

ЮРИДИЧЕСКИЕ НАУКИ / LAW

Научная статья

УДК 343.211

<https://doi.org/10.35266/2949-3455-2024-3-8>



Криминализация незаконного оборота персональных данных

**Наталья Юрьевна Акинина^{1✉}, Валерий Филиппович Анисимов²,
Роман Валерьевич Кочупалов³**

^{1, 2, 3}Югорский государственный университет, Ханты-Мансийск, Россия

¹anu8671@mail.ru ✉

²anisimov.vf@gmail.com

³ko4upalovr@mail.ru

Аннотация. В статье рассматриваются аспекты обоснования криминализации незаконного оборота персональных данных с целью обеспечения их защиты от современных угроз информационного общества. В результате исследования сделан вывод о том, что поскольку данное деяние представляет значительный вред для граждан и является достаточно массовым явлением, оно имеет основания для криминализации.

Ключевые слова: персональные данные, криминализация, незаконный оборот персональных данных, информационная безопасность

Для цитирования: Акинина Н. Ю., Анисимов В. Ф., Кочупалов Р. В. Криминализация незаконного оборота персональных данных // Вестник Сургутского государственного университета. 2024. Т. 12, № 3. С. 84–91. <https://doi.org/10.35266/2949-3455-2024-3-8>.

Original article

Criminalization of personal data illegal trade

Natalya Yu. Akinina^{1✉}, Valeriy F. Anisimov², Roman V. Kochupalov³

^{1, 2, 3}Yugra State University, Khanty-Mansiysk, Russia

¹anu8671@mail.ru ✉

²anisimov.vf@gmail.com

³ko4upalovr@mail.ru

Abstract. The article discusses aspects of the justification for the criminalization of illegal trade of personal data in order to ensure their protection from modern threats of the information society. The authors conclude that there are grounds for criminalizing this phenomenon due to its significant harm to citizens and its widespread nature.

Keywords: personal data, criminalization, illegal trade of personal data, information security

For citation: Akinina N. Yu., Anisimov V. F., Kochupalov R. V. Criminalization of personal data illegal trade. *Surgut State University Journal*. 2024;12(3):84–91. <https://doi.org/10.35266/2949-3455-2024-3-8>.

ВВЕДЕНИЕ

Одним из наиболее востребованных ресурсов современного общества является информация. Такое положение характеризуют как один из этапов развития цивилизации – информационное общество, где знание и информация имеют доминирующее положение по отношению к иным факторам производства.

Государственная политика Российской Федерации стремится к развитию и поддержанию информационного общества, а также его составляющих элементов. Основным стратегическим документом в этой области является Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. [1]. Главная цель этого документа – создание общества знаний, где информация, с учетом стратегических национальных приоритетов Российской Федерации, играет важную роль в развитии граждан, экономики и государства.

Согласно стратегии о национальной безопасности [2] информационная безопасность является одним из видов стратегических национальных приоритетов.

К числу задач Стратегии о национальной безопасности в области информационной безопасности (п. 57 Стратегии) относится оптимизация деятельности, связанной с предотвращением, выявлением и пресечением преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий. Также следует отметить задачу по обеспечению надежной защиты прав и свобод каждого человека и гражданина при обработке и использовании их персональных данных, особенно в контексте информационных технологий.

Вместе с тем проблема, связанная с защитой персональных данных, остается одной из актуальных и значимых мировых проблем, в том числе и России.

Так, количество пользователей информационно-телекоммуникационной сети Интернет за последние десять лет выросло более чем в два раза и на сегодняшний день составляет около 5,35 миллиарда человек по всему миру [3]. При этом численность

интернет-пользователей в России составляет около 130 миллионов человек [4].

Однако количество скомпрометированных записей, содержащих персональные данные, в России за 2023 г. составило 300 миллионов. Основной поток утечек персональных данных происходит посредством интернета [5]. Так, одним из крупных случаев стала утечка данных пользователей сервиса «Яндекс.Еда». Согласно материалам дела сервиса «Яндекс.Еда» допустила утечку персональных данных, подпав под действие ч. 1 ст. 13.11 КоАП РФ. Максимальное наказание по данному составу – 100 тыс. рублей. При этом сервис «Яндекс.Еда» сообщил об утечке данных своих пользователей, указав в качестве причины произошедшего недобросовестные действия одного из сотрудников. Позже в открытом доступе в интернете появился сайт с базой данных клиентов сервиса, на котором можно было найти фамилию, имя, отчество, адрес, телефон и электронную почту пользователя, а также общую сумму заказов [6].

В 2023 г. суд оштрафовал на 60 тыс. руб. Минпросвещения РФ из-за того, что произошла крупная утечка персональных данных пользователей сайта «Российская электронная школа», содержащего 2,019 млн записей, которые включают в себя полное имя, номер телефона, адрес электронной почты, дату рождения, город, должность, место работы, место обучения, сведения о наличии детей. Аналогичные случаи произошли по вине издательства «ЭКМО», курорта «Роза Хутор», Высшей школы экономики [7, 8]. Виновные юридические лица были оштрафованы на 60 тыс. руб., что является несоразмерным между правонарушением и мерой наказания в отношении виновного лица, поскольку персональные данные стали доступными для телефонного мошенничества, а размер штрафа не может влиять на виновных лиц и побуждать их к правомерному поведению. В результате встает вопрос о необходимости применения не только мер административной ответственности в виде штрафов, но и мер уголовной ответственности для должностных лиц, осуществляющих незаконный оборот

персональных данных и подвергающих угрозе причинения имущественного вреда значительный круг лиц, не способных предупредить утечки персональных данных.

МАТЕРИАЛЫ И МЕТОДЫ

Применялись общенаучные методы, в том числе методы анализа, синтеза, классификации, без которых невозможно сделать основные выводы в настоящем исследовании. Среди частнонаучных методов играет важную роль сравнительно-правовой метод, который позволяет рассмотреть уголовно-правовую охрану персональных данных в зарубежных правовых системах. Применение методов правовой статистики позволит изучить правоприменительную практику в области охраны персональных данных.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Вопрос, связанный с уголовно-правовой охраной персональных данных, является обсуждаемым в научном сообществе.

А. Ю. Волкова считает нецелесообразным внедрение нормы, предусматривающей уголовную ответственность за незаконный оборот персональных данных, поскольку уголовно-правовая охрана уже имеется [9]. С. И. Гутник в своем исследовании приходит к выводу о том, что необходимо исходить из режима конфиденциальности персональных данных в каждом рассматриваемом случае [10].

Другого мнения придерживаются А. М. Гвай, С. И. Захарцев, которые предполагают необходимость выделения персональных данных как объекта уголовно-правовой охраны [11]. Аналогичной позиции придерживается и В. А. Чуcreев, при этом не упуская из внимания охрану биометрических персональных данных [12]. Н. В. Довголюк определяет относительно новый вид общественно опасного деяния – информационную торговлю [13]. Кроме того, А. М. Герасимов предлагает подвергнуть уголовно-правовой охране генетические персональные данные [14]. Е. И. Бахтеева и Н. А. Жилиева предлагают привлекать к уголовной ответственности диспетчеров и сотрудников дежурной части «скорой помощи» в случае распространения персональных сведений об умерших лицах [15].

И. Р. Бегишев и Д. В. Кирпичников предлагают сузить понятие персональных данных и оценивать в каждом деле общественную опасность совершенного деяния [16].

Также в научном сообществе предлагается внедрение различных положений, имеющих в уголовной регламентации зарубежных государств. Например, Е. В. Хохлова предлагает установление уголовной ответственности за использование фото человека в СМИ, социальных сетях без согласия субъекта персональных данных [17]. В. В. Вабищевич предлагает установление уголовной ответственности в области персональных данных с учетом международно-правовых положений, заключающихся в единообразии национального и транснационального правового регулирования обработки и передачи персональной информации [18].

При этом, несмотря на наличие дискуссий по поводу охраны персональных данных, не сформировалось такого понятия, как «незаконный оборот персональных данных». Некоторые исследователи используют понятие «утечка персональных данных», «неправомерный доступ к персональным данным» и др. Вместе с тем президент РФ дал поручение рассмотреть вопрос об усилении охраны персональных данных, используя понятие «незаконный оборот персональных данных». Это же понятие использует и экспертное сообщество.

Действительно, понятие «незаконный оборот» более широкое и может включать различные действия, такие как сбор, распространение, передача, использование, сбыт и т. д.

Экспертное сообщество постоянно обращается и к вопросу малой эффективности мер административной защиты персональных данных, и, в частности, за их незаконный оборот.

На заседании Совета по развитию гражданского общества и правам человека председатель Постоянной комиссии по гражданскому участию в развитии правоохранительной системы К. В. Кабанов предложил установить уголовную ответственность за незаконный оборот персональных данных по аналогии

с нормой, предусматривающей ответственность за незаконный оборот наркотических средств [19].

Соответственно, криминализация оборота незаконно полученных персональных данных может обеспечить более действенную их защиту и стать одним из средств в борьбе с этим противоправным деянием. Так, председатель Государственной Думы Вячеслав Володин, комментируя принятые в первом чтении законопроекты об усилении ответственности в области персональных данных, отметил следующее: «Проводил опрос на эту тему в своем ТГ-канале – абсолютное большинство высказалось за необходимость усиления наказания за утечку персональных данных» [20].

Однако, исходя из устоявшейся научно-правовой доктрины в России, в качестве основания криминализации деяния должно быть не усмотрение законодателя, а реальная общественная опасность таких деяний.

Общественная опасность представляет собой внутреннюю характеристику преступления, фиксируемую в законе и имеющую юридическое значение. Это объективное свойство существует независимо от воли законодателя или исполнительных органов, применяющих закон [21].

В уголовно-правовой науке общественная опасность подразумевает объективную способность актов определенного типа вызывать негативные изменения в социальной реальности, нарушать упорядоченность общественных отношений, искажать их и вносить элементы дезорганизации в существующий порядок. Следовательно, основой уголовной ответственности является общественная опасность такого поведения, которое характеризуется причинением либо созданием угрозы причинения общественно опасного вреда наиболее значимым общественным отношениям. Общественно опасный вред в данном ключе может выражаться в причинении вреда или угрозе причинения такого вреда субъектам персональных данных. Так, незаконное распространение персональных данных и получение доступа мошенников к информации

о человеке может привести к причинению ему значительного материального ущерба. Например, злоумышленники могут проводить различные сделки под чужим именем, в том числе и с недвижимостью, создавать банковские счета, оформлять кредиты в банках и микрофинансовых организациях и т. д. Помимо прочего, у злоумышленников повышается вероятность успешной манипуляцией человеком, данные которого скомпрометированы. Нельзя не отметить и вред, наносимый операторам-компаниям вследствие утечки персональных данных. По оценкам экспертов Ф.А.С.С.Т., в открытом доступе в 2023 г. оказалась личная информация на примерно 397 млн строк данных; за первое полугодие 2024 г. – 204,5 млн строк данных, куда входят паспортные данные, адреса, телефоны, пароли [22]. Суммарно за 2023 год и 4 месяца 2024 г. ущерб от IT-преступлений составил 210 млрд руб. [23].

Есть точка зрения, согласно которой общественная опасность определяется наличием характеристик преступлений, свойственных человеческой деятельности, а также способностью совершить подобные преступления в будущем [24].

А. В. Шеслер также отмечает, что понятие общественной опасности включает в себя обе характеристики преступления: его вредность и возможность повторения подобных преступлений в будущем, которая является уникальной для человеческой деятельности [25].

Оценивая данный критерий, стоит отметить, что незаконный оборот персональных данных носит массовый характер. Так, участились случаи массовых утечек таких данных с различных сервисов, онлайн-магазинов. Только в 2023 г. стало доступным 300 млн записей, содержащих такие данные, как имена, адреса, телефоны, электронные почты, паспортные данные, информация о платежах, данные банковских карт и иная чувствительная информация [26].

Случаи утечек происходили у крупных представителей потребительского рынка DNS, Почты России, Яндекс.Еды, российских банков и у других известных компаний [27].

По сообщениям и отчетам МВД России в последние несколько лет в России наблюдается устойчивое увеличение числа киберпреступлений, которые характеризуются активным использованием злоумышленниками информационных технологий. Это направление преступной деятельности стало одним из самых распространенных за короткий промежуток времени – каждое четвертое преступление относится к этой категории. В среднем около 30 % таких преступлений удастся раскрыть [28].

На основании изложенного понятно, что имеется реальная общественная опасность незаконного оборота персональных данных, которая проявляется как в аспекте вреда, так и в аспекте прецедентности.

В целях разграничения между уголовной и административной ответственностью необходимо определить состав преступления как материальный, то есть нарушения законодательства о персональных данных приведут к определенному размеру ущерба.

Для лучшего понимания и разрешения вопроса целесообразно обратиться к зарубежному опыту. Например, в Уголовном кодексе Республики Беларусь имеются составы преступлений, предусмотренных статьями 203¹, 203² в отношении персональных данных.

Так, согласно ч. 1 и 2 ст. 203¹ УК РБ преступлением являются умышленные незаконные сбор, предоставление, распространение информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина (Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-3).

Важной особенностью состава преступления ст. 203¹ УК РБ является факт наступления существенного вреда, который, согласно законодательству Республики Беларусь, является оценочным. Вред может включать в себя как материальный (имущественный) ущерб, так и нематериальный. Здесь стоит отметить, что существенный вред в данных категориях дел подлежит оценке правоприменителем в каждом отдельном случае в связи со спецификой персональных данных и сведений о частной

жизни лица. Кроме того, нельзя не отметить, что подход законодателя рассматривает нарушение именно как реальное изменение объективной действительности, которое повлекло тяжкий вред субъекту персональных данных [29].

Квалифицирующим признаком ч. 2 ст. 203¹ УК РБ является распространение, которое подразумевает под собой передачу любым способом сведений неопределенному кругу лиц. Главное отличие в УК РБ между предоставлением и распространением заключается в количестве конечных получателей охраняемых законом сведений. При предоставлении защищаемая информация передается одному лицу, а при распространении информация, соответственно, – неопределенному кругу лиц. Необходимо также отметить, что при расследовании либо рассмотрении уголовных дел по ст. 203¹ УК РБ должностному лицу следует установить субъективную сторону преступления: была ли цель в передаче данных определенному лицу или неопределенному кругу лиц.

В ст. 203² УК РБ предусмотрена ответственность за несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий.

Важно отметить, что в данном составе выделен специальный субъект состава преступления – оператор персональных данных. Также в нем необходимыми элементами являются одновременно и распространение персональных данных, и причинение тяжких последствий.

При этом, как явно установлено в диспозиции состава, вина характеризуется как неосторожность.

Становится очевидным, что в УК РБ наличествует материальный состав, при котором наступление существенного вреда является моментом окончания преступления. Законодательством Беларуси предусмотрены два состава преступления, разделяющиеся в зависимости от субъективных и объективных признаков.

ЗАКЛЮЧЕНИЕ

Таким образом, на сегодняшний день имеется основание для криминализации незаконного оборота персональных данных, поскольку наличествует реальная общественная опасность такого деяния, которое проявляется как в аспекте вреда, так и в аспекте прецедентности. Незаконный оборот персональных данных носит массовый характер. Участились случаи массовых утечек таких сведений, и они имеют регулярный характер. Организациям и гражданам наносится серьезный ущерб от такого рода противоправной деятельности. При этом незаконный оборот персональных данных с учетом его

массового характера и причинения ущерба либо угрозы ущерба правам и законным интересам граждан должен быть криминализован в виде специальной уголовно-правовой нормы.

Учитывая актуальность охраны персональных данных в современных реалиях, полагаем, что необходимо изучить позитивный опыт уголовного законодательства Республики Беларусь с целью его последующего использования для совершенствования уголовно-правовой защиты персональных данных. Наличие материального состава позволит разграничить административную и уголовную ответственности.

Список источников

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 09.05.2017 № 203. URL: <http://kremlin.ru/acts/bank/41919/page/1> (дата обращения: 29.07.2024).
2. О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 02.07.2021 № 400 // СЗ РФ. 2021. № 27 (часть II). Ст. 5351. Доступ из СПС «Гарант».
3. История Интернета // РИА Новости : офиц. сайт. 2024. URL: <https://ria.ru/20240312/internet-1932278255.html> (дата обращения: 29.07.2024).
4. DIGITAL 2024: THE RUSSIAN FEDERATION // DataReport от 23.02.2024. URL: <https://datareportal.com/reports/digital-2024-russian-federation> (дата обращения: 29.07.2024).
5. В 2023 году в сеть утекло более 300 млн записей о россиянах // ТАСС : офиц. сайт. 2024. URL: <https://tass.ru/obschestvo/19693845> (дата обращения: 29.07.2024).
6. Суд оштрафовал «Яндекс.Еду» на 60 тыс. рублей из-за утечки данных // ТАСС : офиц. сайт. 2022. URL: <https://tass.ru/proisshestiya/14435979> (дата обращения: 29.07.2024).
7. Назначены наказания за громкие утечки данных из Минпросвещения, ЭКМО и «Роза Хутор» // Tadviser : офиц. сайт. 2023. URL: <https://kurl.ru/TsCMH> (дата обращения: 29.07.2024).
8. ВШЭ оштрафовали на 60 тысяч рублей // РИА Новости : офиц. сайт. 2023. URL: <https://ria.ru/20230510/vshe-1870861092.html> (дата обращения: 29.07.2024).
9. Волкова А. Ю. Персональные данные как объект уголовно-правовой охраны // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 132–137.
10. Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных : дис. ... канд. юрид. наук. Красноярск, 2017. 241 с.

References

1. Decree of the President of the Russian Federation dated 09.05.2017 No. 203 “O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody”. URL: <http://kremlin.ru/acts/bank/41919/page/1> (accessed: 29.07.2024). (In Russ.).
2. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation of 02.07.2021 No. 400. Collection of Legislation of the Russian Federation. 2021. No. 27 (Pt. II). Art. 5351. Accessed through Law assistance system “Garant”. (In Russ.).
3. Istoriya Interneta. RIA Novosti, 2024. URL: <https://ria.ru/20240312/internet-1932278255.html> (accessed: 29.07.2024). (In Russ.).
4. DIGITAL 2024: THE RUSSIAN FEDERATION. DataReportal, dated 23.02.2024. URL: <https://datareportal.com/reports/digital-2024-russian-federation> (accessed: 29.07.2024). (In Russ.).
5. V 2023 godu v set uteklo bolee 300 mln zapisey o rossiyanah. TASS, 2024. URL: <https://tass.ru/obschestvo/19693845> (accessed: 29.07.2024). (In Russ.).
6. Sud oshtrafoval “Yandeks.Edu” na 60 tys. rubley iz-za utechki dannyh. TASS, 2022. URL: <https://tass.ru/proisshestiya/14435979> (accessed: 29.07.2024). (In Russ.).
7. Naznacheny nakazaniya za gromkie utechki dannyh iz Minprosveshcheniya, EKSMO i “Roza Hutor”. Tadviser, 2023. URL: <https://kurl.ru/TsCMH> (accessed: 29.07.2024). (In Russ.).
8. VShE oshtrafovali na 60 tysyach rubley. RIA Novosti, 2023. URL: <https://ria.ru/20230510/vshe-1870861092.html> (accessed: 29.07.2024). (In Russ.).
9. Volkova A. Yu. Personalnye dannye kak obekt ugovorno-pravovoy ohrany. *Ugovornoe pravo: strategiya razvitiya v XXI veke*. 2023;(3):132–137. (In Russ.).
10. Gutnik S. I. Ugolovno-pravovaya harakteristika prestupnyh posyagatelstv v otnoshenii personalnyh dannyh: Cand. Sci. Thesis (Law). Krasnoyarsk, 2017. 241 p. (In Russ.).

11. Гвай А. М., Захарцев С. И. Уголовно-правовая охрана персональных данных: проблемные аспекты // Юридическая наука: история и современность. 2022. № 11. С. 66–71.
12. Чукреев В. А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 3. С. 107–116. <https://doi.org/10.17803/2311-5998.2022.91.3.107-116>.
13. Довголюк Н. В. Уголовно-правовая охрана персональных данных: необходимость совершенствования законодательства и дифференциации ответственности // Новеллы права, экономики и управления 2020 : сб. науч. тр. по материалам VI междунар. науч.-практич. конф., 25–26 ноября 2020 г., г. Гатчина. Гатчина : Государственный институт экономики, финансов, права и технологий, 2021. Т. 1. С. 301–305.
14. Герасимов А. М. Цифровые банки персональных генетических данных и их уголовно-правовая охрана // Уголовный закон в эпоху искусственного интеллекта и цифровизации : сб. тр. по материалам Всерос. науч.-практич. конф. с междунар. участием, 09 июня 2021 г., г. Саратов. Саратов : Саратовская государственная юридическая академия, 2021. С. 59–66.
15. Бахтеева Е. И., Жилиева Н. А. Уголовно-правовая защита персональных данных // Экономико-правовые проблемы обеспечения экономической безопасности : материалы III Междунар. науч.-практич. конф., 19 марта 2020 г., г. Екатеринбург / отв. редакторы Е. Б. Дворядкина, Г. З. Мансуров. Екатеринбург : Уральский государственный экономический университет, 2020. С. 146–148.
16. Бегишев И. Р., Кирпичников Д. В. Проблемные вопросы уголовно-правовой охраны персональных данных // Уголовная юстиция. 2020. № 15. С. 11–16.
17. Хохлова Е. В. Уголовно-правовая охрана персональных данных в зарубежных странах // Известия Юго-Западного государственного университета. Серия: История и право. 2022. Т. 12, № 4. С. 62–78.
18. Вабищевич В. В. Правовая охрана персональных данных в контексте их международно-правовой защиты // Вестник Белорусского государственного экономического университета. 2021. № 3. С. 107–118.
19. Заседание Совета по развитию гражданского общества и правам человека. URL: <http://www.kremlin.ru/events/president/news/70046> (дата обращения: 29.07.2024).
20. Принят законопроект об усилении ответственности за утечку персональных данных // Государственная Дума Федерального Собрания Российской Федерации. URL: <http://duma.gov.ru/news/58677/> (дата обращения: 29.07.2024).
21. Прозументов Л. М., Шеслер А. В. Криминология (Общая часть). Томск : Изд. Дом Томского государственного университета, 2017. 284 с.
11. Gvay A. M., Zakhartsev S. I. Uголовno-pravovaya ohrana personalnyh dannyh: problemnye aspekty. *Yuridicheskaya nauka: istoriya i sovremennost*. 2022;(11):66–71. (In Russ.).
12. Chukreev V. A. Personalnye dannye, v tom chisle biometricheskie dannye, kak predmety ugovolno-pravovoy ohrany. *Vestnik Universiteta imeni O. E. Kutafina (MGYUA)*. 2022;(3):107–116. <https://doi.org/10.17803/2311-5998.2022.91.3.107-116>. (In Russ.).
13. Dovgolyuk N. V. Uголовno-pravovaya ohrana personalnyh dannyh: neobhodimost sovershenstvovaniya zakonodatelstva i differentsiatsii otvetstvennosti. In: *Proceedings of the VI International Scientific and Practical Conference “Novelly prava, ekonomiki i upravleniya 2020”*, Gatchina, November 25–26, 2020. Gatchina: Gosudarstvennyy institut ekonomiki, finansov, prava i tekhnologiy, 2021. Vol. 1. P. 301–305. (In Russ.).
14. Gerasimov A. M. Tsifrovye banki personalnyh geneticheskikh dannyh i ih ugovolno-pravovaya ohrana. In: *Proceedings of the All-Russian scientific and practical conference with international participation within I Saratov International Legal Forum “Uголовnyy zakon v epohu iskusstvennogo intellekta i tsifrovizatsii”*, dedicated to the 90th anniversary of the Saratov State Law Academy, Saratov, June 09, 2021. Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2021. P. 59–66. (In Russ.).
15. Bahteeva E. I., Zhilyaeva N. A. Uголовno-pravovaya zashchita personalnyh dannyh. In: *Proceedings of the III International Scientific and Practical Conference “Ekonomiko-pravovye problemy obespecheniya ekonomicheskoy bezopasnosti”*, Ekaterinburg, March 19, 2020. Eds. E. B. Dvoryadkina, G. Z. Mansurov. Yekaterinburg: Uralskiy gosudarstvennyy ekonomicheskii universitet, 2020. P. 146–148. (In Russ.).
16. Begishev I. R., Kirpichnikov D. V. Problemnye voprosy ugovolno-pravovoy ohrany personalnyh dannyh. *Uголовnaya yustitsiya*. 2020;(15):11–16. (In Russ.).
17. Hohlova E. V. Uголовno-pravovaya ohrana personalnyh dannyh v zarubezhnykh stranah. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo*. 2022;12(4):62–78. (In Russ.).
18. Vabishchevich V. V. Pravovaya ohrana personalnyh dannyh v kontekste ih mezhdunarodno-pravovoy zashchity. *Vestnik Belorusskogo gosudarstvennogo ekonomicheskogo universiteta*. 2021;3(146):107–118. (In Russ.).
19. Zasedanie Soveta po razvitiyu grazhdanskogo obshchestva i pravam cheloveka. URL: <http://www.kremlin.ru/events/president/news/70046> (accessed: 29.07.2024). (In Russ.).
20. Prinyat zakonoproekt ob usilenii otvetstvennosti za utechku personalnyh dannyh. Gosudarstvennaya Duma Federalnogo Sobraniya Rossiyskoy Federatsii. URL: <http://duma.gov.ru/news/58677/> (accessed: 29.07.2024). (In Russ.).

22. В 2024 году в публичном доступе оказалось 150 баз российских компаний // РБК Компании : офиц. сайт. 2024. URL: <https://companies.rbc.ru/news/jSch3Zxqsc/v-2024-godu-v-publichnom-dostupe-okazalos-150-baz-rossijskih-kompanij/> (дата обращения: 29.07.2024).
23. МВД оценило ущерб от IT-преступлений в России за полтора года в более 210 млрд рублей // Интерфакс : офиц. сайт. 2024. URL: <https://www.interfax.ru/russia/964843> (дата обращения: 29.07.2024).
24. Фелелов П. А. Механизм уголовно-правовой охраны: основные методол. пробл. М. : Наука, 1992. 229 с.
25. Шеслер А. В., Шеслер С. С. Понятие и общественная опасность личности лица, совершающего преступления, связанные с незаконным оборотом наркотических средств // Вестник сибирского юридического института МВД России. 2019. № 3. С. 80–85.
26. В 2023 году в открытый доступ попало более 300 млн записей персональных данных // Frank Media : офиц. сайт. 2024. URL: <https://frankmedia.ru/150909> (дата обращения: 29.07.2024).
27. В России прошла целая серия утечек персональных данных // Российская газета : офиц. сайт. 2022. URL: <https://rg.ru/2022/10/03/so-vzломom-napereves.html> (дата обращения: 29.07.2024).
28. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2023 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: <https://мвд.рф/reports/item/47055751/?ysclid=lzjp8en5f713679786> (дата обращения: 29.07.2024).
29. Пухов А. А. Уголовно-правовая защита неприкосновенности частной жизни и персональных данных в свете изменений уголовного закона // Право. by. 2021. № 4. С. 85–92.
21. Prozumentov L. M., Shesler A. V. Kriminologiya (Obshchaya chast). Tomsk: Izdatelskiy Dom Tomskogo gosudarstvennogo universiteta, 2017. 284 p. (In Russ.).
22. V 2024 godu v publichnom dostupe okazalos 150 baz rossiyskih kompaniy. RBK Kompanii, 2024. URL: <https://companies.rbc.ru/news/jSch3Zxqsc/v-2024-godu-v-publichnom-dostupe-okazalos-150-baz-rossijskih-kompanij/> (accessed: 29.07.2024). (In Russ.).
23. MVD otsenilo ushcherb ot IT-prestupleniy v Rossii za poltora goda v bolee 210 mlrd. Rubley. Interfaks, 2024. URL: <https://www.interfax.ru/russia/964843> (accessed: 29.07.2024). (In Russ.).
24. Fefelov P. A. Mekhanizm ugodovno-pravovoy ohra-ny: main methodological problems. Moscow: Nauka, 1992. 229 p. (In Russ.).
25. Shesler A. V., Shesler S. S. The concept and social danger of the person committing crimes related with drugs. *Vestnik of Siberian Law Institute of the MIA of Russia*. 2019;(3):80–85. (In Russ.).
26. V 2023 godu v otkrytyy dostup popalo bolee 300 mln zapisey personalnyh dannyh. Frank Media, 2024. URL: <https://frankmedia.ru/150909> (accessed: 29.07.2024). (In Russ.).
27. V Rossii proshla tselaya seriya utechek personalnyh dannyh. Rossiyskaya gazeta, 2022. URL: <https://rg.ru/2022/10/03/so-vzломom-napereves.html> (accessed: 29.07.2024). (In Russ.).
28. Kratkaya harakteristika sostoyaniya prestupnosti v Rossiyskoy Federatsii za yanvar–dekabr 2023 goda. Ministerstvo vnutrennih del Rossiyskoy Federatsii. URL: <https://мвд.рф/reports/item/47055751/?ysclid=lzjp8en5f713679786> (accessed: 29.07.2024). (In Russ.).
29. Puhov A. A. Ugodovno-pravovaya zashchita neprikosnovennosti chastnoy zhizni i personalnyh dannyh v svete izmeneniy ugodovnogo zakona. *Pravo.by*. 2021;(4):85–92. (In Russ.).

Информация об авторах

Н. Ю. Акинина – кандидат юридических наук, доцент.

В. Ф. Анисимов – доктор юридических наук, доцент, профессор.

Р. В. Кочупалов – аспирант.

About the authors

Natalya Yu. Akinina – Candidate of Sciences (Law), Docent.

Valeriy F. Anisimov – Doctor of Sciences (Law), Docent, Professor.

Roman V. Kochupalov – Postgraduate.