

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

CRIMINAL LAW SCIENCES

Научная статья
УДК 343.72
DOI 10.33184/pravgos-2024.3.15

Original article

ГРИГОРЬЕВ Павел Александрович
Национальный исследовательский
университет «Высшая школа экономики»,
Москва, Россия,
e-mail: pav96gri@yandex.ru,
<https://orcid.org/0000-0002-3245-8724>

GRIGOREV Pavel Aleksandrovich
National Research University Higher School of
Economics, Moscow, Russia.

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ОБРАЩЕНИЯ СВЕДЕНИЙ ПУБЛИЧНЫХ РЕЕСТРОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

THE PROTECTION OF CIRCULATION OF DATA CONTAINED IN PUBLIC REGISTERS
UNDER CRIMINAL LAW IN THE CONTEXT OF DIGITALIZATION

Аннотация. На современном этапе развития экономики и права в Российской Федерации существует потребность в надежной уголовно-правовой охране обращения сведений, содержащихся в различных публичных реестрах (ЕГРН, ЕГРЮЛ и др.). При этом стремительная цифровизация институтов регистрации прав и механизмов совершения преступлений оказывает значительное влияние на применение норм уголовного закона в сфере защиты информации публичных реестров. В статье рассматриваются наиболее значимые теоретические и практические вопросы, обусловленные цифровизацией обращения сведений публичных реестров: проблема характеристики электронно-цифровых признаков составов преступлений; проблема обоснованности новых классификационных критериев для обособления группы электронно-цифровых преступлений (как в доктрине, так и в законе); различные правоприменительные проблемы (блокчейн-технологии в публичных реестрах и др.). Цель: анализ актуальных теоретических и практических проблем уголовно-правовой охраны обращения сведений публичных реестров в условиях цифровой трансформации общественных отношений, охраняемых нормами УК РФ. Методы: общенаучные (анализ, описание, сравнение и др.) и формально-правовой, являющийся частнонаучным специально-юридическим методом. Результаты: исследование подтвердило тезис о всепроникающем процессе быстрой цифровизации регулятивного законодательства, регламентирующего порядок обращения сведений публичных реестров, что в конечном счете позволяет сделать вывод и о цифровизации уголов-

Abstract. At the present stage of development of the state in the Russian Federation, there is a need for reliable protection of data contained in various public registers (e.g. the Unified State Register of Real Estate, the Unified State Register of Legal Entities and others) under criminal law. At the same time, the rapid digitalization of institutions for registering rights and mechanisms for committing crimes has a significant impact on the application of criminal law provisions on the protection of information in public registers. This article discusses the most significant theoretical and practical issues caused by the digitalization of circulation of data contained in public registers: the issue of characterization of electronic digital elements of the corpus delicti of crimes; the issue of the validity of new classification criteria for grouping electronic digital crimes (both in studies and in legislation); various issues regarding law enforcement (e.g. blockchain technologies in public registries, etc.). Purpose: to analyze current doctrinal and practical problems of protection of data contained in public registers under criminal law in the conditions of digital transformation of social relations protected by the norms of the Criminal Code of the Russian Federation. Research methodology: general scientific methods (analysis, description, comparison, etc.) and the formal legal method, which is a specific scientific special legal method. Results: the study confirms the statement about the pervasive process of rapid digitalization of legislation regulating the procedure of circulation of data contained in public registers, which ultimately allows us to draw a conclusion about the digitalization of criminal law protection, implemented through the

но-правовой охраны, осуществляемой через применение бланкетных норм УК РФ. Сформулирован ряд выводов, включая вывод о том, что в настоящее время отсутствует необходимость в законодательном обособлении в УК РФ как преступлений, совершаемых против обращения сведений публичных реестров, так и в целом группы электронно-цифровых преступлений.

Ключевые слова: государственная регистрация, государственный реестр, информационное преступление, компьютерное преступление, публичный реестр, реестр прав, фальсификация, цифровизация уголовного права, цифровое преступление

Для цитирования: Григорьев П.А. Уголовно-правовая охрана обращения сведений публичных реестров в условиях цифровизации / П.А. Григорьев. – DOI 10.33184/pravgos-2024.3.15 // Правовое государство: теория и практика. – 2024. – № 3. – С. 131–139.

application of blanket standards of the Criminal Code of the Russian Federation. The article formulates a number of conclusions, including the conclusion that at present there is no need for legislative separation within the framework of the Criminal Code of the Russian Federation of both crimes committed against the circulation of data of public registers, and the group of digital crimes in general.

Keywords: state registration, state register, information-related crime, computer crime, public register, register of rights, falsification, digitalization of criminal law, digital crime

For citation: Grigorev P.A. The Protection of Circulation of Data Contained in Public Registers Under Criminal Law in the Context of Digitalization. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2024, no. 3, pp. 131–139. (In Russian). DOI 10.33184/pravgos-2024.3.15.

ПОСТАНОВКА ПРОБЛЕМЫ: НОВЫЕ ВЫЗОВЫ УГОЛОВНОМУ ПРАВУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Действующий УК РФ содержит ряд норм о преступлениях, совершение которых причиняет вред общественным отношениям по поводу обращения сведений¹, содержащихся в существующих в нашей стране публичных реестрах. Рассматриваемые нормы закреплены в ст. 170, 1701, 1731, 1732, ч. 3 ст. 1852, ст. 243, 2431, ч. 2 и ч. 3 ст. 2432, ст. 2853, ч. 1 и ч. 3 ст. 3301. К охраняемым нормами УК РФ публичным реестрам относятся: Единый государственный реестр недвижимости (ЕГРН), Единый государственный реестр юридических лиц (ЕГРЮЛ), Единый государственный реестр объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, реестр иностранных агентов, а также все иные единые государственные реестры и все реестры владельцев ценных бумаг.

Информационная природа как самих публичных реестров, так и группы указанных преступлений вряд ли может вызвать сомнения: публичные реестры являются инфор-

мационными ресурсами, а диспозиции норм УК РФ, в которых описаны признаки составов преступлений, сконструированы таким образом, что общественные отношения по поводу обращения юридически значимой информации (сведений каждого конкретного публичного реестра) могут рассматриваться в качестве основного и (или) дополнительного непосредственного объекта конкретного преступления.

Последние десятилетия истории человечества ознаменованы чрезвычайно быстрым развитием электронно-цифровых технологий, меняющих традиционные формы хранения, обработки и передачи информации. Если во второй половине XX в. ученые говорили об информатизации, то есть о все более возрастающей роли информации как фактора производства, то в настоящее время, с учетом господства электронно-цифровых форм обработки информации, речь ведется главным образом о цифровизации. И в контексте данных общественных трансформаций в исследованиях преступлений, причиняющих вред обращению сведений публичных реестров, актуализируется набор теоретических и прикладных проблем:

1) цифровизация отдельных признаков в этих составах преступлений;

2) цифровизация объекта в этих составах преступлений;

3) возникновение новых классификационных критериев в науке уголовного права;

¹ Здесь и далее понятия «сведения» и «информация» используются как взаимозаменяемые. Подобный подход обусловлен легальной дефиницией термина «информация», который содержится в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (см.: Собрание законодательства РФ. 2006. 31 июля).

4) юридико-техническая проблема формального закрепления группы электронно-цифровых преступлений в тексте УК РФ;

5) совершенствование на практике способов защиты официальной информации, содержащейся в публичных реестрах.

Обозначенные проблемы заслуживают детального рассмотрения и поиска возможных решений, чему и посвящена настоящая статья.

ЦИФРОВИЗАЦИЯ ОТДЕЛЬНЫХ ПРИЗНАКОВ СОСТАВОВ ПРЕСТУПЛЕНИЙ

В науке уголовного права не без оснований все чаще отмечается, что изучаемые явления последовательно приобретают дополнительное (электронно-цифровое) измерение. «Юридическая практика уже привыкла к цифровым аналогам почтовых сообщений, объектов интеллектуальной собственности, денежных средств, ценных бумаг, платежных карт, официальных документов и др.» – справедливо отмечается в одной из недавних статей [1, с. 587]. Цифровизация не обошла стороной и институты государственной регистрации прав на недвижимость, регистрации юридических лиц и индивидуальных предпринимателей, учета прав на ценные бумаги, а также процедуры администрирования публичных реестров. Это подтверждается анализом многочисленных нормативных правовых актов, регулирующих, в частности, обращение сведений двух крупных публичных реестров – ЕГРН и ЕГРЮЛ.

Так, утвержденный в 2023 г. Порядок ведения ЕГРН² в развитие положений Федерального закона «О государственной регистрации недвижимости»³ (далее – Закон о регистрации недвижимости) устанавливает, что ведение ЕГРН осуществляется в электронной форме с использованием федеральной государственной информационной системы ведения Единого государственного реестра недвижимости (далее – ФГИС ЕГРН), а формирование данных ЕГРН – в форме электронного документа, заверенного усиленной квалифицированной электронной подписью (далее – УКЭП).

2 Об установлении порядка ведения Единого государственного реестра недвижимости : приказ Росреестра от 07.12.2023 № П/0514 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 20.03.2024).

3 О государственной регистрации недвижимости : Федеральный закон от 13.07.2015 № 218-ФЗ // Собрание законодательства РФ. 2015. 20 июля.

В 2023 г. Правительство РФ утвердило Положение о ФГИС ЕГРН⁴. Подзаконный акт определяет структуру, задачи, участников, порядок использования и требования к техническим, программным и лингвистическим средствам ФГИС ЕГРН. Повсеместно в его тексте встречаются следующие словосочетания: «загрузка в электронной форме сведений (данных)», «загрузка документов и сведений», «хранение реестровых дел в электронном виде» и им подобные.

Помимо значительного расширения возможностей Росреестра по обработке содержимого ЕГРН в электронно-цифровой форме, последовательно реформируется и процедура представления документов для государственной регистрации – она становится все более (либо же исключительно) электронно-цифровой по своей форме. Из п. 2 ч. 1 ст. 18 Закона о регистрации недвижимости следует, что заявление может быть подано в форме электронных документов и (или) электронных образов документов, подписанных УКЭП. Утвержден и действует специальный Порядок представления заявлений, который определяет, что заявление в форме электронного документа, по общему правилу, подписывается УКЭП заявителя⁵. И если для граждан еще допускается подача документов на традиционных бумажных носителях, то органы публичной власти обязаны представлять заявления и прилагаемые к ним документы только в форме электронных документов (п. 3.1 Порядка представления заявлений).

В сфере обработки информации, содержащейся в ЕГРЮЛ, тенденции аналогичные: происходит повсеместное усиление электрон-

4 Об утверждении Положения о федеральной государственной информационной системе ведения Единого государственного реестра недвижимости и о внесении изменений в пункт 3 Правил информационного взаимодействия федеральной государственной информационной системы ведения Единого государственного реестра недвижимости с иными государственными или муниципальными информационными системами : постановление Правительства РФ от 29.04.2023 № 683 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 20.03.2024).

5 Об установлении порядка представления заявления о государственном кадастровом учете недвижимого имущества и (или) государственной регистрации прав на недвижимое имущество и прилагаемых к нему документов, а также об их приостановлении и об исправлении технической ошибки в записях Единого государственного реестра недвижимости : приказ Росреестра от 30.12.2020 № П/0509 [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 20.03.2024).

но-цифровой составляющей всех процедур и совершаемых действий. Заслуживает внимания абз. 1 ч. 1 ст. 9 Федерального закона «О государственной регистрации юридических лиц и индивидуальных предпринимателей»⁶, согласно которому в ФНС могут быть направлены электронные документы, подписанные УКЭП. Действует специальный подзаконный акт, регулирующий многие вопросы представления электронных документов в регистрирующие органы⁷, согласно которому в настоящее время допускается широкое использование онлайн-сервисов ФНС и единой системы межведомственного электронного взаимодействия.

На данном этапе может быть сделан промежуточный вывод: охраняемые законом сведения публичных реестров в настоящее время в значительной степени являются информацией, представленной в электронно-цифровой форме, и это ощутимо трансформирует «традиционную» сущность составов преступлений. При фальсификации ЕГРЮЛ (ч. 1 ст. 1701 УК РФ) предмет преступления (ЕГРЮЛ как публичный реестр) и средства его совершения (представляемые в ФНС документы с ложными данными) будут иметь бестелесную электронно-цифровую форму. Если документы будут представляться через интернет-сервис ФНС, то и способ совершения преступления (в режиме онлайн) приобретет электронно-цифровой характер. Идентичная ситуация и с внесением в ЕГРН недостоверных сведений при совершении деяний, предусмотренных ст. 170 и 2853 УК РФ: предмет в составе преступления (ЕГРН как публичный реестр) полностью выступает бестелесным электронно-цифровым явлением и не имеет какой-либо вещественной формы⁸.

Аналогичные проблемы обнаруживаются и при характеристике признаков места и обста-

6 О государственной регистрации юридических лиц и индивидуальных предпринимателей : Федеральный закон от 08.08.2001 № 129-ФЗ // Собрание законодательства РФ. 2001. 13 авг.

7 Об утверждении Порядка взаимодействия с регистрирующим органом при направлении документов, необходимых для государственной регистрации юридических лиц и индивидуальных предпринимателей, в форме электронных документов, а также требований к формированию таких электронных документов : приказ ФНС России от 28.12.2022 № ЕД-7-14/1267@ [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 20.03.2024).

8 При этом законодатель никак не оговаривает в рассматриваемых бланкетных нормах УК РФ возможные электронно-цифровые признаки составов. Это выявляется только при обращении к регулятивному законодательству.

новки совершения фальсификаций публичных реестров. Так, из материалов одного уголовного дела следует, что должностное лицо Росреестра исказило сведения ЕГРН, используя для этого программный функционал администратора ЕГРН, подписало неправомерно вносимые сведения своей УКЭП, при этом совершило все перечисленные действия с использованием собственного компьютера и сети Интернет⁹. Представление подложных документов в ФНС на практике тоже очень часто совершается в электронно-цифровом виде с применением сети Интернет и компьютеров¹⁰. Это обстоятельство позволяет характеризовать признаки составов совершаемых преступлений как обладающие исключительно не вещественной электронно-цифровой природой.

ЦИФРОВИЗАЦИЯ ОБЪЕКТА В СОСТАВАХ ПРЕСТУПЛЕНИЙ

Цифровизация не обходит стороной и объект преступления как обязательный элемент любого состава преступления. В современной науке уголовного права общественные отношения, складывающиеся по поводу информации (информационные отношения), в качестве основного или дополнительного непосредственного объекта в различных составах преступлений рассматриваются довольно часто, и такой подход уже не является чем-то принципиально новым для современной доктрины¹¹.

9 Приговор Дмитровского городского суда Московской области от 02.07.2018 № 1-299/2018 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024).

10 См., например: Приговор Химкинского городского суда Московской области от 05.12.2022 № 1-949/2022 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024) ; Приговор Заводского районного суда г. Саратова от 09.08.2022 № 1-458/2022 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024) ; Приговор Рудничного районного суда г. Прокопьевска Кемеровской области от 26.03.2021 № 1-157/2021 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024) ; Приговор Псковского городского суда Псковской области от 11.03.2021 № 1-178/2021 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024) ; Апелляционный приговор Московского городского суда от 04.02.2015 № 10-0428/2015 [Электронный ресурс] // ГАС «Правосудие». URL: <https://sudrf.ru/> (дата обращения: 20.03.2024).

11 Как будет показано далее, многие исследования по этой теме вышли в свет еще задолго до внесения в УК РФ норм о публичных реестрах (первый крупный пакет таких норм был внесен в Кодекс в 2010 г.).

Например, А.А. Турышев, рассуждая о предусмотренных гл. 22 УК РФ преступлениях, отмечает, что в системе «объект – предмет» информация служит интегрирующим элементом; с одной стороны, она выступает частью объекта преступления, с другой – неотъемлемым свойством предмета преступления [2, с. 6].

А.В. Сулопаров считает, что об информации можно говорить как о дополнительном родовом объекте ряда составов преступлений; общественные отношения по поводу обеспечения информационной безопасности личности, общества и государства являются дополнительным родовым объектом информационных преступлений [3, с. 8].

По мнению М.А. Ефремовой, объектом информационных преступлений являются общественные отношения, обеспечивающие информационную безопасность [4, с. 76].

Считаем, что в составах преступлений, посягающих на обращение сведений публичных реестров, имеют место сложные непосредственные объекты. Неоднородная и комплексная структура непосредственного объекта в составе преступления, подразумевающая возможность одновременного выделения 1) основного непосредственного объекта и 2) дополнительного непосредственного объекта, признается в рамках доктринальных классификаций объектов по горизонтали¹².

Из рассматриваемых составов преступлений (ст. 170, 1701, 1731, 1732, ч. 3 ст. 1852, ст. 243, 2431, ч. 2 и ч. 3 ст. 2432, ст. 2853, ч. 1 и ч. 3 ст. 3301 УК РФ) можно выделить и такие, в которых общественные отношения по поводу обращения сведений публичного реестра – это основной непосредственный объект (например, в ч. 1 ст. 1701 УК РФ – фальсификация ЕГРЮЛ или реестра владельцев ценных бумаг), и такие, где эти же общественные отношения – дополнительный непосредственный объект (либо один из дополнительных непосредственных объектов). К примеру, в составе преступления, предусмотренного ч. 1 ст. 243 УК РФ, основной непосредственный объект – это общественные отношения по поводу охраны объектов культурного наследия, а общественные отношения по поводу

обращения сведений единого государственного реестра объектов культурного наследия (памятников истории и культуры) народов Российской Федерации – дополнительный непосредственный объект.

Признание информационных отношений в качестве составляющей объекта состава преступления позволяет констатировать, что в настоящее время такие информационные отношения – это общественные отношения, развивающиеся в электронно-цифровой форме (так называемые цифровые отношения, киберотношения, общественные отношения в цифровой среде и т. п.¹³). Именно в такой форме рассматриваемые общественные отношения зачастую предстают в сфере ведения публичных реестров, охраняемых нормами УК РФ, что было показано выше в ходе анализа норм регулятивного права. Проще говоря, объект составов преступлений получает не только информационное, но и сугубо электронно-цифровое наполнение (общественные отношения складываются по поводу не только информации, но именно информации, закодированной при помощи компьютерной техники).

НОВЫЕ КЛАССИФИКАЦИОННЫЕ КРИТЕРИИ И ЭЛЕКТРОННО-ЦИФРОВАЯ СИСТЕМАТИЗАЦИЯ ПРЕСТУПЛЕНИЙ

Цифровизация актуализирует теоретический вопрос о понятии и месте преступлений, в составах которых наличествуют электронно-цифровые признаки. В доктрине получили распространение подходы, согласно которым отдельные составы преступлений объединяются в классификационные группы по критериям, связанным с использованием электронно-цифровых технологий.

В 1997 г. В.В. Крылов одним из первых предложил новый классификационный подход к такого рода преступлениям. По его мнению, информационными преступлениями являются общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области информационных правоотношений. Ученый считал, что преступле-

12 Ключевое различие между основным и дополнительным объектами усматривается в том, что уголовно-правовая защита дополнительного объекта осуществляется не самостоятельно, а в неразрывной связи с основным объектом [5, с. 107].

13 Поиск наиболее подходящих терминов не является первоочередной задачей. В настоящее время в условиях отсутствия единообразной терминологии даже в специализированных научных исследованиях, проводимых в области комплексных отраслей информационного права и киберправа, пока окончательно не сформулированы устоявшиеся термины и определения.

ния в области компьютерной информации, выделенные в отдельную главу УК РФ, являются частью информационных преступлений, объединенной общим инструментом обработки информации – компьютером [6, с. 11].

Комментируя спустя 20 лет феномен информационных преступлений, А.А. Гребеньков говорит о расширении данного понятия: изначально распространенным был подход к рассмотрению информационных преступлений как компьютерных преступлений, но современное положение дел требует отхода от такого понимания [7, с. 22–24].

Е.А. Русскевич указывает, что в самом обобщенном виде под преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, следует понимать общественно опасные, уголовно-противоправные деяния, совершаемые в отношении и (или) посредством методов, процессов или программно-технических средств, интегрированных с целью хранения, обработки или передачи компьютерной информации [8, с. 32–33]. Ученый предлагает выделять собственно компьютерные преступления, предусмотренные в гл. 28 УК РФ, а также «компьютеризованные преступления» (по признакам объекта и объективной стороны), нормы о которых могут быть расположены в иных главах Кодекса [8, с. 34–35].

Широкое распространение получают практико-ориентированные подходы к классификациям таких преступлений. Например, классификация по критерию наличия в объективной стороне преступления сети Интернет или УКЭП. С.Л. Нудель и Д.А. Печегин выделяют группу «преступлений, совершаемых с использованием сети Интернет и (или) цифровых технологий». К указанной группе ученые причисляют в том числе и фальсификацию ЕГРЮЛ и реестров владельцев ценных бумаг (ст. 1701 УК РФ) [9, с. 318]. Не менее интересен подход В.Д. Ларичева, который использует термин «преступления, совершаемые с использованием УКЭП» [10]. В указанную группу он включает несколько преступлений, посягающих на обращение сведений публичных реестров (ст. 1701, 1731, 1732 УК РФ) [10, с. 29].

Полагаем, что на теоретическом уровне преступления против обращения сведений публичных реестров могут быть обособлены в автономную группу по критерию наличия публичного реестра (информационного ресурса,

представленного в электронно-цифровой форме) как одного из признаков состава. И в этом качестве исследуемые преступления будут подгруппой в классификационном множестве информационных (информационно-телекоммуникационных, компьютеризованных, электронно-цифровых и т. п.) преступлений¹⁴.

ТРЕБУЕТСЯ ЛИ ГЛОБАЛЬНАЯ РЕФОРМА УГОЛОВНОГО КОДЕКСА РФ?

Возникает следующий, но уже не доктринальный, а сугубо практический (законотворческий) вопрос: существует ли в настоящее время необходимость законодательного обособления электронно-цифровых преступлений в рамках самостоятельного раздела (самостоятельных глав) действующего УК РФ? Отвечая на него, стоит отметить, что если сфера научных исследований позволяет проявлять гибкость, оперировать формально незакрепленными критериями и систематизировать преступления без привязки к конкретным разделам и главам кодифицированного уголовного закона, то очевидно, что в законотворчестве подобная свобода ограничена. Дискуссии о внесении каких-либо системных изменений в УК РФ вроде обособления в нем электронно-цифровых преступлений – это зачастую дискуссии не о простом дополнении Кодекса новыми положениями, а о системном и всепроникающем реформировании всей его архитектоники (или как минимум всей Особенной части).

Полагаем, что в настоящее время нет необходимости в редактировании текста УК РФ таким образом, чтобы электронно-цифровые преступления (или отдельные их подгруппы вроде преступлений против обращения сведений публичных реестров) получили в нем некое особое место и формально обрели собственный родовой или видовой объект. Отсутствует и реальная потребность в законодательном дублировании положений УК РФ просто ввиду того, что конкретное преступление может совершаться с использованием электронно-цифровых технологий.

Так, нет необходимости дублировать существующие составы искажения ЕГРН (ст. 170, 2853 УК РФ), фальсификации ЕГРЮЛ

¹⁴ Напомним, что в выделяемую группу входят составы преступлений из 10 статей УК РФ: ст. 170, 1701, 1731, 1732, ч. 3 ст. 1852, ст. 243, 2431, ч. 2 и ч. 3 ст. 2432, ст. 2853, ч. 1 и ч. 3 ст. 3301.

(ст. 1701, 1731, 1732, 2853 УК РФ) в новых нормах, создавая своего рода «двойников» существующих норм¹⁵. Вред совершением таких преступлений причиняется в первую очередь и главным образом основному непосредственному объекту (общественные отношения в сфере экономической деятельности, общественные отношения по поводу отправления публичной власти и т. д.).

В этой связи заслуживает поддержки мнение, что выделение обособленного вида общественных отношений в области оборота компьютерной (цифровой) информации произошло не по причине их эксклюзивности, а потому, что люди смешали понятия содержания и формы, преувеличив значение последнего. Оперирование цифровыми данными, даже с учетом технологической части процесса, не отличается от привычных способов оборота информации, имеющей другие физические параметры. Важнее не то, что сделали с цифровыми сведениями, а как это повлияло на доступность социальных ценностей для потерпевшего [11, с. 120–121].

При этом отметим, что активное увлечение научного сообщества спецификой электронно-цифровых преступлений действительно полезно для более глубокого анализа новых форм преступного поведения, а также для верной квалификации деяний. Вместе с этим тиражирование выводов, призывающих переписать УК РФ, видится неконструктивным и способным принести кодифицированному уголовному закону больше вреда, чем пользы. В лоне науки уголовного права разумнее будет воспринимать электронно-цифровые технологии как данность современным общественным отношениям, благо, упрощающее социальную жизнь и взаимодействие между людьми, «по умолчанию» допуская, что они могут применяться при совершении «традиционных» преступлений, но не придавать им конститутивного значения. УК РФ в его действующем виде, по нашему мнению, имеет колоссальный потенциал самодостаточности перед вызовами цифровизации, он способен быть применимым без каких-либо изменений, обусловленных распространением цифровых технологий.

¹⁵ В таких нормах-«двойниках» фигурировали бы словосочетания вроде «совершенное с использованием электронно-цифровых технологий», «с использованием сети Интернет», «в сфере компьютерной информации» и им подобные.

ПРАВОПРИМЕНИТЕЛЬНЫЕ ПРОБЛЕМЫ: РАЗЪЯСНЕНИЯ ВЕРХОВНОГО СУДА РФ И БЛОКЧЕЙН-ТЕХНОЛОГИИ

Обсуждаемые в настоящей статье проблемы не остались без оценки Пленума Верховного Суда РФ. Заслуживает внимания постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37¹⁶ (далее – ППВС № 37), состоящее из двух разделов. Первый раздел, включающий п. 1–16, озаглавлен «По делам о преступлениях в сфере компьютерной информации», второй раздел под заголовком «По делам о преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» объединяет п. 17–24. В таком структурировании прослеживается логика судебной инстанции, согласно которой электронно-цифровые преступления не исчерпываются только положениями гл. 28 УК РФ.

К примеру, содержащееся в п. 20 ППВС № 37 разъяснение вносит ясность в понимание того, что вообще следует считать электронно-цифровым преступлением, не названным в гл. 28 УК РФ. Пленум Верховного Суда РФ указывает, что преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, независимо от стадии его совершения, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети.

В нормах УК РФ о преступлениях против обращения сведений публичных реестров не упоминаются признаки, указывающие на использование компьютерной техники и сети Интернет. Но подобные признаки прямо следуют из специального законодательства и подзаконных актов, на которые ссылаются бланкетные нормы Кодекса. Ввиду этого положения ППВС № 37, хотя они специально и не затрагивают исследуемую группу преступ-

¹⁶ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Российская газета. 2022. 28 дек.

плений, на практике могут применяться при их квалификации.

Другой важный правоприменительный аспект противодействия рассматриваемым преступлениям касается вопроса совершенствования системы ведения официальных информационных ресурсов и способов хранения содержащихся в них сведений. Целостность сведений публичных реестров может обеспечить внедрение технологии блокчейн. В 2017–2018 гг. оживленное общественное обсуждение вызвал запланированный государственный эксперимент по блокчейн-тестированию ЕГРН в Москве. Для этого в 2017 г. Минэкономразвития России разработало и предложило проект соответствующего постановления Правительства РФ, который получил положительную оценку регулирующего воздействия, но по неизвестным причинам до настоящего времени так и не принят¹⁷.

Потенциал блокчейн-технологий для ведения публичных реестров высоко оценивается учеными и практиками (причем как в правоведении, так и в технических областях знания). Делается вывод, что существенным достоинством перевода системы регистрации прав на недвижимость на технологию блокчейн называется более высокая защищенность ЕГРН от искажений и неправомерных исправлений. Реестр прав, основанный на технологии блокчейн, не позволяет отменить или изменить ранее сделанные в нем записи [12].

По нашему мнению, технологически надежная система шифрования, обработки и хранения информации о зарегистрированных правах соответствует задачам уголовно-правовой охраны от преступных посягательств. В этом разрезе потенциал технологии блокчейн для администрирования публичных реестров может быть распространен не только на ЕГРН, но и на другие публичные реестры – единые государственные реестры и реестры владельцев ценных бумаг. Вероятно, если новая технология сделает любые преступные фальсификации сведений в принципе невозможными, то в обозримом будущем – после прак-

тической имплементации этого технического решения – может устраниться и необходимость в криминализации рассматриваемых деяний. Впрочем, пока что эта перспектива является лишь плодом теоретических предположений.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Проблемы, рассмотренные в настоящей статье на примере преступлений, совершаемых против обращения сведений публичных реестров, подтвердили тезис о революционном воздействии цифровых технологий на институты уголовно-правовой охраны различных общественных отношений. В рамках исследования было, во-первых, установлено, что составы преступлений, совершаемых против обращения сведений публичных реестров, в настоящее время подвержены цифровизации: происходит электронно-цифровая трансформация отдельных их признаков. Во-вторых, охраняемые УК РФ общественные отношения, складывающиеся по поводу обращения сведений публичных реестров, представленных в электронно-цифровой форме, тоже трансформируются, и это приводит к выводу о цифровизации такого обязательного элемента состава преступления, как его объект. В-третьих, за счет выделения новых критериев меняются доктринальные подходы к классификациям исследуемых преступлений, что выражается в появлении разнообразных доктринальных классификаций преступлений с разными родовыми и видовыми объектами. В-четвертых, можно сделать вывод, что вопрос о внесении изменений в УК РФ не должен быть разрешен по принципу тотального реформирования текста закона в угоду цифровизации и ради учета электронно-цифровых признаков в его нормах, то есть законодателю следует воздержаться от «цифровизации» текста уголовного закона. Наконец, в-пятых, акценты законодателя, правоприменителя и ученых-правоведов должны делаться на решении правоприменительных проблем, наиболее существенными из которых представляются унификация правоприменительной практики по делам о таких преступлениях и внедрение блокчейн-технологий (а равно и иных технологий, обеспечивающих защищенность информации) в обращение сведений публичных реестров.

¹⁷ О проведении на территории г. Москвы эксперимента по использованию технологии «Блокчейн» в целях мониторинга достоверности сведений Единого государственного реестра недвижимости: проект постановления Правительства РФ [Электронный ресурс] // Федеральный портал проектов нормативных актов. URL: <https://regulation.gov.ru/projects/List/AdvancedSearch#npa=74195> (дата обращения: 28.03.2024).

СПИСОК ИСТОЧНИКОВ

1. Русскевич Е.А. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации / Е.А. Русскевич, А.П. Дмитренко, Н.Г. Кадников // Вестник Санкт-Петербургского университета. Право. – 2022. – Т. 13, вып. 3. – С. 585–598.
2. Турышев А.А. Информация как признак составов преступлений в сфере экономической деятельности : автореф. дис. ... канд. юрид. наук : 12.00.08 / А.А. Турышев. – Омск, 2006. – 23 с.
3. Суслопаров А.В. Информационные преступления : автореф. дис. ... канд. юрид. наук : 12.00.08 / А.В. Суслопаров. – Красноярск, 2008. – 23 с.
4. Ефремова М.А. Уголовно-правовая охрана информационно-безопасности : монография / М.А. Ефремова. – Москва : Юрлитинформ, 2018. – 312 с.
5. Уголовное право. Общая часть. Преступление. Академический курс : в 10 т. Т. VI. Объект преступления. Объективная сторона преступления / под ред. Н.А. Лопашенко. – Москва : Юрлитинформ, 2016. – 632 с.
6. Крылов В.В. Информационные компьютерные преступления / В.В. Крылов. – Москва : Инфра, М-Норма, 1997. – 285 с.
7. Гребеньков А.А. Информационные преступления и информационная преступность : монография / А.А. Гребеньков. – Курск : ЮЗГУ, 2017. – 255 с.
8. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е.А. Русскевич. – Москва : Инфра-М, 2022. – 351 с.
9. Нудель С.Л. Тенденции уголовной политики в области охраны экономической деятельности в условиях цифровизации / С.Л. Нудель, Д.А. Печегин // Вестник Пермского университета. Юридические науки. – 2022. – Вып. 56. – С. 309–335.
10. Ларичев В.Д. Характеристика и предупреждение преступлений, совершаемых с использованием усиленной квалифицированной подписи / В.Д. Ларичев // Безопасность бизнеса. – 2020. – № 4. – С. 27–31.
11. Голикова А.В. К вопросу о самостоятельности киберпреступлений в действующем уголовном кодексе Российской Федерации / А.В. Голикова // Уголовный закон в эпоху искусственного интеллекта и цифровизации : сборник трудов по материалам I Саратовского международного юридического форума, Саратов, 9 июня 2021 г. – Саратов : СГЮА, 2021. – С. 116–122.
12. Podshivalov T.P. Improving Implementation of the Blockchain Technology in Real Estate Registration / T.P. Podshivalov // Journal of High Technology Management Research. – 2022. – Vol. 33, iss. 2. – URL: <https://www.sciencedirect.com/science/article/pii/S1047831022000153> (дата обращения: 25.03.2024).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Григорьев Павел Александрович – преподаватель департамента права цифровых технологий и биоправа.

INFORMATION ABOUT THE AUTHOR

Grigorev Pavel Aleksandrovich – Lecturer, School of Digital Law and Bio-Law.

Статья поступила в редакцию 15.05.2024; одобрена после рецензирования 24.06.2024; принята к публикации 24.06.2024. The article was submitted 15.05.2024; approved after reviewing 24.06.2024; accepted for publication 24.06.2024.

REFERENCES

1. Russkevich E.A., Dmitrenko A.P., Kadnikov N.G. Crisis and Palingenesis (Rebirth) of Criminal Law in the Context of Digitalization. *Vestnik Sankt-Peterburgskogo universiteta. Pravo = Vestnik of Saint Petersburg University. Law*, 2022, vol. 13, iss. 3, pp. 585–598. (In Russian).
2. Turyshev A.A. Information as a Sign of Crimes in the Sphere of Economic Activity. *Cand. Diss. Thesis*. Omsk, 2006. 23 p.
3. Susloparov A.V. Information Crimes. *Cand. Diss. Thesis*. Krasnoyarsk, 2008. 23 p.
4. Efremova M.A. Criminal-Legal Protection of Information Security. Moscow, Yurлитinform Publ., 2018. 312 p.
5. Lopashenko N.A. (ed.). Criminal Law. General Part. Crime. Academic course. Moscow, Yurлитinform Publ., 2016. Vol. VI. 632 p.
6. Krylov V.V. Information Computer Crimes. Moscow, Infra, M-Norma Publ., 1997. 285 p.
7. Grebenkov A.A. Information Offences and Information Crime. Southwest State University Publ., 2017. 255 p.
8. Russkevich E.A. Criminal Law and «Digital Crime»: Problems and Solutions. Moscow, Infra-M Publ., 2022. 351 p.
9. Nudel S. L., Pechegin D. A. Criminal Policy in the Field of Economic Security: Trends of the Digital Era. *Vestnik Permskogo universiteta. Juridicheskie nauki = Perm University Herald. Juridical Sciences*, 2022, iss. 56, pp. 309–335. (In Russian).
10. Larichev V.D. Characteristics and Prevention of Crimes Committed with the Use of an Enhanced Qualified Signature. *Bezopasnost' biznesa = Business Security*, 2020, no. 4, pp. 27–31. (In Russian).
11. Golikova A.V. On the issue of the Independence of Cybercrimes in the Current Criminal Code of the Russian Federation. *Criminal law in the Era of Artificial Intelligence and Digitalization. Collection of works based on the materials of the 1st Saratov International Legal Forum, Saratov, June 9, 2021*. Saratov State Law Academy Publ., 2021, pp. 116–122. (In Russian).
12. Podshivalov T.P. Improving Implementation of the Blockchain Technology in Real Estate Registration. *Journal of High Technology Management Research*, 2022, vol. 33, iss. 2. Available at: <https://www.sciencedirect.com/science/article/pii/S1047831022000153>.