DOI 10.17150/2411-6262.2019.10(3).17 http://brj-bguep.ru

УДК 343.3/.7

Р.Р. Феткулин
Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация
А.К. Арюков
Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация

ПРЕСТУПЛЕНИЯ В СФЕРЕ ЦИФРОВОЙ ИНФОРМАЦИИ: ПОНЯТИЕ И ВИДЫ

АННОТАЦИЯ. В работе рассмотрены понятие и виды преступлений в сфере цифровой информации. Авторы отмечают, что в связи с развитием цифровой экономики и глобального информационного общества повсеместное использование получили достижения науки и техники, при помощи которых создаются современные цифровые устройства, системы и сети, обладающие значительным потенциалом. Но также, в процессе развития и совершенствования цифровых технологий повышается и рост преступных деяний в указанной сфере. В уголовно-правовой науке должны получить отражение потребности времени, учтен уровень развития и состояния научно-технического прогресса, так как в настоящее время вышеуказанное не получило достаточной реализации в процессе уголовно-правового регулирования отношений в сфере цифровой информации. Преступления в сфере цифровой информации достаточно опасны еще и тем, что сегодня современные цифровые информационно-телекоммуникационные технологии полностью проникли во все сферы деятельности людей и инициировали преобразование индустриального социума в информационное общество. По причине цифрового прорыва возникли новые угрозы информационной безопасности, причиной которых стала глобализация информационных процессов. Соответственно, все вышесказанное является благодатной средой для совершения преступлений в сфере цифровой информации, так как постоянно развиваются и генерируются новые информационно-телекоммуникационные технологии, следовательно, государство должно оперативно и адекватно реагировать на подобные преступные деяния, создавая безопасную и устойчивую информационную инфраструктуру для граждан и представителей бизнеса в цифровом пространстве. В статье приведен анализ российского уголовного законодательства, предусматривающего ответственность за преступления в сфере компьютерной информации. Выявлены основные теоретические подходы научного сообщества к охране цифровых отношений уголовно-правовыми мерами.

КЛЮЧЕВЫЕ СЛОВА. Информация, преступление, цифровая информация, цифровые преступления, компьютерная информация, компьютерные преступления, цифровая экономика.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 13 июня 2019 г.; дата принятия к печати 4 октября 2019 г.; дата онлайн-размещения 31 октября 2019 г.

R.R. Fetkulin
V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation
A.K. Aryukov
V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation

CRIMES IN THE SPHERE OF DIGITAL INFORMATION: CONCEPT AND TYPES

ABSTRACT. The paper deals with the concept and types of crimes in the field of digital information. The authors note that in connection with the development of the digital

economy and the global information society, the achievements of science and technology are widely used, which contribute to creating present-day digital devices, systems and networks with significant potential. But also, the process of developing and improving digital technologies increases the growth of criminal acts in this area. The criminal law science should reflect the needs of the time, take into account the level of development and the state of scientific and technological progress, as, currently, the above-mentioned statement has not been sufficiently implemented in the process of criminal land legal regulation of relations in the field of digital information. Crimes in the field of digital information are rather dangerous because nowadays the up-to-date digital information and telecommunication technologies have completely penetrated into all spheres of human activity and initiated the transformation of the industrial society into the information society. Due to the digital breakthrough, new threats to information security have arisen, caused by the globalization of information processes. Accordingly, all of the above-said is a fertile environment for committing crimes in the field of digital information, as new information and telecommunication technologies are constantly developed and generated, therefore, the state must promptly and adequately respond to such criminal acts by creating a safe and sustainable information infrastructure for citizens and businesses in the digital space. The article presents an analysis of the Russian criminal legislation providing responsibility for crimes in the field of computer information. It reveals the main theoretical approaches of the scientific community to protection of digital relations by criminal-legal measures.

KEYWORDS. Information, crime, digital information, digital crimes, computer information, computer crimes, digital economy..

ARTICLE INFO. Received June 13, 2019; accepted October 04, 2019; available online October 31, 2019.

Сегодня с развитием цифровых технологий большое распространение получают преступления в сфере цифровой информации. Несмотря на общественную опасность подобных деяний, в теории и практике отсутствует единое определение рассматриваемых преступлений.

Всеобщая цифровизация общества обострила указанную проблему и вызывает острую необходимость разработки соответствующей государственной политики [1].

Опасность таких преступлений обусловлена не только масштабами пагубных воздействий, например, результатами посягательств на критически важные и потенциально опасные информационные инфраструктуры, но и ростом их количества [2].

Несмотря на весьма активное обсуждение этой проблемы, использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьезным вызовом как для правоохранительных, так и законодательных органов. Жертвами преступлений, совершаемых с использованием информационно-коммуникационных технологий, ежегодно становятся миллионы людей и организаций, а также органы власти конкретных государств [3].

Современные реалии таковы, что информационно-телекоммуникационные технологии кардинально изменили нашу повседневную жизнь и, вместе с тем, создали новые виды угроз безопасности информации и всего глобального информационного пространства [4].

Подобные преступления часто именуют «компьютерными». Отечественной уголовно-правовой наукой используется как широкая, так и узкая трактовка указанного понятия: если в узком смысле данное понятие является синонимом преступлений в сфере компьютерной информации; широкий же смысл понятие приобретает тогда, когда компьютер — лишь орудие или средство совершения преступления, предмет преступления, а также способ совершения преступления.

Исследователи сегодня выделяют два основных вида преступлений в сфере цифровой информации. Это преступления, в качестве предмета которого

выступает цифровая информация, и преступления, в качестве способа совершения которых выступают цифровые технологии.

Посягательства на цифровую информацию могут выражаться также в использовании информационно-телекоммуникационных технологий с целью пропаганды идеологии терроризма, ксенофобии, экстремизма, распространения идей национальной исключительности, дестабилизации общественно-политической обстановки в стране и т.п [5].

Уголовно-правовая наука содержит сегодня ряд позиций, определяющих понятие преступления в сфере цифровой информации. В частности, Л.Е. Шведова и В.А. Номоконов в состав компьютерных преступлений включают деяния, где компьютер — это объект или орудие совершения преступления [6]. Другие авторы относят к компьютерным преступлениям только ряд неправомерных действий в сфере обращения информации, которая циркулирует в информационно-телекоммуникационных системах. Существует также и третья точка зрения, согласно которой компьютерные преступления — это информационные преступления [7].

На сегодняшний день общественно опасные деяния в области информационных правоотношений, которые являются угрозой общественной безопасности, особенно если они связаны с порядком применения компьютерной информации, именуются преступлениями в сфере высоких технологий и др. Это совокупность преступных деяний, совершенных при помощи вычислительной техники и средств телекоммуникаций или таких, где объект преступных посягательств — это компьютерная информация [8].

О.С. Герасимова отмечает, несмотря на то, что сегодня понятие «компьютерные преступления» широко распространены в литературы, в законодательные и нормативные акты Российской Федерации оно не включено. Этим обстоятельством определено следующее: общественно-опасные действия, где в качестве средства или объекта преступного посягательства выступает вычислительная техника, но не вносятся изменения в «машинную» информацию или не раскрывается охраняемая законом «машинная» информация, компьютерными преступлениями являться не будут [9].

О.С. Герасимова также обозначает специфические признаки, отличающие преступления в сфере компьютерной информации от других преступлений:

– данные преступления практически скрыты на первый взгляд от людей, и факт преступного события обнаруживается только в тот момент, когда сверяются бумажные документы и компьютерная информация;

– существует возможность совершения таких преступлений дистанционно, соответственно, мошенник может находиться на значительном удалении от объекта преступного посягательства [там же].

Под преступлением в сфере обращения цифровой информации понимается предусмотренное уголовным законом виновно совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации [10].

Наиболее полной и достоверной видится классификация преступлений в сфере цифровой информации, предложенная И.Р. Бегишевым:

1. Неправомерный доступ к компьютерной информации. Это предусмотренное ст. 272 «Неправомерный доступ к компьютерной информации» Уголовного кодекса Российской Федерации[1] (далее — УК РФ) умышленное общественно опасное активное поведение, которое посягает на безопасность компьютерной информации и причиняет вред по меньшей мере собственнику или пользователю этой информации.

[1] Уголовный кодекс Российской Федерации : Федер. закон от 13 июня 1996 г. № 63-ФЗ : (в ред. от 29 мая 2019 г. № 112-ФЗ) // Собрание законодательства РФ. 1996. № 25 Ст. 2954.

Он указывает, что терминология ст. 272 УК РФ и современное состояние науки и техники расходятся по сути друг с другом. Например, основным отличие перехвата от неправомерного доступа, как считает автор, является следующее: под электромагнитный перехват может попасть цифровая информация, которая циркулирует в пространстве, а для совершения неправомерного доступа необходимо нарушить систему защиты информации информационно-телекоммуникационных устройств [11].

Отмечая, что неправомерный доступ к цифровой информации и перехват такой информации близки друг другу по своей сути, автор предлагает внести изменения в ст. 272 УК РФ, а также включить понятие «перехват информации» в примечание к рассматриваемой статье.

2. Создание, использование и распространение вредоносных компьютерных программ. Ответственность за данное преступление регламентируется ст. 273 УК РФ. Данное преступление может нанести вред средствам защиты компьютерной информации, однако в законодательстве, отмечено, что рассматриваемые вредоносные программы имеют своей целью нейтрализовать средства защиты компьютерной информации. Соответственно, предлагается также включить в рассматриваемую статью ответственность за деяния, которые предусматривает ч. 1, 2, 3 ст. 273 УК РФ, если имеет место посягательство на информационно-телекоммуникационные устройства, системы и сети, имеющие отношение к критически важным и потенциально опасным объектам [12].

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Отмечается, что указанная норма — бланкетная и содержит отсылку к нормативно-правовым актам, которые устанавливают требования к средствам хранения, обработки или передачи компьютерной информации. Автор предлагает обобщить указанные средства хранения, обработки или передачи компьютерной информации и именовать их «информационно-телекоммуникационными устройствами, их системами и сетями» [13].

4. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Совершение рассматриваемого преступления также происходит в сфере обращения цифровой информации, а сама цифровая информация является ее объектом. Мошенническое программное обеспечение — это своего рода вредоносная цифровая программа, и уголовная ответственность за такое преступление, должна наступать по ст. 273 УК РФ. Кроме того, совершение рассматриваемого вида преступления возможно не только с использованием вредоносных компьютерных программ, но и предполагает нарушение систем защиты цифровой информации. Соответственно, подобное дополнение должно быть внесено в ч. 2 ст. 159.6. УК РФ [14].

5. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Данный вид преступлений рассматривается ст. 138.1 УК РФ. Автор указывает, что УК РФ недостаточно учитывает общественную опасность неправомерного обращения со специальными техническими средствами, которые используются для негласного получения информации, так как они могут позволить получить сведения о персональных данных, нарушить тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений и пр. Соответственно, необходимо установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 УК РФ, 138 УК РФ, 141 УК РФ и ч. 3 ст. 183 УК РФ [15]. Аналогичной позиции придерживается Т.М. Лопатина [16].

6. Преступления, посягающие на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объек-

тов. Данные преступления касаются неправомерных воздействий на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов.

Предполагается, что, например, в результате компьютерных атак на сервисы для расчета и оплаты коммунальных услуг, мониторинга деятельности управляющих и ресурсоснабжающих организаций и состояния объектов государственного учета жилищного фонда может быть нарушено функционирование государственной информационной системы жилищно-коммунального хозяйства — одной из важнейших социально значимых информационных систем государства [17].

Отмечается, что, если будет разрушена информационная инфраструктура критически важных и потенциально опасных объектов Российской Федерации путем неправомерного доступа к цифровой информации, национальная безопасность может получить значительный ущерб, а также повлечь за собой экологическую катастрофу, человеческие жертвы и иные тяжкие последствия. По причине повышенной опасности таких преступлений необходимо внести изменения в ст. 272 и 273 УК РФ, где нужно установить ответственность за совершение деяний, если их следствием является угроза функционирования информационно-телекоммуникационных устройств, систем и сетей критически важных и потенциально опасных объектов [18].

7. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. Указанная норма в УК РФ отсутствует [19]. Так, информация обычно не признается имуществом, и соответственно в результате манипуляций с ней не может наступить ответственность по ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, так как названная норма под имуществом понимает совокупность вещей и материальных ценностей, которыми владеют или законно их используют физические или юридические лица. Предлагая приравнять цифровую информацию к имуществу и отмечая, что хоть цифровую информацию нельзя потрогать и ощутить, в качестве носителя информации выступает вещественный предмет (Flash-карта), содержащий цифровую информацию и представляющий материальную ценность, автор предлагает установить уголовную ответственность за приобретение или сбыт цифровой информации, которая заведомо добыта преступным путем, и внести дополнение в УК РФ ст. 272.1. [20].

За счет массового внедрения новых информационных технологий не только ускоряется развитие цивилизации, но и возникают различные негативные последствия. Соответственно, для борьбы с такими последствиями должна быть своевременно разработана соответствующая государственная политика, особенно это важно в решении вопросов, связанных с обеспечением безопасности цифровой информации и противодействием преступным посягательствам в сфере, связанной с ее обращением.

По этой причине, проблему обеспечения информационной безопасности в целом и уголовно-правовой защиты цифровой информации в частности необходимо считать приоритетным направлением деятельности российских правоведов.

Переход к цифровой экономике сопряжен с необходимостью решения целого ряда политических, экономических и социальных задач в целях минимизации возможных негативных последствий для общества. Особую роль в указанном процессе занимает создание эффективной системы правового регулирования цифровой экономики, в том числе и системы противодействия преступлениям в указанной сфере [21].

Представляется, что преступления в сфере цифровой информации достаточно опасны еще и тем, что сегодня современные информационно-телекоммуникаци-

онные технологии полностью проникли во все сферы деятельности людей и инициировали преобразование индустриального социума в информационное общество [22]. По причине цифрового прорыва возникли новые угрозы информационной безопасности, причиной которых стала глобализация информационных процессов. Соответственно, все вышесказанное является благодатной средой для совершения преступлений в сфере цифровой информации, так как постоянно развиваются и генерируются новые цифровые информационно-телекоммуникационные технологии, следовательно, государство должно оперативно и адекватно реагировать на подобные преступные деяния.

Подводя итог вышесказанному можно констатировать, что отечественное законодательство об ответственности за преступления в сфере цифровой информации нуждается в изменении и дополнении.

Список использованной литературы

1. Бегишев И.Р. Преступления в сфере обращения цифровой информации: состояние, пробелы и пути их решения / И.Р. Бегишев // Информационное право. — 2010. — № 2. — С. 18–21.

2. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации : дис. ... канд. юрид. наук : 12.00.08 / И.Р. Бегишев. — Казань, 2017. — 204 с.

3. Русскевич Е.А. Проблемы систематизации современного уголовного законодательства об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (ИКТ) / Е.А. Русскевич // Уголовная политика и правоприменительная практика : сб. ст. по материалам VI Междунар. науч.-практ. конф. — Санкт-Петербург, 2019. — С. 351–358.

4. Хисамова З.И. Понятие и сущность преступлений, посягающих на информационную безопасность в сфере экономики / З.И. Хисамова // Общество и право. — 2015. — № 1 (51). — С. 157–161.

5. Нечаева Е.В. Посягательства на цифровую информацию: современное состояние проблемы / Е.В. Нечаева, Э.Ю. Латыпова, Э.М. Гильманов. — DOI 10.33463/1999-9917.2019.27(1-4).1.080-086 // Человек: преступление и наказание. — 2019. — Т. 27, № 1. — С. 80–86.

6. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.

7. Белоножкин В.И. Информационная сущность и структура терроризма / В.И. Белоножкин // Информация и безопасность. — 2007. —

№ 4. — С. 541–546.

8. Гребеньков А.А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории / А.А. Гребеньков // Известия Юго-Западного государственного университета. Серия: История и право. — 2012. — № 1-2. — С. 135–138.

9. Герасимова О.С. Особенности преступлений в сфере компьютерной информации / О.С. Герасимова // Вестник Тамбовского университета. Серия: Гуманитарные науки. — 2007. — № 12-2. — С. 327–330.

10. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации : автореф. дис. ... канд. юрид. наук : 12.00.08 / И.Р. Бегишев. — Казань, 2017. — 31 с.

11. Бегишев И.Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект / И.Р. Бегишев // Информация и безопасность. — 2010. — № 2. — С. 255–258.

12. Бегишев И.Р. Информационное оружие как средство совершения преступлений / И.Р. Бегишев // Информационное право. — 2010. — № 4. — С. 23–25.

13. Бегишев И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / И.Р. Бегишев // Вестник УрФО. Безопасность в информационной сфере. — 2012. — № 1. — С. 15–18.

14. Бегишев И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации / И.Р. Бегишев // Вестник Казанского юридического института МВД России. — 2016. — № 3. — С. 112–117.

15. Бегишев И.Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации / И.Р. Бегишев // Следователь. — 2010. — № 5. — С. 2–4.

16. Лопатина Т.М. Совершенствование уголовно-правового регулирования использования специальных технических средств, предназначенных для негласного получения информации / Т.М. Лопатина // Российское право: образование, практика, наука. — 2018. — № 4 (106). — С. 75–78.

17. Бегишев И.Р. Безопасность критической информационной инфраструктуры Российской Федерации / И.Р. Бегишев // Безопасность бизнеса. — 2019. — № 1. — С. 27–32.

18. Бегишев И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. — 2010. — № 1. — С. 9–13.

19. Бегишев И.Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем / И.Р. Бегишев // Безопасность информационных технологий. — 2010. — Т. 17, № 1. — С. 43–44.

20. Бегишев И.Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И.Р. Бегишев // Актуальные проблемы экономики и права. — 2010. — № 1. — С. 123–126.

21. Хисамова З.И. Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики / З.И. Хисамова. — Краснодар : Изд-во Краснодар. ун-та МВД России, 2018. — 119 с.

22. Богданова Т.Н. К вопросу об определении понятия «преступления в сфере компьютерной информации» / Т.Н. Богданова // Вестник Челябинского государственного университета. Серия: Право. — 2012. — № 37. — С. 64–67.

References

1. Begishev I.R. Crimes in the Sphere of Turnover of Digital Information. *Informatsionnoe pravo = Information Law,* 2010, no. 2, pp. 18–21. (In Russian).

2. Begishev I.R. *Ponyatie i vidy prestuplenii v sfere obrashcheniya tsifrovoi informatsii. Kand. Diss.* [Concept and Types of Crimes in the Sphere of Circulation of Digital Information. Cand. Diss.]. Kazan, 2017. 204 p.

3. Ruskevic E.A. Problems of Systematization of Modern Criminal Legislation on Responsibility for Crimes Committed With the Use of Information and Communication Technologies (ICT). *Ugolovnaya politika i pravoprimenitel'naya praktika. Sbornik statei po materialam VI Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Criminal Policy and the Practice of Law Enforcement. Collected Papers Based on the Materials of the 6th International Research Conference]. Saint Petersburg, 2019, pp. 351–358. (In Russian).

4. Khisamova Z.I. The Concept and Essence of the Crimes Encroaching on Information Security in the Economic Sphere. *Obshchestvo i pravo = Society and Law,* 2015, no. 1 (51). pp. 157–161. (In Russian).

5. Nechaeva E.V., Latypova E.Y., Gil'manov E.M. Attacks on Digital Information: the Current State of the Problem. *Chelovek: prestuplenie i nakazanie = Human: Crime and Punishment,* 2019, vol. 27, no. 1, pp. 80–86. DOI: 10.33463/1999-9917.2019.27(1-4).1.080-086. (In Russian).

6. Nomokonov V.A., Tropina T.L. Cybercrime as a New Criminal Threat. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow*, 2012, no. 24, pp. 45–55. (In Russian).

7. Belonozhkin V.I. Information essence structure of terrorism. *Informatsiya i bezopasnost' = Information and Security,* 2007, no. 4, pp. 541–546. (In Russian).

8. Grebenkov A.A. General Approaches to the Definition of Computer Data. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of South-West State University. Series History and Law,* 2012, no. 1-2, pp. 135–138. (In Russian).

9. Gerasimova O.S. Peculiarities of Crimes in the Sphere of Computer Information. *Vestnik Tambovskogo Universiteta. Serija: Gumanitarnye Nauki = Tambov State University Bulletin. Series: Humanities,* 2007, no. 12-2, pp. 327–330. (In Russian).

10. Begishev I.R. *Ponyatie i vidy prestuplenii v sfere obrashcheniya tsifrovoi informatsii. Avtoref. Kand. Diss.* [Concept and Types of Crimes in the Sphere of Circulation of Digital Information. Cand. Diss. Thesis]. Kazan, 2017. 20 p.

11. Begishev I.R. Manufacture, marketing and acquisition of special technical means designed for violating systems of digital information protection: a legal aspect. *Informatsiya i bezopasnost' = Information and Security,* 2010, no. 2, pp. 255–258. (In Russian).

12. Begishev I.R. Informational Weapon as a Means of Committing Crimes. *Informatsionnoe pravo = Information Law,* 2010, no. 4, pp. 23–25. (In Russian).

13. Begishev I.R. Responsibility for Violating Service Regulations on the Means for Data Storing, Processing and Transferring and Information and Telecommunication Networks. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere = UrFR Newsletter. Information Security,* 2012, no. 1,pp, 15–18. (In Russian).

14. Begishev I.R. Some issue of counteracting swindling in the sphere of computer information. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia,* 2016, no. 3, pp. 112–117. (In Russian).

15. Begishev I.R. Problems of criminal responsibility for dealing with special technical means designed for unstated obtaining of information. *Sledovatel' = Investigator,* 2010, no. 5, pp. 2–4. (In Russian).

16. Lopatina T.M. Improvement of the Criminal-Law Regulation of Using Special Technical Means of Secret Gathering of Information. *Rossiyskoye pravo: obrazovaniye, praktika, nauka = Russian Law: Education, Practice, Researches,* 2018, no. 4 (106), pp. 75–78. (In Russian).

17. Begishev I.R. Security of Critical Information Infrastructure of the Russian Federation. *Bezopasnost' biznesa = Busines security,* 2019, no. 1, pp. 27–32. (In Russian).

18. Begishev I.R. Problems of Counter Action to the Criminal Encroachments on the Information Systems of Critical and Potentially Dangerous Objects. *Informatsionnaya bezopasnost' regionov = Information Security of Regions,* 2010, no. 1, pp. 9–13. (In Russian).

19. Begishev I.R. The Problem of the Responsibility for Illegal Actions with the Information Obviously Extracted Criminal. *Bezopasnost' informatsionnykh tekhnologii = IT Security,* 2010, vol. 17, no. 1, pp. 43–44. (In Russian).

20. Begishev I.R. Criminal responsibility for acquiring or marketing of digital and documented information admittedly obtained by criminal way. *Aktual'niye problemy ekonomiki i prava = Actual Problems of Economics and Law,* 2010, no. 1, pp. 123–126. (In Russian).

21. Khisamova Z.I. *Mezhdunarodnyi opyt ugolovno-pravovogo protivodeistviya prestupleniyam v sfere tsifrovoi ekonomiki* [International experience of criminal law counteraction to crimes in the sphere of digital economy]. Krasnodar University of the Ministry of Internal Affairs of the Russian Federation Publ., 2018. 119 p.

22. Bogdanova T.N. On issue of defining the concept "crimes in the sphere of computer information". *Vestnik Chelyabinskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of Chelyabinsk State University. Series: Law,* 2012, no. 37, pp. 64–67. (In Russian).

Информация об авторах

Феткулин Равиль Радиевич — аспирант, кафедра уголовного права и процесса, Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), Российская Федерация, г. Казань, e-mail: ravilfetkulin@mail.ru.

Арюков Александр Кямильевич — аспирант, кафедра уголовного права и процесса, Казанский инновационный университет им. В.Г. Тимирясова (ИЭУП), Российская Федерация, г. Казань, e-mail: snayp86@gmail.com.

Authors

Ravil R. Fetkulin — Ph.D. Student, Chair of Criminal Law and Procedure, V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation, e-mail: ravilfetkulin@mail.ru.

Alexander K. Aryukov — Ph.D. Student, Chair of Criminal Law and Procedure, V.G. Timiryasov Kazan Innovative University (IEML), Kazan, Russian Federation, e-mail: snayp86@gmail.com.

Для цитирования

Феткулин Р.Р. Преступления в сфере цифровой информации: понятие и виды / Р.Р. Феткулин, А.К. Арюков // Baikal Research Journal. — 2019. — Т. 10, № 3. — DOI : 10.17150/2411-6262.2019.10(3).17.

For Citation

Fetkulin R.R., Aryukov A.K. Crimes in the Sphere of Digital Information: Concept and Types. *Baikal Research Journal*, 2019, vol. 10, no. 3. DOI: 10.17150/2411-6262.2019.10(3).17. (In Russian).