

Современное состояние уголовно-правовой охраны персональных данных: зарубежный опыт

Аннотация. В условиях цифровой экономики персональные данные стали одним из ключевых активов, а с развитием технологий больших данных и искусственного интеллекта объемы собираемых и обрабатываемых персональных данных растут, что увеличивает риски их неправомерного использования. Утечки данных нарушают фундаментальные права на неприкосновенность частной жизни и ставят под угрозу личную безопасность. Согласно официальной статистике, за последние годы наблюдалось значительное увеличение числа инцидентов неправомерного доступа к компьютерной и персональной информации, что стимулировало повышение общественного осознания важности ее защиты. Результаты сравнительно-правового исследования уголовной ответственности за неправомерный доступ к персональным данным в соответствии со ст. 272.1 УК РФ и зарубежного законодательства в области уголовно-правовой охраны персональных данных демонстрируют, что эффективность уголовно-правовой защиты определяется не столько строгими наказаниями, сколько способностью государств адаптировать национальные законодательные акты к быстро меняющимся условиям глобализованного цифрового мира, а также интеграцией правовых норм для обеспечения трансграничной защиты интересов граждан своей страны.

Ключевые слова: персональные данные; киберпреступление; уголовная ответственность; информационные технологии; зарубежное законодательство; компьютерная информация; конфиденциальность; охрана личности; неправомерный доступ; трансграничные угрозы.

Для цитирования: Волкова А. Ю. Современное состояние уголовно-правовой охраны персональных данных: зарубежный опыт // Актуальные проблемы российского права. — 2025. — Т. 20. — № 10. — С. 183–190. — DOI: 10.17803/1994-1471.2025.179.10.183-190.

Current State of Criminal Law Protection of Personal Data: Foreign Experience

Alina Yu. Volkova, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Criminal and Penal Law, Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation
auvolkovs@mail.ru

Abstract. In the context of the digital economy, personal data has become one of the key assets. With the development of big data technologies and artificial intelligence, the volume of collected and processed personal data is growing, which increases the risks of its unlawful use. Data breaches violate fundamental rights to privacy

© Волкова А. Ю., 2025

* Волкова Алина Юрьевна, кандидат юридических наук, доцент, доцент кафедры уголовного и уголовно-исполнительного права Нижегородской академии МВД России
Анкудиновское ш., д. 3, г. Нижний Новгород, Российская Федерация, 603144
auvolkovs@mail.ru

and jeopardize personal safety. According to official statistics, recent years have seen a significant increase in the number of incidents involving unauthorized access to computer and personal information, which has stimulated greater public awareness of the importance of its protection. The results of a comparative legal study of criminal liability for unauthorized access to personal data under Article 272.1 of the Criminal Code of the Russian Federation and foreign legislation in the field of criminal law protection of personal data demonstrate that the effectiveness of criminal law protection is determined not so much by strict punishments, but by the ability of states to adapt national legislation to the rapidly changing conditions of a globalized digital world, as well as by the integration of legal norms to ensure cross-border protection of their citizens' interests.

Keywords: personal data; cybercrime; criminal liability; information technology; foreign legislation; computer information; confidentiality; personal security; unauthorized access; cross-border threats.

Cite as: Volkova AYu. Current State of Criminal Law Protection of Personal Data: Foreign Experience. *Aktual'nye problemy rossijskogo prava*. 2025;20(10):183-190. (In Russ.). DOI: 10.17803/1994-1471.2025.179.10.183-190.

Введение

В современную эпоху цифровизации проблема защиты персональных данных приобретает критическую актуальность ввиду стремительного развития информационных технологий, широкого распространения цифровых сервисов и возрастающих угроз киберпреступности. Персональные данные представляют собой ценный ресурс, который может быть использован как в благих целях, так и для нанесения ущерба. Безопасность персональных данных является серьезной проблемой для всех государственных органов и организаций, а также для всех частных лиц. Неправомерный доступ и распространение данных нарушают фундаментальные права на неприкосновенность частной жизни и ставят под угрозу личную безопасность. Согласно официальной статистике, за последние годы наблюдалось значительное увеличение числа инцидентов неправомерного доступа к компьютерной и персональной информации, что стимулировало повышение общественного осознания важности ее защиты. Так, за пять лет количество зарегистрированных преступлений, связанных с неправомерным доступом к компьютерной информации, которая включает в себя охраняемые персональные

данные, характеризуется беспрецедентным ростом: 2019 г. — 2 420 преступлений; 2020 г. — 4 105; 2021 г. — 6 392; 2022 г. — 9 308; 2023 г. — 36 788. За 2024 г. зарегистрировано 105 311 преступлений, предусмотренных статьей 272 УК РФ¹.

В рамках уголовной доктрины неоднократно выдвигались предложения относительно совершенствования уголовного законодательства в области надлежащей охраны персональных данных в качестве самостоятельного объекта в целях эффективного противодействия новым вызовам и угрозам. Предложения можно разделить по направлениям совершенствования отечественного уголовного закона:

1) отдельные предложения направлены на усиление ответственности за посягательства в отношении персональных данных: предлагается дифференцировать ответственность в зависимости от масштаба наступивших последствий в виде ущерба или же последствий для владельцев персональных данных²;

2) некоторые касаются уточнения формулировок статей УК РФ: введение новых составов преступлений, связанных с неправомерным доступом к персональным данным, включая вредоносное программное обеспечение; уточнение диспозиций ст. 137 и 272 УК РФ в части

¹ Информация о состоянии преступности на территории Российской Федерации: данные ГИАЦ МВД России // URL: <https://мвд.рф/reports> (дата обращения: 05.02.2024).

² См., например: Сердюкова Е. В., Чуниха А. А., Зиновьева Е. О. Особенности уголовной ответственности за преступления в сфере компьютерной информации // *Eastern European Scientific Journal*. 2021. № 8-1 (72). С. 57–59.

установления квалифицирующих признаков, касающихся персональных данных³;

3) встречаются высказывания об адаптации норм к современным вызовам цифровой эпохи⁴ и построению международного сотрудничества в сфере обеспечения безопасности персональных данных⁵.

Федеральным законом от 30.11.2024 № 421-ФЗ⁶ в отечественный уголовный закон была введена статья 272.1, предусматривающая ответственность за незаконные использование и/или передачу, сбор и/или хранение компьютерной информации, содержащей персональные данные, а равно создание и/или обеспечение функционирования информационных ресурсов для хранения или распространения подобной информации. Эта норма отражает реакцию законодателя на небывалый рост числа преступных посягательств в отношении персональных данных, но об эффективности нормы еще рано судить. Ввиду этого следует обратиться к зарубежному опыту уголовно-правовой охраны персональных данных, чтобы выявить уже имеющийся положительный опыт уголовно-правовой охраны персональных данных.

Основная часть исследования

Многие страны стремятся сформировать эффективные правовые механизмы для охраны персональных данных, вводя строгие нормы, регули-

рующие их сбор, обработку и хранение, включающие и нормы уголовной ответственности. На настоящий момент персональные данные — это в первую очередь личная информация, соответственно, государству и организациям она передается на определенных условиях, а не на праве собственности. Хотя имеются отдельные точки зрения об установлении права собственности на персональные данные⁷, сейчас они не нашли должного отражения в системе правового регулирования оборота персональных данных. Уголовно-правовая охрана персональных данных — неотъемлемый компонент этой системы, обеспечивающий защиту граждан от неправомерных посягательств, так как информационные ресурсы в виде персональных данных личности не только позволяют идентифицировать личность, но и повсеместно используются в различных сферах общественной жизни. Зарубежные авторы отмечают, что персональные данные служат ключевым ресурсом для целевой рекламы и персонального профилирования в сети «Интернет»⁸, что в условиях цифровой экономики не исключает преступного вмешательства. По мнению В. Ю. Арчакова, А. Л. Баньковского, А. Ф. Мательского, зарубежный опыт защиты персональных данных может быть востребованным для его потенциального использования при совершенствовании отечественного законодательства⁹. В статье проводится исследование актуального зарубежного законодательства в области уголовно-правовой охраны персональ-

³ См., например: Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных : дис. ... канд. юрид. наук. Владивосток, 2017 ; Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : дис. ... канд. юрид. наук. М., 2016.

⁴ См., например: Малюк А. А. Защита информации в информационном обществе : учебное пособие для вузов. М. : Горячая линия — Телеком, 2015 ; Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. 2019. № 1. С. 108–118.

⁵ См., например: Талапина Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117–150.

⁶ СЗ РФ. 2024. № 49 (ч. IV). Ст. 7412.

⁷ Determann L. No One Owns Data // Hastings Law Journal. 2019. Vol. 70. № 1. P. 5.

⁸ Wheeler A., Winburn M. Cloud Storage Security: A Practical Guide (Computer Science Reviews and Trends) // Elsevier Inc., 2015. P. 75–98.

⁹ Арчаков В. Ю., Баньковский А. Л., Мательский А. Ф. Зарубежный опыт защиты персональных данных и меры ответственности за их распространение // Право.by. 2021. № S5 (73). С. 57.

ных данных с целью выявить и перенять положительный опыт правового регулирования.

Один из наиболее значимых нормативных актов в сфере охраны персональных данных — Общий регламент защиты персональных данных (General Data Protection Regulation — GDPR) Европейского Союза, вступивший в силу в мае 2018 г.¹⁰ GDPR ввел строгие требования к обработке персональных данных и серьезные санкции за их нарушение, что делает его одной из самых прогрессивных правовых инициатив в сфере информационной безопасности. Непосредственно Регламент устанавливает лишь административные штрафы за нарушения в сфере оборота персональных данных, но в соответствии со ст. 84 страны — участницы Европейского Союза (ЕС) вправе установить нормы иной ответственности, возможной за нарушение GDPR.

Из стран — участниц Европейского Союза Германия, Франция и Испания уже ввели в уголовное законодательство нормы за неправомерный доступ, использование и распространение персональных данных. Рассмотрим более подробно имплементацию GDPR в национальное законодательство отдельных европейских стран.

В Уголовном кодексе **Федеративной Республики Германия**¹¹, в частности, § 202a устанавливает, что неправомерное использование персональных данных может повлечь лишение свободы до трех лет, если персональные данные хранятся или передаются электронным, магнитным или иными способами. Эта норма находится в разделе 15, определяющем преступность посягательств на неприкосновенность частной жизни. Но особенностью установления

уголовной ответственности в Германии за неправомерный доступ к персональным данным личности является отсутствие квалифицирующих признаков в § 202a–202d в виде возможного ущерба, не дифференцируется важность тех или иных категорий персональных данных. На основании чего можно сказать, что недавно введенная статья 272.1 УК РФ более полно описывает и дифференцирует степень общественной опасности посягательств на неприкосновенность персональных данных в зависимости от специфики объекта уголовно-правовой охраны. Уголовный закон ФРГ предполагает также иное представление персональных данных в качестве объекта уголовно-правовой охраны: фотоснимки, видео и аудиозаписи и др.¹² Но не определяются возможные последствия, мотивы виновных или способы совершения преступлений.

Во **французском уголовном законодательстве** выделяется несколько групп преступлений в отношении персональных данных. Преступные посягательства можно условно разделить на следующие категории в зависимости от непосредственного объекта:

- 1) нарушения условий обработки персональных данных уполномоченными лицами (например, *ст. 226-20 УК Франции*¹³ — хранение персональных данных свыше срока, указанного в согласии на обработку персональных данных);
- 2) нарушения режима сбора и хранения персональных данных, не связанные с их обработкой уполномоченными лицами и учреждениями (например, *ст. 226-18 УК Франции* — сбор данных обманным, самоуправным или иным запрещенным законом способом);
- 3) посягательства в отношении тех или иных категорий персональных данных, обладающих

¹⁰ Постановление Европейского парламента и Совета Европейского Союза «Общий регламент защиты персональных данных (GDPR) Европейского Союза», 2016 г. // URL: <https://gdpr-text.com/ru/> (дата обращения: 07.02.2025).

¹¹ Уголовный кодекс (StGB) Федеративной Республики Германия (ред. от 07.11.2024) // Das Bundesamt für Justiz. URL: https://www.gesetze-im-internet.de/stgb/_202a.html (дата обращения: 07.02.2025).

¹² Головинков П. В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: Strafgesetzbuch (StGB) : научно-практический комментарий и перевод текста закона. Потсдам : Universitätsverlag Potsdam, 2021. С. 187.

¹³ Уголовный кодекс Франции от 22.07.1992 // Légifrance — Le service public de la diffusion du droit. URL: legifrance.gouv.fr (дата обращения: 20.01.2025).

повышенным уровнем правовой охраны (например, персональные данные, которые прямо или косвенно раскрывают расовое или этническое происхождение, взгляды политические, философские или религиозные, или членство лиц в профсоюзе, или связанные с их здоровьем, или сексуальной ориентацией, или гендерной идентичностью, — *ст. 226-19 УК Франции*). Тем самым можно отметить не только комплексный подход к уголовно-правовой охране персональных данных на территории Франции, но и дифференцированный подход к установлению преступности деяний в зависимости от специфики персональных данных.

В **Великобритании** отсутствует единый кодифицированный уголовный закон, но уголовно-правовая охрана персональных данных осуществляется в соответствии с Законом «О защите персональных данных» (*Data Protection Act — DPA, 2018*)¹⁴, который конкретизирует положения GDPR ЕС. Статья 170 названного Закона устанавливает ответственность за незаконные действия в отношении персональных данных, включая их продажу и предложение продажи (ч. 4, 5 ст. 170 DPA). Особый интерес представляет статья 184 DPA, которая устанавливает ответственность за требования (без соответствующего основания) передачи персональных данных как условия трудоустройства или заключения договора на оказание услуг. Оба указанных действия не имеют прямой аналогии в отечественном уголовном законе, но продажу персональных данных можно сравнить с передачей и сбором персональных данных, совершенными из корыстной заинтересованности. В целом же напрашивается вывод, что положения DPA более конкретизированы под процессы взаимодействия с персональными данными и их использования в тех или иных целях.

Соединенные Штаты Америки обеспечивают уголовно-правовую охрану персональных

данных на основе множества федеральных законов и законов отдельных штатов, таких как Закон 1996 г. «О конфиденциальности медицинской информации» и Закон штата Калифорния «О защите персональных данных потребителей» (CCPA). В отличие от централизованного подхода в странах Европы, в США защита данных осуществляется децентрализованно, что приводит к вариативности уголовной ответственности в зависимости от государственной или местной юрисдикции. Разрозненность правовой базы затрудняет единообразное правоприменение и ограничивает эффективность защиты персональных данных в масштабах всей страны.

Хотелось бы рассмотреть законодательство **Австралии** ввиду специфики сложившегося режима правового регулирования в области уголовно-правовой охраны персональных данных. Применение GDPR ЕС допускается только к австралийским организациям, имеющим установленное присутствие в ЕС, например филиал в одном или нескольких государствах — членах ЕС, но сама страна не обязана приводить свое законодательство в соответствие с этим Регламентом.

Относительно уголовно-правовой охраны персональных данных Уголовный кодекс Австралии¹⁵ содержит положения, не конкретизированные под их специфику (*Division 122 — Secrecy of information*). В случае вмешательства в личную жизнь путем разглашения персональных данных или же распространения сведений, касающихся кредитной информации личности, применяется Закон о конфиденциальности (*Privacy Act 1988 г.*)¹⁶, который предусматривает ответственность в виде штрафных санкций за действия, связанные с нарушением защиты данных. В настоящее время австралийское законодательство в части уголовно-правовой охраны персональных данных находится на начальном этапе своего развития, но надлежащее обраче-

¹⁴ Legislation Government UK. URL: <https://www.legislation.gov.uk/ukpga/2018/12/contents> (дата обращения: 11.02.2025).

¹⁵ Уголовный кодекс Австралии 1995 г. // Attorney-General's Department Australia. URL: <https://www.ag.gov.au/> (дата обращения: 11.02.2025).

¹⁶ Закон Австралии о конфиденциальности 1988 г. // Федеральный реестр законодательства Австралии. URL: <https://www.legislation.gov.au/C2004A03712/2019-08-13/text> (дата обращения: 11.02.2025).

ние с подобной информацией обеспечивается иными нормативными актами Австралийского Содружества.

В Уголовный кодекс **Китайской Народной Республики** в 2009 г.¹⁷ была введена статья 253.1, устанавливающая ответственность за противоправные действия в виде неправомерного доступа, кражи, приобретения и продажи персональной информации граждан. Между тем всё чаще посягательства на персональную информацию граждан происходят в форме ее незаконного использования. Такие нарушения представляют серьезную общественную опасность, но еще не урегулированы уголовным законодательством¹⁸.

Специфика правового регулирования **Японии** определяет возможность привлечения к уголовной ответственности в соответствии с иными нормативными источниками, например Законом «О защите личной информации»¹⁹, а не только согласно Уголовному кодексу Японии 1907 г. Закон Японии 2003 г. «О защите личной информации» в разд. VIII (ст. 176–185) определяет меры уголовной ответственности за неправомерные действия в отношении персональной информации, дефиниция которой дается в ст. 2 данного нормативного акта. Отличительная черта уголовно-правовой охраны персональных данных в Японии — удобство нормативного источника: статья 2 подробно определяет статус информации как персональных данных, раздел VIII устанавливает степень общественной опасности того или иного посягательства.

В **Южной Корее** уголовно-правовая охрана персональных данных обеспечивается Законом 2011 г. «О защите персональной информации» (Personal Information Protection Act — PIPA)²⁰. Этот Закон устанавливает один из самых строгих

в мире режимов защиты персональных данных, который обеспечивается многочисленными обязательствами организаций в сфере обеспечения охраны данной информации, а также широким перечнем действий, которые признаются преступными (ст. 70–74.2). Например: получение персональных данных путем мошенничества или иным незаконным способом (ч. 2 ст. 70); разглашение персональных данных, полученных при исполнении своих обязанностей (ч. 3 ст. 72); непринятие мер по удалению персональных данных по истечении срока их хранения (ч. 2 ст. 73) и др. Помимо наказания в виде лишения свободы или штрафа за указанные действия Закон PIPA предполагает возможность конфискации или взыскания прибыли, полученной в связи с совершением преступлений, предусмотренных статьями 70–73, что действительно обеспечивает серьезный уровень предупреждения посягательств в отношении персональных данных.

Выводы

Анализ зарубежного опыта показывает, что для достижения высокого уровня защиты персональных данных необходима комплексная стратегия, включающая как организационные меры, так и совершенствование уголовного законодательства. Страны ЕС демонстрируют централизованный и жесткий подход к регулированию оборота персональных данных и нарушениям мер по его обеспечению, что помогает достичь высокой степени защищенности персональной информации. В противоположность этому США применяют более гибкую и децентрализованную систему, которая предоставляет отдельным

¹⁷ Уголовный кодекс Китайской Народной Республики 1997 г. // Asian Legal Information Institute. URL: <http://www.asianlii.org/cn/legis/cen/laws/clotproc361/> (дата обращения: 12.02.2025).

¹⁸ Пан Дунмэй, Фу Сянсян. Уголовно-правовая защита персональной информации граждан в Китае: доктрина, законодательная регламентация, правоприменение // Всероссийский криминологический журнал. 2022. № 1. С. 131.

¹⁹ Закон Японии «О защите личной информации» 2003 г. // Japanese Law Translation Database System. URL: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#je_ch1 (дата обращения: 12.02.2025).

²⁰ Закон Южной Кореи «О защите персональной информации» 2011 г. // Korea Legislation research institute. URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=KOR (дата обращения: 12.02.2025).

штатам возможность адаптировать правовые нормы в соответствии с предписаниями местного законодательства, однако это значительно снижает степень унифицированного контроля. В странах Азии, таких как КНР, Япония и Южная Корея, законодательство направлено на строгое противодействие посягательствам в отношении персональных данных, что позволяет эффективно минимизировать риски неправомерного доступа к ним и их использования в преступных целях.

Современное состояние уголовно-правовой охраны персональных данных в различных странах иллюстрирует намерение государств обеспечить максимальную защиту прав граждан в условиях нарастающих угроз, связанных с утечкой и неправомерным использованием личной информации. По мнению В. В. Вабищевича, существующий уровень уголовно-правовой охраны в странах Европейского Союза способствует эффективному исполнению законодательства о персональных данных ввиду серьезности предусмотренных наказаний за подобные посягательства²¹. Считаем, что эффективность такой защиты определяется не только строгими наказаниями, но и способностью государств адаптировать национальные законодательные акты к

быстро меняющимся условиям глобализованного мира, а также интеграцией правовых норм для обеспечения трансграничной защиты интересов граждан своей страны.

Законодательство каждой страны интерпретирует персональные данные как информационный ресурс, с помощью которого можно идентифицировать человека как личность, его предпочтения, маршруты передвижения, профессиональные навыки и т.п. Подобный пласт информации при использовании в преступных целях не только серьезно облегчает совершение противоправных действий, но и дестабилизирует экономическую ситуацию, в исключительных случаях возможны угрозы для безопасности государства.

Современный уровень безопасности персональных данных остается неоднородным: несмотря на строгость законодательства в ряде стран, практическое его исполнение часто сталкивается с трудностями, особенно в трансграничных ситуациях. Для повышения уровня защищенности требуется более глубокая гармонизация национального законодательства стран и международная координация усилий, что позволит предотвратить использование персональных данных в тех или иных преступных целях.

БИБЛИОГРАФИЯ

1. Арчаков В. Ю., Баньковский А. Л., Мательский А. Ф. Зарубежный опыт защиты персональных данных и меры ответственности за их распространение // *Право.by*. — 2021. — № 55 (73). — С. 52–59.
2. Вабищевич В. В. Зарубежный опыт уголовно-правовой охраны персональных данных // *Журнал Белорусского государственного университета. Право*. — 2019. — № 1. — С. 72–80.
3. Головненков П. В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: *Strafgesetzbuch (StGB)* : научно-практический комментарий и перевод текста закона. — Потсдам : Universitätsverlag Potsdam, 2021. — 311 с.
4. Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных : автореф. дис. ... канд. юрид. наук. — Владивосток, 2017. — 241 с.
5. Малюк А. А. Защита информации в информационном обществе : учебное пособие для вузов. — М. : Горячая линия — Телеком, 2015. — 230 с.
6. Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты : дис. ... канд. юрид. наук. — М., 2016. — 40 с.

²¹ Вабищевич В. В. Зарубежный опыт уголовно-правовой охраны персональных данных // *Журнал Белорусского государственного университета. Право*. 2019. № 1. С. 79.

7. Пан Дунмэй, Фу Сянсян. Уголовно-правовая защита персональной информации граждан в Китае: доктрина, законодательная регламентация, правоприменение // Всероссийский криминологический журнал. — 2022. — № 1. — С. 122–134.
8. Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. — 2019. — № 1. — С. 108–118.
9. Сердюкова Е. В., Чуниха А. А., Зиновьева Е. О. Особенности уголовной ответственности за преступления в сфере компьютерной информации // Eastern European Scientific Journal. — 2021. — № 8-1 (72). — С. 57–59.
10. Талапина Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. — 2018. — № 5. — С. 117–150.
11. Determann L. No One Owns Data // Hastings Law Journal. — 2019. — Vol. 70. — № 1. — 45 p.
12. Wheeler A., Winburn M. Cloud Storage Security: A Practical Guide (Computer Science Reviews and Trends). — Elsevier Inc., 2015. — 144 p.

Материал поступил в редакцию 11 февраля 2025 г.

REFERENCES (TRANSLITERATION)

1. Archakov V. Yu., Bankovskiy A. L., Matelskiy A. F. Zarubezhnyy opyt zashchity personalnykh dannykh i mery otvetstvennosti za ikh rasprostranenie // Pravo.by. — 2021. — № S5 (73). — S. 52–59.
2. Vabishchevich V. V. Zarubezhnyy opyt ugovovno-pravovoy okhrany personalnykh dannykh // Zhurnal Belorusskogo gosudarstvennogo universiteta. Pravo. — 2019. — № 1. — S. 72–80.
3. Golovnenkov P. V. Uголовное ulozhenie (Uголовный kodeks) Federativnoy Respubliki Germaniya: Strafgesetzbuch (StGB): nauchno-prakticheskiy kommentariy i perevod teksta zakona. — Potsdam: Universitätsverlag Potsdam, 2021. — 311 s.
4. Gutnik S. I. Uголовно-pravovaya kharakteristika prestupnykh posyagatelstv v otnoshenii personalnykh dannykh: avtoref. dis. ... kand. yurid. nauk. — Vladivostok, 2017. — 241 s.
5. Malyuk A. A. Zashchita informatsii v informatsionnom obshchestve: uchebnoe posobie dlya vuzov. — M.: Goryachaya liniya — Telekom, 2015. — 230 s.
6. Mnatsakanyan A. V. Informatsionnaya bezopasnost v Rossiyskoy Federatsii: ugovovno-pravovye aspekty: dis. ... kand. yurid. nauk. — M., 2016. — 40 s.
7. Pan Dunmey, Fu Syansyan. Uголовно-pravovaya zashchita personalnoy informatsii grazhdan v Kitae: doktrina, zakonodatel'naya reglamentatsiya, pravoprimeneniye // Vserossiyskiy kriminologicheskiy zhurnal. — 2022. — № 1. — S. 122–134.
8. Rassolov I. M., Chubukova S. G., Mikurova I. V. Biometriya v kontekste personalnykh dannykh i geneticheskoy informatsii: pravovye problemy // Lex russica. — 2019. — № 1. — S. 108–118.
9. Serdyukova E. V., Chunikha A. A., Zinoveva E. O. Osobennosti ugovovnoy otvetstvennosti za prestupleniya v sfere kompyuternoy informatsii // Eastern European Scientific Journal. — 2021. — № 8-1 (72). — S. 57–59.
10. Talapina E. V. Zashchita personalnykh dannykh v tsifrovuyu epokhu: rossiyskoe pravo v evropeyskom kontekste // Trudy Instituta gosudarstva i prava RAN. — 2018. — № 5. — S. 117–150.
11. Determann L. No One Owns Data // Hastings Law Journal. — 2019. — Vol. 70. — № 1. — 45 p.
12. Wheeler A., Winburn M. Cloud Storage Security: A Practical Guide (Computer Science Reviews and Trends). — Elsevier Inc., 2015. — 144 p.