

Гавчук Д.В.♦

DOI: 10.25108/2304-1730-1749.iolr.2024.75.51-60

УДК: 347

### Защита персональных данных в индустрии гостеприимства как цель устойчивого развития

**Аннотация:** Актуальность данного исследования ознаменована тем, что индустрия гостеприимства во все большей степени полагается на сбор и обработку персональных данных своих гостей. От бронирования номеров до заказа еды и напитков, службы доставки, рестораны и отели собирают и хранят обширную информацию о своих гостях. Поскольку уважение к конфиденциальности становится все более важной проблемой для потребителей, для индустрии гостеприимства становится критически важным защищать персональные данные и соответствовать нормативным требованиям по защите данных.

**Ключевые слова:** персональные данные; гражданское право; нематериальные блага; согласие на обработку персональных данных; сделка.

Объектом исследования выступает защита персональных данных гостей российского ресторанного и отельного бизнеса.

**Методологическую основу** исследования составляют труды отечественных и зарубежных ученых, изучающих данную тематику.

**Степень научной разработанности проблемы:** Первую из них составляют публикации, подготовленные по отдельным проблемам уголовно-правовой охраны частной жизни и персональных данных. Это труды Э.И. Атагимовой, С.В. Барина, И.Р. Бегишева, К.С. Беловой, Л.А. Букалеровой, М.А. Бучаковой, Е.С. Вологдиной, А.С. Горденко, В.Е. Дивольд, М.А. Дударевой, А.С. Журавлевой, Г.Г. Камаловой, О.С. Капинус, Д.В. Карелина, Д.В. Кирпичникова, Д.А. Конева, Ю.А. Кузьмина, Э.Ю. Латыповой, В.А. Мазурова, А.В. Макарова, Е.О. Машуковой, Т.Н. Нуркаевой, А.С. Озеровой, А.А. Павлинова, Н.И. Пикурова, А.Т. Потемкиной, М.А. Радовой, Е.А. Русскевича, Е.Н. Рязановой, В.С. Соловьева, С.А. Стяжкиной, А.Р. Сысенко, А.С. Унуковича, М.А. Филатовой, Э.Т. Халиулиной, И.Г. Цопановой, В.А. Чукреева, А.А. Шутовой, И.А. Юрченко и др.

Вторую группу составили научные работы по проблеме права на защиту персональных данных в контексте конституционного права на неприкосновенность частной жизни, личную или семейную тайну М.Ю. Авдеева, И.А. Вельдера, И.В. Винюковой, Ю.А. Говенко, С.П. Гришаева, В.М. Елина, А.А. Елисеевой, А.К. Жаровой, В.П. Иванского, Д.А. Ильютювича, Н.Е. Крыловой, С.Е. Кузахметовой, Б.М. Леонтьева, М.Н. Малеиной, Л.Г. Мачковского, Е.А. Миндровой, И.А. Михайловой, В.А. Новикова, С.Ю. Пашаева, И.Л. Петрухина, М.И. Проскуряковой, В.Д. Рузановой, О.Ф. Засемковой, Т.Ю. Сапранковой, О.В. Судаковой, Ю.С. Телиной, А.Х. Хуаде, Э.А. Цадыковой, И.А. Шевченко и др.

♦ Гавчук Денис Васильевич - магистрант права Московского финансово-правового университета «Синергия», член Торгово-промышленной палаты РФ (Российская Федерация). E-mail: midk@bk.ru

Третья группа источников включает научные труды представителей науки информационного права и общей теории права по вопросам защиты персональных данных: М.С. Абламейко, М.Н. Алексашиной, А.И. Алексеенцева, Е.В. Андреевой, В.В. Архипова, О.В. Афанасьевой, И.Л. Бачило, М.В. Бундина, М.А. Важоровой, А.В. Губаревой, А.Н. Гулемина, Е.К. Волчинской, В.В. Дятленко, И.С. Иванова, В.Н. Лопатина, А.В. Минбалеева, А.Г. Мираева, В.Б. Наумова, В.В. Павлюкова, В.Н. Петрова, Н.И. Петрыкиной, С.Г. Пилипенко, Н.И. Платоновой, О.Б. Просветовой, А.И. Савельева, В.И. Солдатовой, Л.К. Терещенко, А.С. Федосина, М.А. Федотова, Н.Е. Циулиной и др.

Современное общество сталкивается с растущим количеством угроз в сфере информационной безопасности. С каждым днем мы все больше становимся зависимы от цифровых технологий – от социальных сетей до онлайн-банкинга, от медицинских записей до электронной почты. Однако, с развитием цифровых технологий появляются новые уязвимости и риски.

Персональные данные как высокодоходный «товар» стали первопричиной образования и тотального разрастания в Российской Федерации подпольного рынка торговли конфиденциальной информацией о человеке. О масштабной трансформации этого теневого сегмента свидетельствуют закрытые интернет-платформы, на которых размещены массовые объявления о сбыте информационных массивов – баз данных, содержащих миллионное количество строк-записей о гражданах.

Персональные данные – крайне широкая категория, охватывающая любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу. Понимание того, являются ли определенные сведения персональными данными в совокупности с информированностью о соответствующем законодательном регулировании, позволяет гражданину эффективно защищать свои права, в частности, следить за распространением своих персональных данных и соблюдением требований к их обработке, требовать их удаления. «Персональная информация является новой нефтью Интернета и валютой в цифровом мире» [13]. Такое сравнение не случайно. Надо иметь четкое представление о таком ценном активе.

"Российский рынок данных — быстрорастущий и перспективный. По прогнозам экспертов, к 2030 году его объем достигнет 800 миллиардов рублей, а применение технологий искусственного интеллекта добавит более 11 триллионов рублей к ВВП", - заявил вице-премьер РФ Дмитрий Чернышенко. Он напомнил, что Президент РФ Владимир Путин поручил запустить новый национальный проект "Экономика данных". В его рамках будут развиваться ключевые технологические направления, включая квантовые технологии, облачные сервисы, искусственный интеллект и платформенные технологические решения, а для выполнения нацпроекта будут запущены 10 федеральных проектов [12].

Сфера гостеприимства постоянно подвержена повышенной опасности утечки информации. По данным аналитического центра Falcongaze, каждая восьмая утечка происходит именно в этой области.

В базах данных таких компаний хранится огромное количество информации об адресах, платежеспособности и личности их клиентов. Гостиницы, рестораны и туристические фирмы — одни из основных источников краденых номеров кредитных и дебетовых карт. Обычно их системы безопасности защищены не так хорошо, как, например, у предприятий в

финансовом и страховом секторе, поэтому в глазах злоумышленников они являются более уязвимой целью.

Один из первых громких случаев массовой утечки данных связан как раз с похищением информации в сфере гостеприимства. В 2006 году были скомпрометированы данные 234 000 пользователей сайта Hotels.com. А в мае 2015, взломаны были системы казино и отеля Hard Rock в Лас-Вегасе. Преступники получили доступ к информации о банковских картах посетителей заведения. На протяжении пяти месяцев вредоносное ПО находилось в системе и незаметно «сливало» данные злоумышленникам [5].

Отели Marriott обнаружили это на собственном опыте в 2020 году, когда были скомпрометированы семь миллионов профилей гостей. Хакеры собрали такие данные, как имена, номера телефонов и паспортов. Ключи расшифровки, сохраненные на том же сервере, также были просмотрены вместе с зашифрованной информацией о кредитной карте. В октябре 2020 года офис Комиссара Великобритании по информации уличил Marriott в нарушении законов страны о конфиденциальности данных и наложил штраф в размере 18,4 миллиона фунтов стерлингов. Хотя это было бы серьезным финансовым ударом, ущерб их репутации мог бы обойтись гораздо дороже.

MGM Resorts International, The Ritz в Лондоне и Choice Hotels International - другие крупные бренды, также пострадавшие от громких краж данных. Это демонстрирует, насколько гостиничные компании являются серьезной мишенью для хакеров и киберпреступников из-за объема хранящихся у них ценных данных.

Неслучайно в указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» в качестве целей государственной политики обозначены снижение до минимально возможного уровня количества утечек персональных данных и нарушений требований по их защите, а также обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий (п. 57).

В 2022 году прошла реформа законодательства о персональных данных, и у субъектов предпринимательской деятельности появились новые обязанности по взаимодействию с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Чтобы оценить масштаб проблемы: только в Москве 1900 гостиниц и хостелов с номерным фондом на 87 128 мест. По статистике, в среднем гостиницы загружены на 60-80%. Даже если брать по минимуму, то ежедневно в организациях сферы гостеприимства «оседает» около 52 200 скан-копий паспортов, которые никто не охраняет. И это только в столице РФ.

В 2023 году по РФ путешествовало 78 млн россиян [1]. Даже если поделить эту цифру пополам, количество незащищенных персональных данных остается слишком велико, чтобы не обращать на проблему внимания.

Кроме гостиниц, паспорта сканируют в фитнес- и бизнес-центрах, на проходных режимных объектов и даже в развлекательных учреждениях.

#### **Устойчивое развитие и защита данных**

В условиях стремительного развития информационных технологий и масштабной цифровизации персональные данные стали ценным активом, генерирующим новые возможности для создания экономической и социальной ценности, что привело к включению данного во-

проса во все элементы ESG-повестки и привлечению внимания к нему как со стороны клиентов компаний, так и со стороны инвесторов, акционеров и иных заинтересованных лиц.

Устойчивое развитие — это концепция, которая охватывает социальные, экономические и экологические аспекты. Защита персональных данных является важнейшим критерием информационной безопасности страны и неотъемлемой частью социальной устойчивости, поскольку она защищает основные права и свободы людей. Нарушения защиты персональных данных могут привести к потере доверия, финансовым потерям и ущербу репутации [3].

В настоящее время компании, придерживающиеся ESG-принципов и стандартов ответственного ведения бизнеса, должны принимать меры по обеспечению конфиденциальности информации, собираемой ими и ее защите от несанкционированного доступа и разглашения. Соответствующие меры могут быть интегрированы в ESG-политику компании.

В марте 2022 года количество кибератак, совершенных Украиной и Россией и от их имени, исследователи Check Point Software (CPR) называли «ошеломляющим». Около 400 000 международных хакеров вызвались помочь противостоять цифровым атакам России, заявлял президент CyberProof и один из бывших руководителей министерства разведки Израиля Юваль Воллман [14]. «Впервые в истории любой желающий может присоединиться к кибервойне, — рассуждал в интервью CNBC Лотем Финкельштейн, руководитель направления киберразведки CPR. — Мы видим участие всего киберсообщества, в котором группировки и отдельные лица приняли сторону либо России, либо Украины» [15].

«Количество кибератак на российскую информационную инфраструктуру все последние годы постоянно растёт – именно все последние годы, ну а с началом специальной военной операции на Донбассе, на Украине вызовы в этой сфере стали ещё более острыми и серьёзными, более масштабными. По сути, против России развязана настоящая агрессия, война в информационном пространстве» - сообщил Владимир Путин на заседании Совета Безопасности РФ [2].

Info Watch описывает то, как в общий доступ утекают персональные данные. В феврале 2022 года сервис «Яндекс.Еда» упустил в Сеть миллионы данных пользователей включая фамилии, номера телефонов, адреса доставок, компания первоначально заявляла, что причиной инцидента стали недобросовестные действия персонала, но новая версия – утечка была реализована с помощью хакерской атаки на внешнюю инфраструктуру.

На памяти также сливы от другого сервиса доставки еды – Delivery Club. В мае отличилась сеть медицинских лабораторий «Гемотест», которая допустила утечку двух баз данных на 0,5 млрд. заказов и 31 млн строк с информацией, причем там были и ФИО, и даты рождения, и адреса, и номера телефонов, и электронная почта, и даже серии и номера паспортов, а в довесок – результаты анализов. При большом желании базы можно сверять с данными из ГИБДД, операторов сотовой связи, микрофинансовых организаций, соцсетей, сервисов по продаже билетов, онлайн-кинотеатров и банков [6].

За 2023 год в Сеть утекли 240 млн. уникальных телефонных номеров россиян, говорится в исследовании сервиса DLBI. Всего в Роскомнадзоре за год зафиксировали 168 сливов персональных данных. Лидеры по утечкам — ритейл и банки. От целевых атак хакеры перешли к массовым. Взломы баз компаний — это часть гибридной войны против России, подчеркнули в Роскомнадзоре. Чтобы защитить россиян, власти хотят ввести для организаций оборотные штрафы — такой подход поддерживают в Минцифры и Центробанке. Также в стране может появиться механизм компенсации для пострадавших [4].

На рынке все больше сервисов, позволяющих создать цифровую копию человека, которая может превосходить «оригинал» по тем или иным параметрам. Вскоре развитие технологий позволит бизнесменам и политикам общаться от имени цифровой личности так, что клиенты и избиратели даже не заметят подмены, а большим брендам — проводить свои маркетинговые кампании. О рисках, связанных с этим процессом пишет преподаватель НИУ ВШЭ Анна Подпрятва [7].

В России наблюдается лавинообразный рост потерь персональных данных, коммерческой или личной информации. Число доступных на сером рынке персональных записей уже в несколько раз превысило население нашей страны. Фактически почти все население страны существует в режиме полной информационной беззащитности, поскольку вся информация о работе, месте проживания, прививках и состоянии здоровья, интернет-покупках, собственности или подробностях семейных отношений уже утекла в интернет. Только за последний год объем утечек чувствительной информации вырос почти втрое. Власти пытаются остановить утечки повышением штрафов. Однако эти усилия пока не отразились на объемах утекающей информации. Президент РФ Владимир Путин поручил правительству к июлю 2023 года разобраться с ситуацией.

Одновременно с ужесточением ответственности в сфере обращения с персональными данными эксперты ТПП РФ считают целесообразным разработать меры поддержки, которые стимулировали бы компании инвестировать средства в обеспечение информационной безопасности, способствовали импортозамещению технологий защиты данных и облегчали их внедрение в информационные системы российского бизнеса, в том числе малого и среднего [10].

Актуальность исследованию придает и неэффективность имеющихся в уголовном и гражданском праве норм, опосредованно оберегающих персональные данные, их недостаточный предупредительный потенциал, что подтверждается несоответствием числа выявленных преступлений показателям криминальной деаномизации личной информации о россиянах в информационных ресурсах [11].

### **Нормативные требования**

В международных актах и в законодательстве страны закреплены соответствующие нормы, которые дают гарантию, что личные данные не должны распространяться без ведома самого гражданина. Всеобщая декларация прав человека содержит в себе информацию о том, что незаконное вмешательство в личную, а также семейную жизнь гражданина, карается законом. Также о соблюдении приватности и прав личности говорится в Конвенции о защите прав человека. Общественность должна уважать сохранность личной информации и выбор человека. Она не в праве вмешиваться в жизнь гражданина. Конституция Российской Федерации также гарантирует конфиденциальность данных каждого гражданина, проживающего на территории страны.

Во многих странах действуют строгие нормативные требования, регулирующие сбор, обработку и хранение персональных данных. Эти требования включают:

- Общий регламент по защите данных (GDPR) в ЕС
- Закон о конфиденциальности потребителей Калифорнии (CCPA) в США
- Закон о защите персональных данных в Бразилии.

Эти нормативные акты устанавливают стандарты для получения согласия, прозрачности, безопасности и прав субъектов данных.

В Российской Федерации также существуют определенные правила и нормы, которые регулируют конфиденциальность персональных данных. Одним из таких законов является Федеральный закон №152-ФЗ "О персональных данных". Нарушение этих норм может повлечь за собой наложение штрафов, административную ответственность, а в некоторых случаях даже возбуждение уголовного дела. Кроме того, нарушение процедур обработки персональных данных может привести к потере деловой репутации и утечке клиентов. В связи с этим, соблюдение требований, установленных Федеральным законом № 152-ФЗ и другими нормами, регулирующими область персональных данных, является важным аспектом для любой компании, которая работает с персональными данными, независимо от того, являются ли они непосредственными операторами персональных данных или осуществляют обработку данных от имени оператора.



Рис. 1. Категории персональных данных

Постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» установлены определенные требования к обеспечению безопасности персональных данных при их обработке в информационных системах.

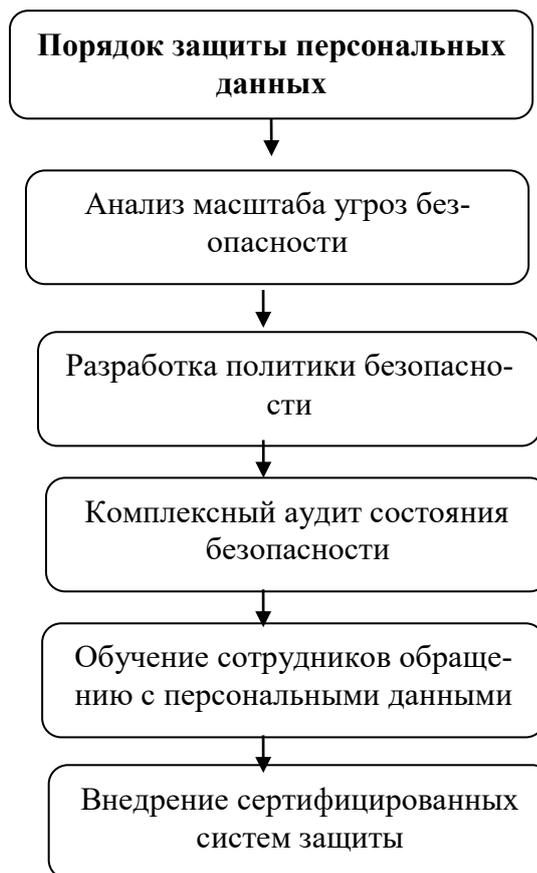


Рис. 2. Порядок защиты персональных данных

### Преимущества защиты персональных данных

Защита персональных данных в индустрии гостеприимства приносит многочисленные преимущества, в том числе:

- **Повышение доверия клиентов:** Гости могут быть уверены, что их личная информация защищена, что повышает их доверие к гостинице.
- **Соблюдение нормативных требований:** Соответствие нормативным требованиям по защите данных снижает риск штрафов и судебных разбирательств.
- **Улучшение репутации:** Гостиницы с хорошей репутацией в области защиты данных привлекают больше клиентов и сохраняют лояльность существующих клиентов.
- **Повышение эффективности:** Эффективная система защиты данных может улучшить операционную эффективность и сократить расходы.
- **Инновации:** Защита данных является основой для инноваций в индустрии гостеприимства, таких как персонализированные услуги и автоматизация.

### Практические шаги

Рестораны и отели могут предпринять следующие практические шаги для защиты персональных данных:

- **Получение согласия:** Получите явное и информированное согласие на сбор и обработку персональных данных.

- **Соблюдение принципов защиты данных:** Соблюдайте принципы защиты данных, такие как ограничение цели, минимизация данных и обеспечение безопасности.
- **Шифрование данных:** Шифруйте персональные данные во время передачи и хранения.
- **Регулярные проверки безопасности:** Проводите регулярные проверки безопасности для выявления и устранения уязвимостей.
- **Обучение персонала:** Обучайте персонал по вопросам защиты данных и процедурам.
- **Сотрудничество с поставщиками:** Сотрудничайте с поставщиками, которые соблюдают стандарты защиты данных.

### Заключение

Защита персональных данных в индустрии гостеприимства является критически важной целью устойчивого развития. Соблюдая нормативные требования и внедряя эффективные практики защиты данных, рестораны и отели могут повысить доверие клиентов, улучшить свою репутацию и обеспечить долгосрочное устойчивое развитие. Защита персональных данных должна стать неотъемлемой частью общей стратегии устойчивого развития в индустрии гостеприимства.

### Библиография

1. Егоршева Н. Чернышенко: В 2023 году по России путешествовали 78 млн россиян [Электронный ресурс]. URL: <https://rg.ru/2024/02/03/chernyshenko-v-2023-godu-po-rossii-puteshestvovali-78-mln-rossiiian.html>.
2. Заседание Совета Безопасности РФ. [Электронный ресурс]. URL: <http://www.kremlin.ru/events/president/news/68451>
3. Засемкова О.Ф. Защита персональных данных как один из компонентов ESG-повестки // Международное публичное и частное право. - 2024. - № 1. - С. 41-45.
4. Ильина Н., Перцева Е. Лично сданные в 2023-м утекли 240 млн. уникальных телефонных номеров россиян. [Электронный ресурс]. URL: <https://iz.ru/1635265/natalia-ilina-evgeniia-pertceva/lichno-sdannye-v-2023-m-utekli-240-mln-unikalnykh-telefonnykh-nomerov-rossiiian>
5. Каждая восьмая утечка информации приходится на сферу гостеприимства. [Электронный ресурс]. URL: <https://falcongaze.com/ru/pressroom/publications/articles/data-breach-in-hospitality.html>
6. Комраков А. Россия становится лидером по утечке персональных данных. [Электронный ресурс]. URL: [https://www.ng.ru/economics/2023-04-18/4\\_8709\\_russia.html](https://www.ng.ru/economics/2023-04-18/4_8709_russia.html)
7. Подпрятова А. Лучше, чем люди: могут ли цифровые «двойники» стать проблемой для общества. [Электронный ресурс]. URL: <https://www.forbes.ru/mneniya/497910-lucse-chem-ludi-mogut-li-cifrovye-dvojniki-stat-problemoj-dla-obsestva>
8. Рожков Р., Гаврилюк А. Как хакеры ведут свою войну против России. [Электронный ресурс]. URL: <https://www.forbes.ru/tekhnologii/484230-kak-hakery-vedut-svou-voynu-protiv-rossii>
9. Рузанова В.Д. Персональные данные как гражданско-правовая категория // Правовое государство: теория и практика. - 2022. - № 3. - С. 77-83.

10. ТПП РФ поддерживает разработку регуляторных мер по повышению защиты персональных данных, но с оговорками. [Электронный ресурс]. URL: [https://kapital-rus.ru/uznai/news/tpp\\_rf\\_podderjivaet\\_razrabotku\\_reguljatornh\\_mer\\_po\\_povsheniu\\_zaschit\\_personaln\\_dannh\\_no\\_s\\_ogovorkam/](https://kapital-rus.ru/uznai/news/tpp_rf_podderjivaet_razrabotku_reguljatornh_mer_po_povsheniu_zaschit_personaln_dannh_no_s_ogovorkam/)

11. Фарахиев Д. М. Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве // Юридическая наука и практика: Вестник Нижегородской академии МВД России. - 2022. - № 4. - С. 249-254.

12. Чернышенко спрогнозировал увеличение объема рынка данных в России. [Электронный ресурс]. URL: <https://ria.ru/20231122/dannye-1911062370.html>

13. Meglena Kuneva. Keynote Speech.Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009. [Электронный ресурс]. URL: [www.europa.eu/rapid/press-release\\_SPEECH-09-156\\_en.pdf](http://www.europa.eu/rapid/press-release_SPEECH-09-156_en.pdf)

14. Pitrelli M. 'For the first time in history anyone can join a war': Volunteers join Russia-Ukraine cyber fight. [Электронный ресурс]. URL: <https://www.cnbc.com/2022/03/14/volunteers-sign-up-to-help-in-cyberwars-between-russia-and-ukraine-.html>

15. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. [Электронный ресурс]. URL: <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>

Gavchuk D.V.\*

DOI: 10.25108/2304-1730-1749.iolr.2024.75.51-60

UDC: 347

### Protection of personal data in the hospitality industry as a sustainable development goal

**Abstract:** The relevance of this study is marked by the fact that the hospitality industry increasingly relies on the collection and processing of personal data of its guests. From booking rooms to ordering food and drinks, delivery services, restaurants and hotels collect and store a wealth of information about their guests. As respect for privacy becomes an increasingly important issue for consumers, it becomes critical for the hospitality industry to protect personal data and comply with data protection regulations.

**Key words:** personal data; civil law; intangible benefits; consent to the processing of personal data; transaction.

#### References

1. Egorysheva N., Chernyshenko V. In 2023, 78 million Russians traveled around Russia. Available at: <https://rg.ru/2024/02/03/chernyshenko-v-2023-godu-po-rossii-puteshestvovali-78-mln-rossiian.html> (in Russian).

---

\* Gavchuk Denis Vasilievich - Master's student at Moscow University financial and legal university "Synergy", Member of the Chamber of Commerce and Industry of the Russian Federation. E-mail: [midk@bk.ru](mailto:midk@bk.ru)

2. Meeting of the Security Council of the Russian Federation. Available at: <http://www.kremlin.ru/events/president/news/68451> (in Russian).
3. Zasekova O.F. Personal data protection as one of the components of the ESG agenda // *Mezhdunarodnoe publichnoe i chastnoe pravo - International public and private law*. 2024. No. 1, pp. 41-45 (in Russian).
4. Il'ina N., Pertseva E. 240 million unique telephone numbers of Russians, personally handed over in 2023, were leaked. Available at: <https://iz.ru/1635265/natalia-ilina-evgeniia-pertseva/lichno-sdannye-v-2023-m-utekli-240-mln-unikalnykh-telefonnykh-nomerov-rossiian> (in Russian).
5. Every eighth information leak occurs in the hospitality industry. Available at: <https://falcongaze.com/ru/pressroom/publications/articles/data-breach-in-hospitality.html> (in Russian).
6. Komrakov A. Russia becomes the leader in personal data leakage. Available at: [https://www.ng.ru/economics/2023-04-18/4\\_8709\\_russia.html](https://www.ng.ru/economics/2023-04-18/4_8709_russia.html) (in Russian).
7. Podpryatova A. Better than people: can digital “twins” become a problem for society. Available at: <https://www.forbes.ru/mneniya/497910-lucse-cem-ludi-mogut-li-cifrovye-dvojniki-stat-problemoj-dla-obsestva> (in Russian).
8. Rozhkov R., Gavriyuk A. How hackers are wagging their war against Russia. Available at: <https://www.forbes.ru/tekhnologii/484230-kak-hakery-vedut-svou-voynu-protiv-rossii> (in Russian).
9. Ruzanova V.D. Personal data like a civil legal category // *Pravovoe gosudarstvo: teoria i praktika – Legal state: theory and practice*. 2022. No. 3, pp. 77-83 (in Russian).
10. The RF CCI supports the development of regulatory measures to improve the protection of personal data, but with reservations. Available at: [https://kapital-rus.ru/uznai/news/tpp\\_rf\\_podderjivaet\\_razrabotku\\_reguliatornh\\_mer\\_po\\_povsheniu\\_zaschit\\_person\\_alnh\\_dannh\\_no\\_s\\_ogovorkam/](https://kapital-rus.ru/uznai/news/tpp_rf_podderjivaet_razrabotku_reguliatornh_mer_po_povsheniu_zaschit_person_alnh_dannh_no_s_ogovorkam/) (in Russian).
11. Farakhiev D. M. Ways and methods of de-anonymization of persons committing crimes in the information space // *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii - Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 2022. No. 4, pp. 249-254 (in Russian).
12. Chernyshenko predicted an increase in the volume of the data market in Russia. Available at: <https://ria.ru/20231122/dannye-1911062370.html> (in Russian).
13. Meglena Kuneva. Keynote Speech.Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009. Available at: [www.europa.eu/rapid/press-release\\_SPEECH-09-156\\_en.pdf](http://www.europa.eu/rapid/press-release_SPEECH-09-156_en.pdf)
14. Pitrelli M. ‘For the first time in history anyone can join a war’: Volunteers join Russia-Ukraine cyber fight. Available at: <https://www.cnbc.com/2022/03/14/volunteers-sign-up-to-help-in-cyberwars-between-russia-and-ukraine-.html>
15. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. Available at: <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>