Научная статья
УДК 343.9.01
doi: 10.35750/2071-8284-2022-3-118-123

Екатерина Николаевна Рязанова
адъюнкт
https://orcid.org/0000-0002-1666-1968, spbryazanova@mail.ru

Санкт-Петербургский университет МВД России
Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1

Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий

Аннотация: В данной статье исследуется проблема хищения персональных данных, совершаемого как непосредственно в виртуальном пространстве, так и с использованием средств информационно-коммуникационных технологий. Киберпространство стало не только местом работы для большинства граждан, но и средством организации досуга и развлечений, а также способом реализации бытовых потребностей (покупка продуктов питания и товаров повседневного спроса, получение услуг).

В ходе совершения таких действий на всевозможных сайтах происходит ввод персональных данных, что может повлечь за собой их раскрытие и завладение третьими лицами. В настоящее время IT-решения интенсивно внедряются во все сферы жизни общества: онлайн-банкинг и другие сервисы финансово-кредитных организаций; приложения по предоставлению государственных услуг; электронные дневники для учащихся; всевозможные приложения интернет-магазинов и т. д. Все это создает возможности для утечки персональных данных.

Параллельно с совершенствованием IT-сферы развивается и сфера защиты персональных данных.

Цель работы заключается в исследовании проблемных вопросов защиты персональных данных.

Автором использованы следующие методы исследования: статистический, сравнительно-правовой, анализа, формальной логики.

В качестве результатов исследования выделяются факторы, способствующие росту краж персональных данных, а также рекомендации по предотвращению злоупотреблений в указанной сфере.

Научная новизна выражается в изучении процесса правовой защиты информации в меняющихся условиях.

Практическая значимость работы заключается в выработке предложений по введению норм, предусматривающих ответственность за незаконное распространение и ненадлежащее хранение персональных данных.

Важно отметить, что способы кражи персональных данных чаще всего сопряжены с халатностью при их хранении и передаче, поэтому осведомленность о возможностях их сохранности является важной составляющей финансовой безопасности граждан.

Ключевые слова: хищение, персональные данные, информационно-коммуникационные технологии, кража, личность

Для цитирования: Рязанова Е. Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 3 (95). – С. 118–123; doi: 10.35750/2071-8284-2022-3-118-123.

Ekaterina N. Riazanova
Graduate
https://orcid.org/0000-0002-1666-1968, spbryazanova@mail.ru

Saint Petersburg University of the MIA of Russia
1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation

Responsibility for the dissemination of personal data as a way to counteract offenses in the field of information and communication technologies

Abstract: This article examines the problem of personal data theft committed both directly in the virtual space and using information and communication technologies. Virtual or cyberspace has become not only a place of work for most citizens, but also a means of organizing leisure and entertainment, as well as a way to realize household needs (buying food and everyday goods, receiving services).

During the commission of such actions, personal data is entered on various sites, which may entail their disclosure and possession by third parties. Currently, there is an intensive implementation of IT solutions in the social spheres of society: online banking and other services provided by financial and credit organizations; applications for the provision of public services; electronic diaries for students; various applications of online stores, etc. All this will create opportunities for personal data leakage.

Accordingly, in addition to improving the IT sphere, the sphere of personal data protection is also developing, which deserves special attention in the future.

The purpose of the work is to study problematic issues of personal data protection.

The author uses the following research methods: statistical, comparative legal, analysis, formal logic.

As the results of the study, the factors contributing to the growth of personal data theft, as well as recommendations for the prevention of abuse in this area, are highlighted.

Scientific novelty is expressed in the study of the process of legal protection of information in changing conditions.

The practical significance of the work lies in the development of proposals for the introduction of norms providing for liability for illegal distribution and improper storage of personal data.

It is important to note that the methods of personal data theft are most often associated with the negligence of their storage and transfer, therefore, awareness of citizens about the possibilities of their safety is an important component of their financial security.

Keywords: theft, personal data, information and communication technologies, theft, identity

For citation: Ryazanova E. N. Responsibility for the dissemination of personal data as a way to counteract offenses in the field of information and communication technologies // Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2022. – № 3 (95). – P. 118–123; doi: 10.35750/2071-8284-2022-3-118-123.

По мере развития информационных технологий всё большую актуальность приобретает проблема хищения персональных данных и последующего их использования в преступных целях.

В эпоху современных технологий и бурного развития компьютеризации происходит построение информационного общества, что способствует появлению и развитию новых форм преступности. При этом совершению преступлений в сфере экономики с использованием информационно-коммуникационных технологий в отдельных случаях способствует хищение персональных данных потенциальных жертв.

Первый известный факт взлома коммуникационного устройства (телефона) отмечен в выпуске газеты «The Tech» в 1963 году[1]. За последние шестьдесят лет коммуникационные системы приобрели глобальные масштабы, превосходящие возможности человечества по защите информации.

Данные, в том числе персональные, становятся для нового тысячелетия практически тем, чем было электричество в XIX веке, – мощным импульсом для дальнейшего технологического развития, «новым природным ресурсом» [7]. По экспертным данным, к 2025 году в мире с использованием возможностей информационно-коммуникационных технологий будет храниться около 200 зеттабайт данных. По мере увеличения объема информации будет расти количество «слепых зон» в безопасности[2].

Ежедневно новые пользователи информационно-коммуникационных ресурсов вводят свои персональные данные на различных сайтах, приложениях и устройствах, становясь таким образом потенциальными жертвами преступников.

Кража личных данных может быть совершена полностью или частично с использованием информационно-коммуникационных технологий (ИКТ), исключая тем самым физический контакт между преступником и жертвой, позволяя совершать такие деяния на расстоянии [4].

[1] Lichstein Henry. Telephone hackers active. The Tech 24.11.1963 [Электронный ресурс] – URL / http://tech.mit.edu/V83/PDF/V83-N24.pdf (дата обращения: 27.01.2022).

[2] Steve Morgan On Hackers: «Cyber Crime Is The Greatest Threat To Every Company In The World». [Электронный ресурс] – URL / https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/?sh=4dd69f7a73f0 (дата обращения: 27.01.2022).

Исторически совершение хищения путём мошенничества предполагало общение злоумышленника и пострадавшего лицом к лицу, поскольку без непосредственного контакта такого вида деяние совершить было невозможно. Распространение информационно-коммуникационных технологий оказало глубокое влияние на природу преступности, изменились механизмы совершения преступного деяния. Сейчас преступники могут совершать такие преступления в сфере экономики, как мошенничество, используя для этого рассылку электронных писем, поддельные интернет-сайты, сообщения в мессенджерах и социальных сетях. Они обманывают десятки тысяч людей по всему миру и затрачивают для этого значительно меньше усилий, чем их предшественники. Такие преступления сложнее раскрываются сотрудниками правоохранительных органов, поскольку совершаются дистанционно. При этом их общественная опасность существенно выше, чем у контактных преступлений. Люди, у которых были украдены персональные данные, затрачивают потом длительное время для устранения неприятных последствий, созданных преступниками. Им приходится в лучшем случае менять свои документы, сим-карты, в худшем случае инициировать судебные разбирательства относительно легитимности оформленных на их имя кредитов.

В 2021 году было взломано 5,1 млрд записей о данных граждан по всему миру[3]. Кроме того, каждый год, начиная с 2001-го, денежный ущерб, причиняемый такого вида преступлениями, увеличивается в геометрической прогрессии. Например, в 2020 году он составил около 4,2 млрд американских долларов[4]. И это цифры только зарегистрированных случаев преступных деяний. Прогнозируемый экспертами финансовый вред составит в 2025 году примерно 10,5 трлн долларов[5].

Согласно проведенному в США исследованию[6] о преступлениях, которых больше всего боялись американцы в 2021 году, 74 % респондентов беспокоились о том, что у них могут украсть их личную информацию, кредитную карту или финансовую информацию, 72 % опасались кражи персональных данных. При этом стать жертвой ограбления боятся только 33 % респондентов[7].

Дальнейшее развитие технологий будет способствовать возникновению принципиально новых угроз для общества. В связи с этим некоторые исследователи настроены ещё глубже рассматривать проблему «кражи личности», привязывая её к социальным ролям индивида, имея в виду использование преступниками не только персональных данных, документов и внешности, но и черт характера, переживаемых эмоций [3], манеры поведения. Таким образом, преступник, завладевший конфиденциальной информацией, начинает эксплуатировать не только имя человека, но и его личность.

В футуристических литературных произведениях герои часто примеряют на себя чужие образы, меняют личность. В современной виртуальной реальности с каждым годом растёт число людей, выдающих себя за других. Полагаем, многие сталкивались со взломом личной страницы или страницы друга в социальной сети «Вконтакте», когда злоумышленники делают рассылку от имени существующего аккаунта с просьбой перечислить денежные средства.

Сейчас появились программные продукты, способные создавать с помощью искусственных нейронных сетей изображения и звуки, которые воспринимаются как реальные, представляя человека в существующем изображении. И если в настоящее время данные программы находятся в зачаточном состоянии и используются в основном для развлечений, то с их развитием до достаточного уровня достоверности создаваемого контента возрастёт заинтересованность в них преступного мира.

Вероятнее всего, злоумышленники станут активно использовать подобные методы работы с изображением для совершения преступных деяний в сфере экономики. Считаем, что уже сегодня законодатель должен рассматривать вопросы, посвящённые защите от хищения не только персональных данных, но и личности в целом.

Понятие «кража личности» (дословный перевод с английского «identity theft») было введено в оборот в 1950-х годах английским психологом Эриком Эриксоном. Однако, по нашему мнению, точнее было бы толковать этот термин как кражу идентификационных данных (личных или персональных данных).

В Российской Федерации создана нормативная правовая база документов, регламентирующих защиту персональных данных, среди которых: Федеральный закон «О персональных данных»; Федеральный закон «Об информации, информационных технологиях и о защите информации»; Указ Президента «Об утверждении перечня сведений конфиденциального характера»; постановления Правительства «Об утверждении требований к материальным носителям

[3] Ирвин Люк. Утечки данных и кибератаки в 2021 году: 5,1 миллиарда взломанных записей. [Электронный ресурс] – URL / https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2021-5-1-billion-breached-records (дата обращения: 26.01.2022).

[4] Исследовательский центр «Финансы онлайн». [Электронный ресурс] – URL / https://financesonline.com/cybercrime-statistics/ (дата обращения: 22.01.2022).

[5] Морган Стив. К 2025 году киберпреступность будет обходиться миру в 10,5 трлн долларов в год. [Электронный ресурс] – URL / https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (дата обращения: 26.01.2022).

[6] Статистическая консалтинговая компания Statista. [Электронный ресурс] – URL / https://www.statista.com/statistics/339735/crime-worries-in-the-united-states/ (дата обращения: 22.01.2022).

[7] Исследование проводилось с 1 по 19 октября 2021 года в США методом телефонного интервьюирования. Охват составил 823 респондента в возрасте от 18 лет.

биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»; «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Помимо этого, стоит упомянуть документы, разъясняющие некоторые вопросы, касающиеся работы с персональными данными граждан, как, например, приказ Роскомнадзора по их обезличиванию [8].

С позиций криминологического подхода интересно рассмотреть факторы, способствующие росту краж персональных данных.

Одним из основных факторов является время, поскольку, во-первых, между непосредственной кражей персональных данных и хищением, совершённым с их использованием, может пройти значительное время. Гражданин, в отношении которого будет совершено преступное деяние, не всегда сможет осознать, как преступники завладели его персональными данными, когда это произошло. Во-вторых, чем больше времени пройдет с момента утраты персональных данных в пользу третьих лиц до момента обнаружения этого факта, тем значительнее могут быть негативные последствия для жертвы в результате совершенного хищения. Этим пользуются лица, получившие доступ к таким данным в силу своих должностных обязанностей, в частности, операторы офисов обслуживания физических лиц, которые, используя персональные данные клиентов, в течении длительного времени похищают с их счетов небольшие суммы. Такие действия совершаются в основном до обнаружения службой безопасности финансово-кредитных организаций, операторов связи, почтовых отделений.

Так, например, в апреле 2021 года Советским районным судом г. Орла вынесен приговор № 1-47/2021 (1-252/2020) о признании гражданки А. виновной в совершении преступлений, предусмотренных ч. 3 ст. 272 и п. «в» ч. 3 ст. 159.6 УК РФ. Данная гражданка на протяжении полугода работала специалистом офиса ПАО «Вымпел-Коммуникации», где из программы «1CRetail» ей стали известны персональные данные клиентов, в том числе их лицевые счета. Воспользовавшись инструкцией, которую она нашла в сети интернет, из корыстных побуждений, с помощью проведения процедуры поэтапной модификации сим-карт она осуществила вывод денежных средств с лицевых счетов абонентов ПАО «ВымпелКом» («Билайн»). Фактически используя персональные данные абонентов, гражданка А. в течение 6 месяцев оформляла на них сим-карты, о существовании которых они не догадывались и не могли ими соответственно воспользоваться. Получала сим-карты в своё пользование и выводила через них деньги с сим-карт абонентов. Таким образом, семеро пострадавших не знали о доступе к их персональным данным третьих лиц и о своём статусе потерпевших до момента вызова их в полицию для дачи показаний. Сумма ущерба составила 35 тыс. рублей.

Следующим фактором обозначим доступность персональных данных в интернете, деловой переписке, в приложениях, на сайтах. Зачастую пользователи сети регистрируются на различных сайтах, не знакомясь с политикой их конфиденциальности и безопасности, давая согласие на манипуляцию со своими персональными данными, которая может привести к их недобросовестному использованию или хищению. Также существует возможность использования персональных данных в преступных целях сотрудниками телекоммуникационных, кредитно-финансовых и других организаций, в чьём доступе они находятся [1]. При этом компании и организации не несут никакой ответственности за распространение информации о своих клиентах. Более того, оформляя с согласия граждан скидочные карты, карты постоянного покупателя, они завладевают данными и могут использовать их по своему усмотрению, в том числе продавая сторонним организациям [6]. Впоследствии граждане начинают получать звонки и смс-сообщения от незнакомых абонентов с рекламными предложениями, а также рассылку на адрес электронной почты. К тому же большинство людей не проявляют должной бдительности в вопросах защиты своих личных данных и сами предоставляют доступ к ним, не задумываясь о возможных последствиях.

Третьим фактором, на наш взгляд, является уровень материального благосостояния и образованности жертвы. Лица с более низким уровнем материального благосостояния склонны обращаться в сомнительные организации для получения микрофинансовых займов, не только сообщая там свои персональные данные, но и оставляя свои документы, удостоверяющие личность. Для работников подобных организаций в силу специфики их морально-деловых качеств, оформление на попавших в финансовое затруднение лиц микрокредитов о которых последние не будут знать, является распространенной практикой. В силу недостаточной образованности таким жертвам требуется больше времени, чтобы обнаружить и сообщить в правоохранительные органы о преступном деянии, совершенном в отношении их. Иногда граждане делают это только после начала преследований со стороны коллекторских компаний или возникших банковских проблем, связанных с вызовом в суд в связи с невыплатами по кредиту. Дела о признании таких кредитных договоров ничтожными рассматриваются в рамках гражданского судопроизводства. Однако пострадавшая сторона вправе обратиться в правоохранительные органы с заявлением о совершении в отношении неё мошеннических действий.

Четвёртым фактором можно назвать доступность в интернете информации, содержащей инструкции по доступу к персональным данным граждан и пошаговые руководства по

совершению хищений с использованием таких сведений.

В отечественной уголовно-правовой практике при квалификации хищения персональных данных применяется норма, регламентирующая либо неприкосновенность частной жизни, либо нарушение тайны переписки, телефонных переговоров и иных сообщений, либо неправомерный доступ к компьютерной информации. Кроме того, существует статья, предусматривающая ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Судами при вынесении приговоров деяния, связанные с кражей персональных данных и последующим их использованием, квалифицируются по двум статьям УК РФ.

В октябре 2020 года Одинцовский городской суд Московской области вынес обвинительный приговор № 1-627/2020 в отношении гражданина А., который, являясь специалистом офиса продаж ООО «Русская Телефонная Компания», действуя из корыстных побуждений, осуществил неправомерный доступ к персональным данным клиентов (фамилии, имена, отчества, адреса регистрации, серии и номера паспортов, номера лицевых счетов, сведения об остатках денежных средств на абонентских номерах), фотографировал и передавал их третьему лицу за вознаграждение. Давая юридическую оценку, суд квалифицировал его действия по ч. 3 ст. 272 УК РФ (неправомерный доступ к компьютерной информации с использованием служебного положения) и по ч. 3 ст. 183 УК РФ (сбор сведений, составляющих коммерческую тайну и их разглашение). Судом было назначено наказание в виде 2 лет 6 месяцев условного лишения свободы, с испытательным сроком три года. Таким образом, фактически гражданин А. не понёс существенного наказания за свои действия. К тому же, если юридическое лицо, сотрудником которого он являлся, не проявит должной степени ответственности и просто наймёт другого работника, подобная ситуация не исключена в последующем. Каким образом могут быть использованы украденные данные и какие последствия возникнут для их обладателей, в данной ситуации никого не интересует, даже если это способствует правонарушению. Доказать же связь между деянием гражданина А., передавшего персональные данные третьим лицам, и, например, мошенничеством, совершённым в отношении обладателей этих данных, практически невозможно.

Обратим внимание на законодательство зарубежных стран, в частности, США, где введена уголовная ответственность непосредственно за кражу персональных (личных) данных. Под таким деянием подразумевается «сознательная передача или использование без права на то персональных данных лица с намерением совершить или способствовать совершению преступного деяния»[8]. За такое преступление предусмотрено наказание в виде лишения свободы на срок до 15 лет, а также штраф и конфискация личного имущества, используемого для совершения преступления. Под личными данными понимаются не только имя жертвы, ее дата рождения, номер социального страхования, но и адрес проживания и девичья фамилия матери.

В Стратегии безопасности Европейского Союза на 2020–2025 годы обращается внимание на разработку инновационных мер защиты персональных данных, где особое значение придаётся изучению возможных рисков хищения персональных (личных) данных [9].

Как мы уже отмечали, можно установить прямую связь между развитием информационно-коммуникационных технологий и возрастающим риском кражи персональных данных. Хищение персональных данных может иметь серьёзные последствия для граждан, начиная от кражи денег с лицевых счетов, оформления на них банковских кредитов и заканчивая в обозримом будущем возможностью завладения личностью, используя её персональные данные.

Существует множество рекомендаций, как обезопасить себя от хищения персональных данных. Конечно, бдительность при совершении любых действий, связанных с передачей личной информации, является некоторым барьером для возможных злоупотреблений. Однако не всегда психоэмоциональное состояние жертвы позволяет ей оставаться внимательной и исключить случаи совершения в отношении неё преступных деяний. Например, распространённый вид мошенничества в отношении граждан, совершаемого посредством оказания оккультных услуг (гадания). Жертвами становятся вполне уверенные в себе и собранные люди. В настоящее время преступники также применяют методы психологического воздействия на потенциальную жертву [2]. При выполнении таких манипуляций потенциальный потерпевший может не сразу осознать совершение в отношении него преступления. Но, даже осознавая данный факт, жертва может пребывать в уверенности, что ей удастся избежать негативных последствий.

Важно отметить, что способы кражи персональных данных чаще всего сопряжены с халатностью при их хранении и передаче, поэтому осведомлённость граждан о возможностях их сохранности является важной составляющей финансовой безопасности.

Хищение персональных данных видится нам достаточно серьезной проблемой в обозримом будущем, поскольку такое деяние может принимать различные формы [4]: от кражи данных должностным лицом кредитной организации или отделения почты для несанкционированного снятия со счетов граждан денежных средств до хищения полных данных о человеке и присвоения себе его «личности».

Рассмотрев проблемы сохранности персональных данных в современном мире, считаем,

[8] Закон о предотвращении кражи личных данных от 1998 г. 18 USC §1028(a) (7) (свод законов США) [Электронный ресурс] – URL: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (дата обращения: 22.01.2022).

что необходимо введение в отечественное уголовное законодательство нормы, регламентирующей ответственность как граждан, так и юридических лиц за незаконное распространение, ненадлежащее хранение персональных данных. Однако при разработке такой нормы законодателю стоит обратить внимание, что кража личных данных будет образовывать преступное деяние лишь тогда, когда такая информация используется для совершения других незаконных действий.

Список литературы

1. *Антоненко А. Д.* Защита персональных данных как основа экономической безопасности в банковской сфере // Скиф. Вопросы студенческой науки. – 2019. – № 5-2 (33). – С. 140–144.

2. *Антонова Т. С., Смирнов В. М.* Фишинг как неизученное киберпреступление // StudNet. – 2021. – Т. 4. – № 6. – С. 69–75.

3. *Атагимова Э. И., Потёмкина А. Т., Цопанова И. Г.* «Кража личности» как самостоятельное преступление или разновидность мошенничества // Правовая информатика. – 2017. – № 3. – С. 14–22.

4. *Борисова Е. С., Белоусов А. Л.* Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. – 2019. – Т. 13. – № 3. – С. 1330–1342. – DOI 10.21202/1993-047X.13.2019.3.1330–1342.

5. *Денисова А. В.* Уголовная ответственность за преступления в сфере финансовых рынков по законодательству Сингапура // Lex russica. – 2021. – Т. 74. – № 1. – С. 148–156. – DOI: 10.17803/1729-5920.2021.170.1.148–156.

6. *Кузьмин Ю. А.* Кража персональных данных (криминологический аспект) [Электронный ресурс] // Oeconomia et Jus. – 2020. – № 3. – С. 48–57. – DOI: 10.47026/2499-9636-2020-3-48-57.

7. *Озеров И. Н., Озеров К. И.* Новые способы совершения мошеннических действий в сфере IT-технологий в период коронавирусной инфекции // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2021. – № 1. – С. 24–28.

8. *Салимова Т. А., Атнабаева Ю. В.* Особенности обеспечения безопасности персональных данных в Российской Федерации // Международный журнал гуманитарных и естественных наук. – 2021. – № 11-1 (62). – С. 119–123. – DOI 10.24412/2500-1000-2021-11-1-119-123.

9. *Терентьева Л. В.* Критерий «направленной деятельности» применительно к отношениям, связанным с защитой персональных данных // Правовая информатика. – 2021. – № 1. – С. 61–69. – DOI 10.21681/1994-1404-2021-1-61-69.

10. *Тучков А. В.* Криминологическая характеристика хищений, совершаемых с использованием информационных и телекоммуникационных технологий // Академическая мысль. – 2019. – № 2 (7). – С. 57–61.

References

1. *Antonenko A. D.* Zashchita personal'nykh dannykh kak osnova ekonomicheskoy bezopasnosti v bankovskoy sfere // Skif. Voprosy studencheskoy nauki. – 2019. – № 5-2(33). – S. 140–144.

2. *Antonova T. S., Smirnov V. M.* Fishing kak neizuchennoye kiberprestupleniye // StudNet. – 2021. – T. 4. – № 6.

3. *Atagimova E. I., Potemkina A. T., Tsopanova I. G.* «Krazha lichnosti» kak samostoyatel'noye prestupleniye ili raznovidnost' moshennichestva // Pravovaya informatika. – 2017. – № 3. – S. 14–22.

4. *Borisova Ye. S., Belousov A. L.* Innovatsii kak instrument obespecheniya informatsionnoy bezopasnosti i povysheniya effektivnosti deyatel'nosti bankovskoy sistemy // Aktual'nyye problemy ekonomiki i prava. – 2019. – T. 13. – № 3. – S. 1330–1342. – DOI 10.21202/1993-047X.13.2019.3.1330–1342.

5. *Denisova A. V.* Ugolovnaya otvet·stvennost' za prestupleniya v sfere finansovykh rynkov po zakonodatel'stvu Singapura // Lex russica. – 2021. – T. 74. – № 1. – S. 148–156. – DOI: 10.17803/1729-5920.2021.170.1.148–156.

6. *Kuz'min Yu. A.* Krazha personal'nykh dannykh (kriminologicheskiy aspekt) [Elektronnyy resurs] // Oeconomia et Jus. – 2020. – № 3. – S. 48–57. – DOI: 10.47026/2499-9636-2020-3-48-57.

7. *Ozerov I. N., Ozerov K. I.* Novyye sposoby sovershenіya moshennicheskikh deystviy v sfere it-tekhnologiy v period koronavirusnoy infektsii // Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii imeni I. D. Putilina. – 2021. – № 1. – S. 24–28.

8. *Salimova T. A., Atnabayeva Yu. V.* Osobennosti obespecheniya bezopasnosti personal'nykh dannykh v Rossiyskoy Federatsii // Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk. – 2021. – № 11-1 (62). – S. 119–123. – DOI 10.24412/2500-1000-2021-11-1-119-123.

9. *Terent'yeva L. V.* Kriteriy «napravlennoy deyatel'nosti» primenitel'no k otnosheniyam, svyazannym s zashchitoy personal'nykh dannykh // Pravovaya informatika. – 2021. – № 1. – S. 61–69. – DOI 10.21681/1994-1404-2021-1-61-69.

10. *Tuchkov A. V.* Kriminologicheskaya kharakteristika khishcheniy, sovershayemykh s ispol'zovaniyem informatsionnykh i telekommunikatsionnykh tekhnologiy // Akademicheskaya mysl'. – 2019. – № 2(7). – S. 57–61.

Статья поступила в редакцию 23.02.2022; одобрена после рецензирования 29.06.2022; принята к публикации 17.08.2022.

The article was submitted February 23, 2022; approved after reviewing June 29, 2022; accepted for publication August 17, 2022.