2008. №1.

*Саратовская государственная
юридическая академия
Сульдина Елизавета Дмитриевна
E-mail: suldina.elizaveta@yandex.ru*

*Saratov State Law Academy
Suldina Elizaveta Dmitrievna
E-mail: suldina.elizaveta@yandex.ru*

Трофимова Мария Юрьевна

Воронежский государственный университет

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДОГОВОРОВ
КУПИ-ПРОДАЖИ НА МАРКЕТПЛЕЙСАХ**

Trofimova Maria Yuryevna

Voronezh State University

**LEGAL REGULATION OF PURCHASE
AND SALE AGREEMENTS IN MARKETPLACES**

Аннотация: статья посвящена анализу новелл правового регулирования приобретения товаров на маркетплейсах, заключения договора купли-продажи дистанционным способом, в частности, подтверждения факта купли-продажи, правовому регулированию отдельных IT-решений, связанных с приобретением товаров и способам защиты.

Abstract: the article is devoted to the analysis of novelties of the legal regulation of the purchase of goods in marketplaces, the conclusion of a purchase and sale agreement by remote means, in particular, confirmation of the fact of purchase and sale, the legal regulation of individual IT-solutions related to the purchase of goods and methods of protection.

Ключевые слова: гражданское законодательство, маркетплейс, регулирование купли-продажи, новеллы законодательства, it-регулирование на маркет-плейсах, защита интересов российских граждан, цифровое право, дистанционная торговля.

Keywords: civil legislation, marketplace, regulation of purchase and sale, new legislation, it regulation on market places, protection of the interests of Russian citizens, digital law, remote trading.

В настоящее время все большее количество сделок по приобретению различных товаров и услуг происходит дистанционно через интернет-магазины (маркетплейсы) такие, как «СберМегаМаркет», «Яндекс.Маркет», «Wildberries», «Ozon» с применением

достижений в информационной среде. Приобретение товаров дистанционным способом позволяет сэкономить время, а также увеличивает возможность купить товары из заграницы.

С ростом дистанционных продаж в законодательство Российской Федерации вносится все больше изменений, связанных с заключением договора купли-продажи сторонами удаленно.

Так, например, в 2019 году ст. 160 Гражданского кодекса Российской Федерации дополнена положениями, касающимися заключения сделок в письменной форме с помощью электронных либо иных технических средств, позволяющих воспроизвести содержание сделки на материальном носителе в неизменном виде. При этом для подписи может быть использован любой способ, позволяющий достоверно определить лицо, выразившее волю¹. А ранее в 2018 году в Законе о защите прав потребителей появились нормы, касающиеся владельцев агрегаторов информации о товарах и услугах, чем, по сути, в большинстве своем и являются маркетплейсы².

Однако, несмотря на удобство приобретения товаров и услуг на интернет-площадках, существуют некоторые проблемы правового регулирования купли-продажи товаров дистанционным способом, в том числе и через маркетплейсы.

К таким проблемам можно отнести, например, неправильную квалификацию правоотношений между продавцом, покупателем и агрегатором, аннулирование заказа продавцом или самой площадкой без наличия на то должных оснований, а также покупку товаров на маркетплейсах третьими лицами без согласия на это граждан-владельцев аккаунтов. Одни проблемы связаны непосредственно с заключением договора, другие – с его исполнением.

Анализируя судебную практику по спорам, связанным с качеством товаров, приобретенных в интернет-магазинах, видится, что у потребителей могут возникать сложности из-за выбора надлежащего ответчика. При этом единообразной практики по этому вопросу тоже нет.

Так, в одних случаях суды считают обоснованным взыскать деньги непосредственно с маркетплейса (решение мирового судьи судебного участка № 332 Бабушкинского района г. Москвы от 26.05.2017 дело 2-234/2017³, апелляционное опреде-

ление Белгородского областного суда от 16.03.2021 дело 33-1341/2021⁴), в других – напрямую с продавца (определение Шестого кассационного суда общей юрисдикции от 08.11.2021 дело 88-23859/2021⁵, определение Шестого кассационного суда общей юрисдикции от 08.11.2021 дело 88-22746/2021⁶).

При этом неочевидной для потребителя является ответственность иных субъектов, а не самого маркетплейса, поскольку интерфейс интернет-площадки, а также информация, предоставляемая потребителю агрегатором, может не позволять точно определить, с кем и о чем им заключается договор. Кроме того, потребитель может совершать оплату за товар именно в адрес владельца агрегатора как платёжного агента, а также вступать в переписку со специалистами технической поддержки самого маркетплейса и невольно заблуждаться о лице, с которым им, по его мнению, заключается договор купли-продажи.

Решением данной проблемы видится императивное закрепление за владельцами агрегаторов обязанности указывать в доступной и наглядной форме помимо информации о продавце еще и информацию о лице, уполномоченном принимать претензии, связанные с качеством товаров. Также нелишним будет установить требования к интерфейсу подобных сервисов, закрепляющих нормы использования мелкого и нечитаемого шрифта, мест размещения текста оферты, правил пользования сервисом и т.д.

Другой важной проблемой, вытекающей из квалификации правоотношений с потребителем, является аннулирование заказа продавцом или площадкой.

Под аннулированием чаще всего понимается односторонний отказ продавца или площадки от исполнения договора, что в соответствии со статьями 310, 426, 450.1 ГК РФ не допускается.

Так, в обоснование такой отмены заказов интернет-площадка может ссылаться на технические сбои, невозможность доставки, отсутствие товара на складе, что по большому счету не влияет на установленный законом запрет отказываться от заключенного договора.

Ярким примером может послужить нашумевший спор гражданина с ЦУМом, который заказал товары через интернет по цене в 846 раз ниже фактической, а магазин сообщил о невозможности доставки товара и отменил заказ. При этом сам граж-

данин настаивал на исполнении заключенного им с магазином договора⁷.

Верховный суд отметил, что характер технического сбоя и установление вины самого магазина в таком сбое имеет значение для правильного разрешения дела. Кроме того, важным является сам факт заключения договора, и на каких условиях он был заключен.

Так, Второй кассационный суд общей юрисдикции, рассматривая дело об отмене продавцом предоплаченного заказа, указал, что предплата является акцептом оферты, договор сторонами был заключен, и покупатель вправе потребовать передачи предоплаченного товара, а односторонний отказ лица, обязанного заключить публичный договор, от его исполнения не допускается⁸.

Кроме того, учитывая характер правоотношений между всеми участниками интернет-торговли, также остается открытым вопрос о субъекте ответственности и праве маркетплейса самостоятельно отменять заказы, продавцом которых он не выступает.

При этом каждая конкретная ситуация сводится к нахождению определённого баланса интересов продавца и покупателя. И аннулирование заказа покупателя не всегда связано с злоупотреблением именно со стороны продавца или маркетплейса. Однако, в любом случае, оферта маркетплейса является по сути договором присоединения, поскольку его условия не определяются совместно с потребителем, и площадка несет повышенную ответственность за соответствие ее положений закону.

Отдельно стоит проблема заключения договоров купли-продажи на маркетплейсах от лица граждан без их согласия.

Так, Верховных в своем решении от 31.08.2023 по делу N АКПИ23-703 указывает на проблему совершения сделок третьим лицом от имени другого, что причиняет материальный ущерб гражданину, через чей аккаунт совершаются сделки⁹. При этом факт заключения сделки иным лицом сложно доказуем. Как правило, потерпевшие обращаются в правоохранительные органы для поиска лица, совершившего указанное правонарушение. Таким образом, в настоящее время актуальным является вопрос о правовой защите аккаунтов покупателей.

Одним из возможных решений подобной проблемы может стать, например, двухфакторное подтверждение заказа. Первым рубежом является подтверждение заказа с использованием элементов интерфейса на самом маркетплейсе, а втором, например, – введение специального кода, который поступает покупателю по СМС на подтверждённый номер телефона или электронную почту.

Также подтверждение заказа, а равно и заключение договора возможно с использованием электронно-цифровой подписи. В настоящее время существует несколько сервисов, позволяющих сгенерировать одноразовую электронную подпись, например, «Норарет» или государственный «Госключ».

Указанные способы позволяют подтвердить факт приобретения товаров, а также дополнительно снизить возможность совершения противоправных действий, связанных с приобретением имущества от имени владельца аккаунта.

В заключение хотелось бы отметить, что в целях устранения правовых пробелов, снижения рисков покупок, совершаемых в интернете необходимо регулярно дополнительно анализировать судебную практику, а также внедрять достижения в области развития информационных технологий.

¹ Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 года № 51-ФЗ (ред. от 24.07.2023 № 351-ФЗ) // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

² Закон РФ «О защите прав потребителей» от 07 февраля 1992 года № 2300-1 (ред. от 04.08.202 № 474-ФЗ) // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

³ Решение мирового судьи судебного участка № 332 Бабушкинского района г. Москвы от 26.05.2017 дело 2-234/2017 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁴ Апелляционное определение Белгородского областного суда от 16.03.2021 дело 33-1341/2021 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁵ Определение Шестого кассационного суда общей юрисдикции от 08.11.2021 дело 88-23859/2021 // Официальный интернет-портал пра-

вовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁶ Определение Шестого кассационного суда общей юрисдикции от 08.11.2021 дело 88-22746/2021 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁷ Определение Верховного суда Российской Федерации от 06.06.2023 № 16-КГ23-6-К4 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁸ Определение Второго кассационного суда общей юрисдикции от 17.11.2021 № 88-25640/2021 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

⁹ Решение Верховного суда Российской Федерации от 31.08.2023 дело АКПИ23-703 // Официальный интернет-портал правовой информации. – URL: <http://www.consultant.ru> (дата обращения: 01.10.2023).

*Воронежский государственный
университет
Трофимова Мария Юрьевна
E-mail: marishka.trofimiva.2002@
mail.ru*

*Voronezh State University
Trofimova Maria Yuryevna
E-mail: marishka.trofimiva.2002@
mail.ru*

Филипенко Никита Андреевич

Воронежский государственный университет

НАЛОГООБЛОЖЕНИЕ КРИПТОВАЛЮТ

Filipenko Nikita Andreevich

Voronezh State University

TAXATION OF CRYPTOCURRENCIES

Аннотация: *цель исследования заключается в разрешении некоторых проблем, возникающих в теоретических и практических сферах, связанных с налогообложением криптовалют. В данной статье особое внимание уделяется теоретическому обоснованию возможности такого налогообложения. Проведен сравнительно – сопоставительный анализ различных толкований положений глав 21, 25, 32 Налогового кодекса Российской Федерации с законодательством о налогообложении криптовалют зарубежных стран. Были предложены способы налогообложения такого объекта.*

Abstract: *the purpose of the study is to resolve some problems arising in theoretical and practical areas related to the taxation of cryptocurrencies. This article pays special attention to the theoretical justification of the possibility of such taxation. A comparative analysis of various interpretations of the provisions of Chapters 21, 25, 32 of the Tax Code of the Russian Federation with the legislation on taxation of cryptocurrencies of foreign countries was carried out. Methods for taxing such an object have been proposed.*

Ключевые слова: *налоги, криптовалюты, налогообложение в зарубежных странах, сравнительное правоведение.*

Keywords: *taxes, cryptocurrencies, taxation in foreign countries, comparative law.*

С момента появления криптовалют в гражданском обороте и распространения инвестиционных вложений в них среди граждан, законодатель и юридическая наука выдвигала множе-

ство версий того, как можно определить правовое положение криптовалют, чем они являются по своей природе, и возможно ли облагать их налогами. В Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»¹ был сделан значительный шаг в разрешении данного вопроса. Несмотря на то, что всесторонне и полно законодатель не урегулировал вопрос криптовалют, в указанном законе было установлено, что криптовалюты являются имуществом. Соответственно, в связи с тем, что специальных норм в данной сфере законодатель не принял, к криптовалютам справедливо применять все положения законодательства, связанные с регулированием имущества граждан и юридических лиц. И действительно, если обратиться к доктринальным понятиям, определяющим функции денег, если рассматривать в качестве альтернативного варианта квалификацию статуса криптовалюты как денежные средства, то криптовалюты не обладают таким свойством как средство обращения, ведь несмотря на развитие технологий, криптовалюту невозможно в полной мере использовать как деньги, ведь в случае с применением их в гражданском обороте, они будут лишь выступать в качестве предмета бартера, который возможно обменять на денежные средства, эмитентом которых выступает государство, при этом курс данного обмена определяется не Центральным банком, и даже не их эмитентом, а биржевым методом, что, разумеется, недопустимо для денег².

При этом, шаг законодателя к легальному определению сущности криптовалюты даёт возможность с значительной долей уверенности предположить то, каким образом может сложиться практика по налогообложению криптовалют, ведь имущество выступает в качестве предмета налогообложения без каких-либо проблем. Поэтому, на наш взгляд, криптовалюты могут облагаться налогами на имущество физических лиц и на имущество организаций, при этом налоговая база может определяться относительно стоимости криптовалюты и её изменений на протяжении всего налогового периода. Для этого возможно либо разграничивать налоговый период, соразмерно уменьшая или увеличивая размер налоговой базы, или же

вычислять её по среднему значению. Также к криптовалютам применим налог на добавленную стоимость, и налог на прибыль физических лиц, а также налог на прибыль организаций. Однако, существует проблема установления факта наличия у налогоплательщиков криптовалют, поскольку, зачастую, они производят инвестиции в них именно для того, чтобы избежать налогообложения, либо скрыть свои доходы и расходы, также подлежащие налогообложению. Данная проблема имеет несколько способов решения, которые можно применять совокупно. Первый из них – специализированные сервисы по отслеживанию криптовалют, которые, зачастую, сотрудничают непосредственно с самими разработчиками криптовалют и позволяют отслеживать перемещения между счетами криптовалютных активов. С использованием данных сервисов могут возникать сложности в связи с тем, что они принадлежат иностранным компаниям, а следовательно, российские налоговые органы не смогут контролировать их регулярную и бесперебойную работу. Второй вариант решения данной проблемы – отслеживание операций по счетам налогоплательщиков, которые не обоснованы их открытой коммерческой деятельностью, при этом, зачастую, связанных с крупными суммами³. Похожим методом, только связанным с значительным потреблением электроэнергии, как показывает практика, возможно отслеживать активность граждан, занимающихся так называемым майнингом криптовалют⁴.

Если сравнить данные предложения для законодателя с практикой налогообложения криптовалют за рубежом, то можно заметить, что такие развитые страны, как Япония, Сингапур, Германия и США приблизительно такими же методами облагают налогами криптовалюты. Так, в Японии криптовалюты признаны легальной альтернативной денежными средствами, при этом на операции с обменом криптовалют на валюты традиционные установлен налог на добавленную стоимость⁵. В Сингапуре, привлекающем своей налоговой политикой инвестиции со всего мира, налогами облагаются только операции с криптовалютами, производимые юридическими лицами, физические же лица от данных налогов освобождены, хотя криптовалюты также, как и в нашей стране признаются имуществом⁶. В Гер-

мании, признавшей криптовалюты аналогом денег, в части налогообложения сделок с виртуальными валютами немецкие финансовые органы опираются на решение Европейского суда по делу Шведского агентства по налогам против Д. Хэдквиста касательно применения Директивы о НДС к сделкам с виртуальными валютами. Так, в 2015 г. Европейский суд постановил, что виртуальные валюты нельзя расценивать как «физическое имущество». Таким образом, обмен виртуальной валюты на фиатную валюту и обратно следует трактовать как отдельную услугу. В целях расчета налога на добавленную стоимость данная услуга освобождается от НДС как обмен валюты⁷. В США же модель определения сущности криптовалюты очень похожа на российскую, при этом, применительно к налогообложению, операции с использованием виртуальной валюты в США должны отражаться также в долларах США по справедливой рыночной стоимости виртуальной валюты на дату платежа или получения оплаты. Если виртуальная валюта торгуется на бирже и ее обменный курс устанавливается рыночным спросом и предложением, то справедливая рыночная стоимость виртуальной валюты определяется путем преобразования виртуальной валюты в доллары США по единым и постоянным принципам. Компании и физические лица, которые получают виртуальную валюту в качестве оплаты товаров, работ или услуг, справедливую рыночную стоимость виртуальной валюты в долларах США на дату получения оплаты включают в валовой доход. При майнинге справедливая рыночная стоимость виртуальной валюты на дату получения входит в валовой доход. Если майнинг виртуальной валюты представляет собой торговую или коммерческую деятельность, а майнер не выступает как нанятый работник, то его чистый доход (рассчитываемый как валовой доход от бизнеса, уменьшенный на разрешенные вычеты), возникающий в результате такой деятельности, является доходом от самозанятости и облагается соответствующим налогом⁸.

Таким образом, можно сделать вывод, что исходя из теоретических, правовых оснований и подтверждая зарубежным опытом, криптовалюты могут облагаться налогами на имущество физических лиц, имущество организаций, добавленную стоимость, и доходы физических лиц, прибыль организаций.

¹ Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ: Принят Государственной Думой 22 июля 2020 г.: [в ред. от 28 июня 2022 г.] // Собрание Законодательства Российской Федерации. – 2020. – № 31 (ч. 1). – Ст. 5018.

² Карасева М. В. Актуальные проблемы финансового права / М.В. Карасева. – Москва: Проспект, 2023. – С. 199

³ Акимов О. М. Правовое регулирование эмиссии и обращения цифровых денег / О.М. Акимов О.И. Ларина. – Томск : Вестник Томского Государственного Университета, 2019. – №447.

⁴ Ермакова Е. А. Особенности налогообложения криптовалютных операций / Е. А. Ермакова. – Промышленность: экономика, управление, технологии, 2019. — №4 (78).

⁵ PWC (2018) / Worldwide tax summary, 2018-2019. – 2834 p.

⁶ EY (2018) / Worldwide Personal Tax and Immigration Guide, 2018/2019. – 1640 p.

⁷ Regulation of Cryptocurrency in Selected Jurisdictions (2018) / The Law Library of Congress, Global Legal Research Center, 2018. – 72 p.

⁸ Кочергин Д. А., Налоговое регулирование обращения виртуальных валют: опыт зарубежных стран и перспективы для России / Д. А. Кочергин, Н. В. Покровская, В. Л. Достов. – Вестник Санкт-Петербургского университета. Экономика, 2020. – №1.

*Воронежский государственный
университет
Филипенко Никита Андреевич
E-mail: tommarketpravo@gmail.com*

*Voronezh State University
Filipenko Nikita Andreevich
E-mail: tommarketpravo@gmail.com*

Хорошенькова Валерия Михайловна

Воронежский государственный университет

ЭЛЕКТРОННЫЙ АУКЦИОН ПО ПРЕДОСТАВЛЕНИЮ ЗЕМЕЛЬНЫХ УЧАСТКОВ, НАХОДЯЩИХСЯ В ПУБЛИЧНОЙ СОБСТВЕННОСТИ

Khoroshenkova Valeria Mikhailovna

Voronezh State University

ELECTRONIC AUCTION FOR THE PROVISION OF PUBLICLY OWNED LAND PLOTS

Аннотация: в данной статье рассматриваются причины цифровизации порядка проведения торгов по предоставлению земельных участков из публичной собственности, а также особое внимание уделяется практике проведения таких аукционов и возникающих при этом проблемам механизма. Были предложены перспективы развития данной формы предоставления земельных участков.

Abstract: this article examines the reasons for the digitalization of the bidding procedure for the provision of land plots from public ownership, as well as special attention is paid to the practice of conducting such auctions and the problems of the mechanism that arise. Prospects for the development of this form of land grant were proposed.

Ключевые слова: электронный аукцион, земельный участок, публичная собственность.

Keywords: electronic auction, land plot, public property.

Цифровизация общества и государственного управления – неотъемлемая составляющая современной жизни. Одной из задач государства является эффективное управление земельными ресурсами, которые находятся в государственной и муниципальной собственности. Стремительное развитие информационных

технологий привело к закреплению в земельном законодательстве обязательности электронного аукциона по предоставлению земельных участков, находящихся в публичной собственности. Об электронных торгах как способе обеспечения рационального землепользования писала Е.В. Лунева¹, в частности исследуя перспективу использования обязательных электронных торгов по предоставлению “публичных” земельных участков.

Причинами цифровизации порядка проведения торгов можно назвать обеспечение принципа гласности, стимулирование развития конкуренции, решение вопроса недобросовестной конкуренции, разработку антикоррупционных механизмов, проведение прозрачных и справедливых торгов, защиту публичных и частных интересов и, безусловно, обеспечение рационального землепользования. Рассмотрим данные причины подробнее. Можно сказать, что любые электронные торги обеспечивают высокую гласность, которая выражается в наличии любой интересующей информации в свободном доступе, в опубликовании результатов и в транслировании всей процедуры. Стимулирование развития конкуренции происходит за счет привлечения максимального числа потенциальных контрагентов, в том числе и из других регионов страны с помощью дистанционного формата торгов. Исходя из этой причины, вытекают две следующие – законодатель борется с недобросовестной конкуренцией, а также разрабатывает антикоррупционные механизмы, которые позволяют справиться с манипуляциями в отношении добросовестных участников земельного аукциона. Таким образом, обеспечивается проведение прозрачных и справедливых торгов. Также важно отметить, как причины защиты публичных и частных интересов и обеспечение рационального землепользования, что в целом обеспечивает устойчивость всей системы земельных правоотношений за счет соблюдения базовых принципов земельного права. Как можно заметить, все причины цифровизации взаимосвязаны между собой, а следовательно, действия законодателя по введению электронных торгов как обязательной процедуры можно считать вполне обоснованными.

Однако первоначально с 2014 года, когда ст. 39.13 Земельного кодекса РФ (далее – ЗК РФ) была введена в законодательство, она не подлежала применению ввиду отсутствия специального

регулирования. В соответствии с позицией Конституционного Суда РФ, выраженной в одном из определений², проведение аукционов по предоставлению земельных участков в электронной форме должно быть дополнительно регламентировано; а до момента вступления в силу специального федерального закона их проведение противоречит требованиям земельного законодательства. На сегодняшний день порядок функционирования земельных аукционов в электронной форме регулируется Федеральным законом №385-ФЗ³, вступившим в силу с 1 марта 2023 года.

Электронный аукцион по предоставлению земельных участков, находящихся в публичной собственности, представляет собой специальную форму торгов, при которой лица имеют возможность участвовать в данной процедуре без физического присутствия в месте проведения аукциона, то есть в дистанционном формате. Подготовка и проведение электронного аукциона осуществляется в порядке, который уже был раньше предусмотрен ст. 39.11-39.12 ЗК РФ, но теперь с учетом особенностей ст. 39.13 ЗК РФ. Сегодня вся процедура цифровизирована: от подачи заявки и размещения на электронных площадках лота, содержащего сведения о выставленном на торги земельном участке, до заключения по итогам аукциона договора купли-продажи либо договора аренды такого земельного участка. Как уже было сказано, действия совершаются на информационных площадках, которые определены законодателем и ранее уже использовались для проведения торгов в других сферах – ООО “РТС-тендер” и ГИС Торги.

На официальном сайте ГИС Торги⁴ расположена статистика проведения земельных аукционов за 2023 год. По состоянию на 23 ноября 2023 года всего за год было проведено 165 354 аукциона по предоставлению земельных участков из публичной собственности. Из них 106 753 аукциона (около 64,5 % от общего числа) не состоялось без возможности заключения договора, то есть, когда не было заявок по сформированным лотам и участников, которые бы соответствовали предъявляемым условиям, или же проведение торгов не предусмотрено нормативно-правовыми актами. Указанные данные могут свидетельствовать о наличии некоторых проблем в процессе осуществления механизма земельных электронных аукционов.

Одна из основных проблем, на мой взгляд, связана с защитой информации и проблемой аутентификации сообщений в процессе проведения аукциона. Это может породить трудности в обеспечении легитимности электронных операций, при определении личности. Сейчас данная проблема решается использованием усиленной квалифицированной электронной подписи (УКЭП) для подтверждения своих действий, однако тут уже стоит говорить о нюансах, связанных с самой УКЭП.

С технической точки зрения важно рассмотреть и различные сбои во время аукциона. Шаг его проведения составляет 10 минут, но если в глубинке России возникнут проблемы, допустим, со светом или же Интернетом, потенциальный победитель может лишиться своего участка. В связи с этим законодатель установил переходный период до 1 января 2026 года: органами государственной власти субъектов может быть определен перечень муниципальных образований, внутри которых данные аукционы в связи с технической невозможностью проводится не будут. Кроме того, решением названной проблемы может послужить заимствование из области электронных торгов по закупкам механизма государственной информационной системы “Независимый регистратор”, что, прежде всего, позволит обеспечить дополнительную защиту участников земельных аукционов. “Независимый регистратор” осуществляет видеофиксацию действий пользователя, производимых на электронных площадках, проверку наличия Интернет-подключения, доступности сайта электронной площадки в текущий момент времени, соответствия различных показателей действительности (например, время на используемом устройстве).

Также проблемой при проведении земельных аукционов выступает некоторая правовая неопределённость заявителей, о чем свидетельствует приведенная выше статистика о несостоявшихся аукционах без возможности заключения договора. В данном случае можно рассматривать ситуацию, когда участие в торгах осуществляется через профессионального посредника, который бы помогал гражданам и юридическим лицам разобраться в новой системе. Однако в таком случае представляется разумным предусмотреть в законодательстве виды юридического посредничества, как это сделано в банкротных торгах.

Отдельно хочется обратить внимание на перспективу минимизации коррупционных схем при проведении электронных аукционов по предоставлению земельных участков из публичной собственности. Это связано в первую очередь с тем, что участники не могут непосредственно взаимодействовать между собой, а значит, справедливость и конкуренция обеспечиваются более полно.

Таким образом, введение электронного аукциона в качестве общего правила предоставления государственных или муниципальных земельных участков обусловлено прежде всего функциональным назначением торгов, позволяющим рационально использовать земельные участки в условиях открытой, законной и эффективной конкуренции.

¹ Лунева Е. В. Электронные торги по предоставлению земельных участков, находящихся в публичной собственности, как способ обеспечения рационального землепользования / Е. В. Лунева // Журнал российского права. – 2019. – № 4.

² Об отказе в принятии к рассмотрению жалобы общества с ограниченной ответственностью "Вектор Плюс" на нарушение его конституционных прав положениями статьи 39.13 Земельного кодекса Российской Федерации: Определение Конституционного Суда Рос. Федерации от 28 сентября 2023 г. № 2464-О

³ О внесении изменений в Земельный кодекс Российской Федерации и признании утратившей силу части 7 статьи 34 Федерального закона "О внесении изменений в Земельный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации": Федер. закон Рос. Федерации от 07 октября 2022 г. № 385-ФЗ // Собр. законодательства Рос. Федерации. – 2022. – № 41. – Ст. 6947.

⁴ ГИС Торги – продажи государственного и муниципального имущества: [сайт]. – URL: <https://torgi.gov.ru/new/public> (дата обращения: 23.11.2023).

*Воронежский государственный
университет
Хорошенькова Валерия Михайловна
E-mail: en.valermi@gmail.com*

*Voronezh State University
Khoroshenkova Valeria
Mikhailovna
E-mail: en.valermi@gmail.com*

Чеботарев Денис Алексеевич

Воронежский государственный университет

**ПРОБЛЕМА СОБЛЮДЕНИЯ ПРАВА ЧЕЛОВЕКА
НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ
В ЭПОХУ ЦИФРОВИЗАЦИИ**

Chebotarev Denis Alekseevich

Voronezh State University

**THE PROBLEM OF RESPECTING
THE HUMAN RIGHT TO PRIVACY**

Аннотация: в данной статье рассматриваются перспективы внедрения системы социального рейтинга в Российскую правовую действительность. Оценивается ее перспективное влияние на жизнь граждан в плане воздействия на ряд их конституционных прав. Также исследуется практика зарубежных стран, активно использующих систему социального рейтинга.

Abstract: in this article are considered the perspectives of involving the social rating system in Russian legal system. Influencing on citizen society, respectively influencing on some constitutional rights are also estimating. Also researched the practice of foreign countries actively using the system of social rating.

Ключевые слова: конституционные права, право на личную неприкосновенность, социальный рейтинг, цифровизация

Keywords: constitutional rights, the right for privacy, social rating, digitalization.

В последнее десятилетие в мире наблюдается активное развитие цифровых технологий и рост уровня цифровизации общества. Высокий уровень цифрового развития коснулся и юриспруденции. Особенно это относится к развитию искусственного интеллекта, способности которого за последний год серьезно возросли. Общество может видеть, что даже в юридической среде, где, каза-

лось бы, невозможно использовать механизированные действия, признаются его заслуги настолько, что имел место случай использования GPT-chat для вынесения судебного решения¹.

Наблюдается рост уровня цифровизации в России. По данным The World Bank, Россия вошла в топ-10 стран по уровню GovTech Maturity Index, где индекс цифровой зрелости составил 0.897 балла, что является достаточно высоким показателем². Действительно, сложно отрицать что цифровые сервисы, разработанные и внедренные в общественную жизнь правительством, упрощают жизнь рядовому гражданину не только в бытовом плане, но и в плане взаимодействия с государством.

Однако, не стоит также недооценивать минусы цифровизации. Ни для кого не секрет, что чрезмерное проникновение новых благ цивилизации в нашу жизнь может нарушать права человека и гражданина. Данная тема заслуживает обсуждения, так как в XXI веке человек является референтом безопасности. Его права и свободы должны быть защищены, обеспечены, и любые попытки их умалить должны пресекаться.

В цифровую эпоху право человека на неприкосновенность частной жизни претерпевает определенное негативное воздействие со стороны цифровых технологий.

То, что это становится проблемой, можно наблюдать на примере соседних стран. Так, в Китайской Народной Республике уже с 2013 года правительство разработало систему социального кредитования, что следует из документа «Программа создания системы социального кредита (2014–2020)»³. По данной программе, человек с высоким социальным рейтингом обладает определенными преференциями при приеме на работу, при получении кредита, при получении скидок в магазинах и так далее. Человек же с более низким социальным рейтингом либо не получает данных преференций, либо претерпевает разного рода лишения. Данные о «благополучности» гражданина оцениваются в режиме реального времени и привязываются к удостоверению личности⁴.

Таким образом, в КНР уже достаточно давно существует система «социального кредита», где слово «кредит» понимается гораздо шире, чем в схожей американской системе FICO, которая предназначена для оценки платежеспособности заемщика. Если

данная система подразумевает «кредит» исключительно как термин, пришедший из области финансовых отношений, то в системе КНР данный термин приобретает морально-этический и даже политический смысл.

Представляется очевидным, что поражение человека в правах за социально неодобряемое поведение является катастрофическим нарушением международных стандартов прав человека и конституционных принципов, провозглашающих права человека и гражданина высшей ценностью.

Это обстоятельство, к сожалению, не принимается во внимание в России. В 2022 году в Российском государственном социальном университете разработали и начали тестировать новую, отечественную систему социального рейтинга, под названием «Мы». Важно в данном контексте отказаться от проведения аллюзий к небезызвестному произведению Евгения Замятина и оценить данный вопрос с точки зрения правовой, а именно – с точки зрения действующей Конституции Российской Федерации.

Согласно опубликованному докладу РГСУ⁵, данные о человеке будут представлены в форме двухкомпонентного скоринг-кода, определяющего социальный статус человека и его социальный уровень. «Например 47–29. Социальный статус – отражение своего рода заслуг человека, а социальный уровень – оцифровка как бы его перспектив», – отмечено в докладе. Этот код должен быть добавлен к персональным данным граждан.

По мнению депутата Государственной Думы Федерального Собрания РФ – Станислава Наумова, данные технологии должны быть приняты во внимание на государственном уровне в России. С точки зрения парламентария, такие социальные категории, как «...пьяница, отщепенец, неопрятный человек, ... ударник труда, семьянин, успешный специалист или предприниматель...» должны оцениваться государством, что поможет «меньше тратить» на людей с социально неодобряемыми качествами и, как следствие, поощрять людей с социально одобряемыми качествами⁶.

Оценивая цели законодателя следует отметить, что при законодательном регулировании таких личных характеристик, как «пьяница» или «неопрятный человек» будет нарушено конституционное право человека, закрепленное в статье 23 Конституции Российской Федерации (далее – Конституции)⁷, на неприкосно-

венность частной жизни. В науке⁸ под такими человеческими характеристиками как «характер, облик, здоровье, материальное состояние, семейное положение, образ жизни, факты биографии, отношения с родственниками, друзьями, знакомыми и т.п.» и понимается частная жизнь человека. Такой массив данных может помочь сформировать у отдельных лиц представление о личности человека и это допустимо. Но законодательное закрепление необходимости оценки такого человека – это нарушение 23 статьи Конституции.

Нарушение только одного конституционного права в данной ситуации будет означать также и затрагивание других прав человека. В этой связи стоит также отметить, обращаясь к зарубежному опыту наших – соседей, что гражданам с высоким социальным рейтингом предоставляются и преференции при поступлении на государственную службу. И наоборот, людям с низким «кредитом» доступ на нее или ограничен или закрыт полностью. Если в полной мере пойти по стопам КНР в этом вопросе и все-таки использовать на государственном уровне систему, представленную РГСУ, то таким образом будет нарушено и право закрепленное в части 4 статьи 32 Конституции, которое предусматривает равный доступ граждан к государственной службе.

Можно обратить также внимание, что открытость социального рейтинга, существующая в Китае, может повлечь за собой нарушение права граждан. Ведь если любой человек при любых обстоятельствах сможет ознакомиться с особенностями частной жизни человека, то будут определенные проблемы, например, в сфере судопроизводства. В силу УПК РФ⁹, с участием присяжных заседателей не исследуются факты прежней судимости, и любые другие характеристики (о состоянии здоровья, о семейном положении), способные вызвать предубеждение присяжных в отношении подсудимого. Таким образом, если гражданин с низким социальным рейтингом обретет статус подсудимого, то нововведения в области цифровизации могут повлечь проблемы в обеспечении беспристрастности в уголовном процессе.

В Совете по правам человека при Президенте РФ¹⁰ справедливо отметили возможное злоупотребление моральными категориями «хорошего» и «плохого» людьми, разработчиками искусственного интеллекта, которые не были избраны народом, но

сформировали систему рейтинга, прямо касающуюся вопросов этики. Причем, эти категории будут иметь нормативное подкрепление. По факту может произойти казус, при котором управление страной будут осуществлять меритократы, программисты, которых избиратели даже не будет знать.

Таким образом, мы видим интенцию законодателя вторгнуться в гарантируемый Конституцией правовой статус человека, используя при этом цифровые технологии и условия цифровизации. Зарубежный опыт показывает, что такие изменения приведут к повсеместному нарушению прав человека. Поэтому законодателю необходимо внимательнее относиться к инициативам, которые могут прямым образом нарушать конституционные права граждан, и аккуратнее подходить к нормотворчеству в сфере цифровизации.

¹ Судья в Колумбии использовал чат-бот ChatGPT для вынесения приговора // Российская Газета. – [сайт]. URL: <https://www.gazeta.ru/tech/news/2023/02/03/19647793.shtml> (дата обращения: 31.12.2023)

² GovTech Maturity Index (GTMI) Data Dashboard // The World Bank. – [сайт]. URL: <https://www.worldbank.org/en/data/interactive/2022/10/21/govtech-maturity-index-gtmi-data-dashboard> (дата обращения: 31.12.2023)

³ 国务院关于印发社会信用体系建设 规划纲要（2014—2020年）的通知 // Gov.cn. – [сайт]. URL: https://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 31.12.2023)

⁴ Большой брат 2.0. Как Китай строит цифровую диктатуру // Carnegie endowment for international peace. – [сайт]. URL: <https://carnegiemoscow.org/commentary/71546>

⁵ Проект платформы социального скоринга (материалы к Учёному совету РГСУ) // РГСУ life. – [сайт]. URL: https://rgsu.net/about/activities/press_centre/life/platform/rgsu-life_20.html

⁶ В Госдуме рассказали, зачем в России нужна система социального рейтинга граждан // Российская Газета. – [сайт]. URL: <https://www.gazeta.ru/social/news/2023/10/05/21435607.shtml?updated> (дата обращения: 31.12.2023)

⁷ Конституция Российской Федерации, Законы о флаге, гербе и гимне Российской Федерации. – 6-е изд., испр. – М. – ВАКО, 2023. – 80 с., [8] с. цв. илл.

⁸ Малеина М.Н. Личные неимущественные права граждан: понятие, осуществление, защита. – М., 2001. – 244 с.

⁹ Уголовно-процессуальный кодекс Российской Федерации. – Москва: Проспект, 2022. – 416 с.

¹⁰ Нужно законодательно запретить любые попытки введения тех или иных видов социального рейтинга // Совет по правам человека. – [сайт]. URL: https://www.president-sovet.ru/members/blogs/post/nuzhno_zakonodatelno_zapretit_lyubye_popytki_vvedeniya_tekh_ili_inykh_vidov_sotsialnogo_reytinga/ (дата обращения: 31.12.2023)

*Воронежский государственный
университет
Чеботарев Денис Алексеевич
E-mail: chebotarevdlaw@gmail.com*

*Voronezh State University
Chebotarev Denis Alekseevich
E-mail: chebotarevdlaw@gmail.com*

Чернецова Валерия Владимировна

Саратовская государственная юридическая академия

**УГОЛОВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Chernetsova Valeria Vladimirovna

Saratov State Law Academy

**SOCIAL CONDITIONALITY OF CRIMINAL LAW
PROTECTION OF INTELLECTUAL PROPERTY
AND MODERNIZATION OF THE PUNISHMENT
SYSTEM FOR CRIMES AGAINST ITS OBJECTS
IN THE DIGITAL ECONOMY**

Аннотация: в статье рассмотрена актуальность и роль информации в условиях развития цифровой экономики. Авторами рассмотрена динамика преступлений посягающих на информационные права граждан, общества и государства. В завершение сформулированы направления модернизации уголовно-правового регулирования информационной безопасности.

Abstract: the article examines the relevance and role of information in the context of the development of the digital economy. The authors consider the dynamics of crimes encroaching on the information rights of citizens, society and the state. In conclusion, the directions of modernization of the criminal law regulation of information security are formulated.

Ключевые слова: информационная безопасность, Уголовный кодекс, преступление, санкция, цифровизация, информационные права.

Keywords: information security, Criminal Code, crime, sanction, digitalization, information rights.

В условиях цифровой экономики информация выступает одним из двигателей научно-технического процесса. Данной тенденции способствует глобализация и повсеместное внедрение информационных технологий. Повышение экономической и социальной значимости информации обуславливает необходимость ее уголовно-правовой защиты от преступных посягательств.

Цифровизация и развитие компьютерных технологий способствовали трансформации преступной деятельности, ее переходу на качественно новый уровень. В научной литературе информационные технологии называют «кровеносной системой» преступности поскольку, они не только упрощают процесс совершения традиционных видов преступлений, но и порождают возможность возникновения новых видов. Согласно статистическим данным, опубликованным Генеральной прокуратурой, 25% всех преступлений совершается посредством сети Интернет. В абсолютных значениях данный показатель увеличился в 12 раз за последние 7 лет¹.

В сложившихся реалиях принципиальное значение приобретает обеспечение информационной безопасности. Понятие информационной безопасности подробно раскрывается в Указе Президента России от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности в Российской Федерации»².

Многие отрасли российского законодательства в той или иной мере регулируют общественные отношения, связанные с использованием и распространением информации. Ефремова М. А. в своей работе отмечает, что в наименьшей степени при регулировании информационной безопасности использован потенциал уголовно-правовых средств воздействия³.

Современная законодательная и судебная практика сталкивается с множеством проблем, обусловленных отличительными чертами информации как объекта преступления. Во-первых, тайное хищение данных часто не предусматривает их исчезновения из системы. Во-вторых, не всегда удастся точно оценить величину ущерба, нанесенного кражей сведений. В-третьих, велика возможность возникновения проблем при отстаивании прав, если отсутствует юридически закрепленная привязка информации к носителю.

Переходя к рассмотрению уголовного законодательства, стоит отметить, что преступления против информационной безопасности не объединены в отдельную главу. Многие правоведы критикуют данный факт и утверждают, что в целях систематизации уголовного законодательства необходимо преступлениям в информационной сфере посвятить отдельную главу.

На сегодняшний день преступления, посягающие на различные аспекты информационной безопасности, предусмотрены ст. 137 УК РФ, ст. 138 УК РФ, ст. 183 УК РФ, ст. 185.6 УК РФ, ст. 207.1-207.3 УК РФ, ст. 275 УК РФ, ст. 276 УК РФ, ст. 283 УК РФ, ст. 283.1 УК РФ, ст. 272-274.1 УК РФ⁴. Все они регулируют обеспечение информационной безопасности в тех или иных сферах жизни общества – частной, экономической, политической.

Необходимым представляется пояснение о том, что предметом уголовно-правового регулирования и защиты выступает информация, правообладатель которой желает уберечь ее от незаконного собирания и распространения. Указанные действия могут повлечь за собой нанесение ущерба владельцу информационных данных.

С. А. Стяжкина говорит о необходимости модернизации уголовно-правового регулирования и защиты компьютерной информации, поскольку в данном случае важно не материальное содержание данных, а форма их фиксации, хранения и представления. Согласно статистическим данным, именно компьютерная информация наиболее часто подвергается атакам преступников, поскольку большая часть современного общества хранит сведения в электронном виде из-за удобства и возможности быстрого доступа к ним⁵.

Следует признать, что действующая редакция Уголовного кодекса не в полной мере способна реагировать на вызовы цифровой трансформации. Так, например, уголовно правовая защита средств платежа, электронных финансовых инструментов и электронного документооборота содержит множество пробелов, которые необходимо ликвидировать в самые ближайшие сроки.

Незаконное использование и распространение информации может быть одним из способов ведения гибридной войны и затрагивать государственные интересы. В ст. 207.1-207.3 УК РФ предусмотрена ответственность за публичное распространение

заведомо ложной информации, причиняющей вред интересам личности, общества и государства. «Фейковые» оказать могут носить деструктивное влияние на общественные отношения и авторитет государственной власти в стране. Поэтому многие ученые-юристы выдвигают идею применения и совершенствования превентивных мер по отношению к подобного рода преступным деяниям⁶.

Исходя из вышеупомянутого, можно сделать вывод о том, что необходимость обеспечения информационной безопасности обусловлено трансформацией экономики и переходом к цифровому обществу. Уголовно-правовое регулирование и защита частной, корпоративной и государственной информации является стратегически важной частью дальнейшего развития человечества. На сегодняшний день система уголовного законодательства Российской Федерации в данной области требует модернизации и усовершенствования согласно требованиям научно-технического прогресса и развития цифрового сознания общественности.

¹ Число совершенных через мобильную связь и интернет преступлений в России // ТАСС

² Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) "Об информации, информационных технологиях и о защите информации"

³ Карданов Руслан Рейзаевич УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Вестник Сибирского юридического института МВД России. 2022. №2 (47).

⁴ "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.11.2023)

⁵ Стяжкина, С. А. Информационная безопасность: уголовно-правовой аспект / С. А. Стяжкина // Уголовная политика в условиях цифровой трансформации : сборник статей материалов II Всероссийской научно-практической конференции, Казань 2023 года. – Казань: Издательство "Отечество", 2023. – С. 146-151.

⁶ Корабельников, С.М. Преступления в сфере информационной безопасности / С.М. Корабельников. – М.: Юрайт, 2020. См...: с.111

Чернецова Валерия Владимировна
Саратовская государственная
юридическая академия
E-mail: valeriasima2728@mail.ru

Chernetsova Valeria Vladimirovna
Saratov State Law Academy
E-mail: valeriasima2728@mail.ru

Научное издание

**ТРИБУНА
МОЛОДЫХ УЧЕНЫХ**

Сборник научных статей

Выпуск 20

**ЦИФРОВИЗАЦИЯ ОБЩЕСТВА
И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ**

Под редакцией *О. С. Рогачевой*

Издано в авторской редакции
Компьютерная верстка *А. Ю. Хаустовой*

Подписано в печать 27.09.2024. Формат 60×84/16.
Уч.-изд. л. 6,3. Усл. п. л. 7,0. Тираж 50 экз. Заказ 259

Издательский дом ВГУ
394018 Воронеж, пл. Ленина, 10
Отпечатано в типографии Издательского дома ВГУ
394018 Воронеж, ул. Пушкинская, 3