

DOI: 10.17803/1994-1471.2026.189.8.094-101

Д. А. Кудашкин\*

## Новые правовые риски операторов персональных данных

**Аннотация.** В статье анализируются изменения в Федеральном законе «О персональных данных», вступившие в силу в 2025 г. Отмечается, что реформа носит системный характер и направлена на кардинальное ужесточение требований к операторам персональных данных. Ключевыми новациями являются введение дифференцированных административных штрафов за утечки данных, размер которых зависит от количества пострадавших субъектов, и ужесточение уголовной ответственности. Подробно рассматриваются новые правила получения действительного согласия на обработку данных, которые с 1 сентября 2025 г. должны быть оформлены в виде отдельного документа. Затрагиваются также вопросы регулирования обезличивания данных и запрета трансграничной передачи до первичного размещения в России. Делается вывод о значительном повышении правовых и финансовых рисков для операторов, что требует от них принятия незамедлительных комплексных организационно-технических мер для приведения деятельности в соответствие с обновленным законодательством.

**Ключевые слова:** право; Роскомнадзор; безопасность; информация; персональные данные; обработка персональных данных; оператор; правовые риски; административная ответственность; утечка данных

**Для цитирования:** Кудашкин Д. А. Новые правовые риски операторов персональных данных // Актуальные проблемы российского права. — 2026. — Т. 21. — № 8. — С. 94–101. — DOI: 10.17803/1994-1471.2026.189.8.094-101

### New Legal Risks for Personal Data Operators

**Dmitriy A. Kudashkin**, Postgraduate Student, Central Russian Institute of Management,  
Branch of the Russian Presidential Academy of National Economy and Public Administration,  
Orel, Russian Federation  
dima\_kudashkin@vk.com

**Abstract.** The paper analyses amendments to the Federal Law «On Personal Data» that entered into force in 2025. It notes that the reform is systemic in nature and is aimed at substantially tightening the requirements imposed on personal data operators. The principal innovations include the introduction of differentiated administrative fines for data breaches, the amount of which depends on the number of affected data subjects, as well as stricter criminal liability. The paper examines in detail the new requirements for obtaining valid consent to personal data processing: from 1 September 2025, such consent must be executed as a separate document. It also addresses the regulation of data anonymization and the prohibition on cross-border data transfers prior to the initial storage of data in Russia. The article concludes that the amendments significantly increase legal and financial risks for personal

© Кудашкин Д. А., 2026

\* Кудашкин Дмитрий Александрович, аспирант Среднерусского института управления — филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации  
Октябрьская ул., д. 12, г. Орел, Российская Федерация, 302028  
dima\_kudashkin@vk.com

data operators, requiring them to adopt without delay comprehensive organizational and technical measures to bring their activities into compliance with the updated legislation.

**Keywords:** law; Roskomnadzor; security; information; personal data; personal data processing; operator; legal risks; administrative liability; data breach

**Cite as:** Kudashkin DA. New Legal Risks for Personal Data Operators. *Aktual'nye problemy rossijskogo prava*. 2026;21(8):94-101. (In Russ.). DOI: 10.17803/1994-1471.2026.189.8.094-101

**Ф**едеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»<sup>1</sup> на протяжении почти двух десятилетий является основным правовым актом, регулирующим обращение информации о физических лицах. Динамичное развитие цифровых технологий, увеличение объемов данных и частота случаев их незаконного использования обуславливают постоянную эволюцию законодательства в этой сфере. 2025 год стал знаковым в этом процессе: в Закон о персональных данных внесен ряд фундаментальных изменений, которые кардинально ужесточают требования к операторам и значительно повышают уровень их ответственности.

Как справедливо отмечал в своих работах В. Ф. Бадюков, еще в 2020 г. эмпирические исследования констатировали высокую степень общественной опасности, сопряженную с перспективой увеличения числа утечек персональных данных. Ученый подчеркивал, что недостаточная развитость нормативно-правового регулирования в этой сфере являлась ключевым фактором, предопределившим низкий интерес со стороны российских коммерческих организаций<sup>2</sup>.

Актуальность проблем обеспечения конфиденциальности и безопасности персональных данных острее всего просматривается в финансовом секторе, что обусловлено концентрацией в нем значительных массивов чувствительной информации. В последний период наблюдается устойчивая тенденция к росту числа инцидентов, связанных с компрометацией таких данных, что наглядно демонстрируют масштабные

утечки в ряде системообразующих кредитно-финансовых организаций (Сбербанк, Альфа-Банк, Совкомбанк). Указанный тренд свидетельствует о наличии системных вызовов в области защиты информационных ресурсов<sup>3</sup>.

*Системная уязвимость информационных инфраструктур.* Наблюдается устойчивая тенденция к увеличению масштабов кибератак, следствием которых являются масштабные утечки персональных данных. Эти инциденты свидетельствуют о структурной дефектности существующих систем хранения и обработки информации, что ставит под сомнение работоспособность действующих моделей безопасности и деликтного права.

*Кризис трансграничной прозрачности и необходимость ребалансировки правомочий.* В настоящее время существует значительный дисбаланс в отношениях «субъект персональных данных — оператор». Пользователи зачастую лишены действенного инструментария для реализации своего права на контроль над информацией, предусмотренного, в частности, статьей 14 Закона о персональных данных. В этой связи актуализируется задача по выработке правовых механизмов, обеспечивающих, с одной стороны, предоставление субъекту интуитивно понятных и эффективных средств управления согласием, а с другой — установление для бизнеса четких и пропорциональных процедур информирования, минимизирующих избыточные административные обременения.

*Формирование этико-правового регулятора для технологий искусственного интеллекта.* Интенсивное внедрение алгоритмов машин-

---

<sup>1</sup> СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

<sup>2</sup> Бадюков В. Ф., Докучаев М. Н. Риски цифровой экономики: особенности и перспективы развития киберстрахования в России // Страховое право. 2021. № 1 (90). С. 42–44.

<sup>3</sup> Швыряев П. С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. С. 226–241.

ного обучения порождает новую плоскость юридической ответственности. Вопрос о распределении бремени ответственности между разработчиками и операторами систем искусственного интеллекта за противоправную или этически недопустимую обработку данных требует незамедлительной доктринальной проработки и последующей легализации. В качестве перспективной модели может рассматриваться презумпция виновности владельца алгоритма, если не доказано иное<sup>4</sup>.

Таким образом, развитие законодательства о персональных данных является прямым ответом на современные угрозы безопасности. Вводимые правовые нормы создают значительно обновленные правовые рамки для всех организаций, работающих с персональными данными. Единые требования применяются как к крупным корпорациям, так и к малому бизнесу, а их нарушение влечет за собой серьезные правовые последствия и значительные штрафные санкции. Однако эти изменения порождают определенные риски для операторов персональных данных.

Так, в 2025 г. проведена масштабная законодательная реформа регулирования в области персональных данных, которая затронула как материальные, так и процессуальные нормы Закона. Изменения носят не точечный, а системный характер, направлены на усиление контроля за оборотом данных и максимизацию их обработки на территории Российской Федерации.

Наиболее существенным изменением, вступившим в силу 30 мая 2025 г., стало радикальное увеличение размеров административных штрафов за нарушения при обработке персональных данных, а также введение новых составов административных правонарушений.

Центральный элемент новой системы наказаний — введение градуированных штрафов за утечку персональных данных, размер которых теперь напрямую зависит от масштаба инцидента.

Утечка данных 1 тыс. — 10 тыс. субъектов или 10 тыс. — 100 тыс. идентификаторов:

- 1) граждане: 100 тыс. — 200 тыс. руб.;
- 2) должностные лица: 200 тыс. — 400 тыс. руб.;
- 3) юридические лица: 3 млн — 5 млн руб.

Утечка данных 10 тыс. — 100 тыс. субъектов или 100 тыс. — 1 млн идентификаторов:

- 1) граждане: 200 тыс. — 300 тыс. руб.;
- 2) должностные лица: 300 тыс. — 500 тыс. руб.;
- 3) юридические лица: 5 млн — 10 млн руб.

Утечка данных свыше 100 тыс. субъектов или свыше 1 млн идентификаторов:

- 1) граждане: 300 тыс. — 400 тыс. руб.;
- 2) должностные лица: 400 тыс. — 600 тыс. руб.;
- 3) юридические лица: 10 млн — 15 млн руб.

Отдельно и в еще более крупных размерах установлена ответственность за утечку данных специальных категорий (о здоровье, политических взглядах и т.д.) и биометрических данных. Штраф за утечку биометрии для юридических лиц может достигать 15 млн — 20 млн руб., а для граждан 400 тыс. — 500 тыс. руб.

Были ужесточены также санкции за неупоминание Роскомнадзора о начале обработки персональных данных и, что особенно важно, о самом факте утечки. За несообщение об утечке оператору грозит штраф от 1 млн до 3 млн руб., что в 10 раз превышает предыдущие санкции<sup>5</sup>.

Норма ч. 1 ст. 22 Закона о персональных данных устанавливает императивную обязанность оператора уведомить уполномоченный орган (Роскомнадзор) о начале осуществления обработки персональных данных. Однако в соответствии с ч. 2 той же статьи указанная обязанность не распространяется на случаи, когда обработка осуществляется исключительно без использования средств автоматизации.

Возникает сложность однозначного отнесения конкретного процесса обработки к автоматизированному или неавтоматизированному.

<sup>4</sup> Чернышов К. Д. Актуальные подходы к обработке персональных данных: анализ и развитие законодательства // Вестник науки. 2025. Т. 2. № 1 (82). С. 431–435.

<sup>5</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступившими в силу с 6 сентября 2025 г.) // СЗ РФ. 2002. № 1 (ч. I). Ст. 1.

Основная проблема — отсутствие в законодательстве детализированного и исчерпывающего определения как средств автоматизации, так и критериев, позволяющих квалифицировать обработку как осуществляемую *исключительно* без таковых.

Отмеченный терминологический дефицит приводит к правовой неопределенности: оператор вынужден самостоятельно интерпретировать границы применимости исключения, что сопряжено с высоким риском ошибочной оценки. Неверная квалификация, в свою очередь, влечет за собой неприменение уведомительного порядка в случаях, когда он является обязательным, что образует состав административного правонарушения, предусмотренного статьей 13.11 КоАП РФ.

Таким образом, сохраняющаяся законодательная неточность в определении важнейших понятий создает устойчивую зону регуляторного риска, требуя от оператора повышенной осмотрительности и способствуя необходимости обращения к доктринальному толкованию и сложившейся правоприменительной практике Роскомнадзора для минимизации потенциальной ответственности<sup>6</sup>.

Поправки затронули и уголовное законодательство. Были ужесточены санкции по ст. 137 УК РФ<sup>7</sup> «Нарушение неприкосновенности частной жизни», а также внесена поправка в ч. 1 этой статьи, а именно — она была дополнена: «за исключением случаев, предусмотренных статьей 272.1 настоящего Кодекса».

До недавнего времени в Уголовном кодексе отсутствовала отдельная норма, непосредственно криминализирующая неправомерные действия с компьютерными данными, содержащими персональную информацию. В связи с этим правоприменительная практика вынуж-

дена была использовать совокупность статей о нарушении неприкосновенности частной жизни (ст. 137 УК РФ) и о компьютерных преступлениях, что зачастую осложняло точную юридическую квалификацию противоправных деяний. Введенная 11 декабря 2024 г. статья 272.1 УК РФ направлена на устранение этого правового пробела. Теперь за незаконное распространение персональных данных в преступных целях грозит лишение свободы на срок до четырех лет, а если преступление совершено в отношении несовершеннолетнего — до пяти лет<sup>8</sup>. Если же действия привели к тяжким последствиям или совершены организованной группой, максимальное наказание достигает 10 лет лишения свободы со штрафом до 3 млн руб.

По нашему мнению, все эти изменения были необходимы для создания механизма дополнительной защиты от утечки и неправомерного использования личной информации в цифровой среде. Этот довод подтверждается также словами других представителей экспертного сообщества, что позволяет констатировать: ключевым фактором для реформирования законодательства в сфере защиты персональных данных послужила прогрессирующая криминализация информационного пространства, выражающаяся в значительном увеличении количества киберпреступлений. Предыдущая редакция КоАП РФ в части, касающейся ответственности операторов, характеризовалась недостаточной степенью их ответственности. Штрафные санкции не выполняли в полной мере превентивной функции, а отклонение установленных размеров санкций от потенциального объема ущерба, наносимого субъектам персональных данных в результате инцидентов безопасности, сводило на нет сдерживающий эффект от их применения<sup>9</sup>.

---

<sup>6</sup> Булочников С. Ю. О правотворчестве и правовых новациях в части защиты от утечек персональных данных // Новизна. Эксперимент. Традиции. 2025. № 1. С. 6–15.

<sup>7</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 1 сентября 2025 г.) // СЗ РФ. 1996. № 25. Ст. 2954.

<sup>8</sup> Петрова К. А. Защита конфиденциальности данных и прав личности в цифровой среде: правовое регулирование и практические механизмы // Научные записки молодых исследователей. 2025. № 2. С. 46–53.

<sup>9</sup> Шичанин М. Штрафы за утечку персональных данных повысят до 15 млн руб.: к чему еще готовиться бизнесу? // URL: <https://www.garant.ru/article/1746375/> (дата обращения: 06.10.2025).

Еще одно из нововведений с 1 сентября 2025 г. — принципиально новые правила получения согласия на обработку персональных данных. В соответствии с изменениями в ст. 9 Закона о персональных данных согласие должно быть оформлено в виде отдельного документа и не может быть включено в текст договора, пользовательского соглашения или политики конфиденциальности. Это требование направлено на обеспечение осознанного и добровольного волеизъявления субъекта, исключая ситуации, когда согласие «спрятано» в основном документе и дается пользователем автоматически.

Содержание нового согласия стало более детализированным и должно включать развернутый перечень сведений: полные данные оператора и субъекта персональных данных (в том числе паспортные данные субъекта и юридический адрес оператора); конкретные цели обработки; исчерпывающий перечень обрабатываемых данных и действий с ними (таких как сбор, хранение, уточнение, использование, передача); сведения о третьих лицах, которым могут быть переданы данные; срок действия согласия и четкий порядок его отзыва. Важно отметить, что для передачи данных третьим лицам необходимо получать отдельное согласие, в котором будут указаны наименования этих лиц и цели передачи<sup>10</sup>.

Рассматриваемая поправка в первую очередь нацелена на устранение правовой неопределенности и защиту граждан от недобросовестных операторов, которые на практике часто включали условия о согласии в объемные тексты договоров, что приводило к путанице и неосознанному предоставлению согласия на обработку данных. Отдельное оформление согласия позволит более четко определить усло-

вия и цели обработки, а также повысит уровень информированности граждан о том, каким образом и с какой целью будут использоваться их персональные данные.

Мнения экспертов и практиков сводятся к тому, что для соблюдения новых требований бизнесу и организациям необходимо предпринять ряд шагов. Рекомендуется провести внутренний аудит всех процессов, связанных с обработкой персональных данных; проверить все договоры, пользовательские соглашения и другие документы на наличие «скрытых» согласий; разработать и внедрить отдельные формы согласия для каждого вида обработки; подать уведомление в Роскомнадзор (если это не было сделано ранее), а также обучить сотрудников, работающих с персональными данными, новым правилам<sup>11</sup>.

Еще одним важным изменением является усиление регуляторного контроля за обезличенными данными. С 1 сентября 2025 г. операторы обязаны по запросу Минцифры России передавать в государственные информационные системы обезличенные массивы персональных данных. При этом установлен запрет на передачу результатов обработки таких данных некоторым категориям иностранных лиц.

Введение в действие постановления Правительства РФ от 01.08.2025 № 1154<sup>12</sup>, призванного унифицировать процедуру обезличивания персональных данных, актуализировало вопрос о методологической достаточности применяемых технических средств. Как показывает сравнительно-правовой анализ, перечень методов, предложенных в новом нормативном акте, практически полностью репродуцирует подходы, изложенные в утратившем актуальность приказе Роскомнадзора от 05.09.2013 № 996.

<sup>10</sup> Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (с изм. и доп.) // СЗ РФ. 2008. № 38. Ст. 4320.

<sup>11</sup> Согласие на обработку персональных данных с 1 сентября 2025 года: новые правила оформления и штрафы до 700 тыс. руб. за их нарушение // URL: <https://www.garant.ru/article/1862510/> (дата обращения: 06.10.2025).

<sup>12</sup> Постановление Правительства РФ от 01.08.2025 № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных» // СЗ РФ. 2025. № 32. Ст. 4929.

Основное различие состоит в целях и правовых последствиях использования этих методов. Постановление № 1154 было разработано для конкретной цели — регулирования процесса передачи обезличенных данных в государственную информационную систему ЕИП НСУД (Единая информационная платформа национальной системы управления данными) по требованию Минцифры России. В отличие от приказа № 996, который носил более общий характер, новое Постановление устанавливает обязательные для исполнения требования, согласованные с ФСБ России.

Это различие в цели порождает и главное технологическое различие — требование необратимости обезличивания. При использовании методов Постановления № 1154 для передачи данных в государственную систему должна быть гарантирована невозможность преобразования обезличенных данных обратно в исходный вид, позволяющий идентифицировать субъекта. В то время как для внутренних нужд оператора, регулируемых в том числе новым приказом Роскомнадзора, сохраняется возможность деанонимизации (деобезличивания) с помощью специальных ключей или справочников.

Таким образом, фокус сместился с технологического обновления на формализацию и детализацию самого процесса обезличивания. Установлены строгие требования к выбору метода, его документированию, организации хранения обезличенных массивов информации и устранению угроз повторной идентификации. Безусловно, это способствует повышению системности и ответственности при обработке данных.

Тем не менее проблемой, остающейся без разрешения, является соответствие методик современному уровню развития информационных технологий. В силу рисков, порождаемых сложными алгоритмами анализа связанных данных и повышения вычислительных мощностей, необходимо применение более прогрессивных и устойчивых к реидентификации методов. Следовательно, несмотря на прогресс в области процессуального регулирования, вопрос об эффективности и адекватности самих методов обезличивания в современных условиях оста-

ется открытым и нуждается в дальнейшей научной проработке.

Указанные законодательные изменения формируют новый, более высокий уровень правовых рисков для операторов. Эти риски носят комплексный характер и требуют незамедлительного принятия превентивных мер.

Ключевой риск, возникающий после 1 сентября 2025 г., — недействительность полученных согласий. Если согласие интегрировано в договор или политику конфиденциальности, оно не будет соответствовать нормам закона, что означает фактическое отсутствие правового основания для обработки данных. Это влечет за собой административную ответственность по ч. 2 ст. 13.11 КоАП РФ (штраф для юридических лиц до 700 тыс. руб.) и делает всю обработку данных незаконной.

Пути минимизации:

1. Разработка отдельной формы согласия, соответствующей всем новым требованиям ст. 9 Закона о персональных данных.

2. Пересмотр всех существующих процессов сбора данных (на сайте, в мобильном приложении, в офлайн-точках) для обеспечения получения нового согласия.

3. Ведение реестра согласий с фиксацией даты, способа получения и версии формы.

С 1 июля 2025 г. вступили в силу поправки, ужесточающие правила трансграничной передачи. Запрещена передача персональных данных на зарубежные сервисы до их первичного размещения в России. На практике это означает, что использование популярных иностранных инструментов, таких как Google Analytics, Google Forms, reCAPTCHA, виджеты WhatsApp и Telegram, а также ряда SaaS-сервисов, которые передают данные напрямую за рубеж, может быть признано нарушением.

Пути минимизации:

1. Аудит сайта и ИТ-инфраструктуры на предмет наличия запрещенных интеграций и внешних подключений.

2. Замена иностранных сервисов на отечественные аналоги (например, «Яндекс.Метрика» вместо Google Analytics).

3. Настройка прокси-серверов или иных механизмов, обеспечивающих первичное сохра-

нение данных на российских серверах перед их возможной передачей за границу (если такая передача правомерна).

Новая градация штрафов за утечки делает как никогда важным инвестирование в системы защиты данных. Риск многомиллионных штрафов становится материальным даже для среднего бизнеса. Кроме того, крайне опасным является риск несвоевременного уведомления Роскомнадзора об утечке.

Пути минимизации:

1. Внедрение современных средств защиты информации, в частности шифрования, систем обнаружения вторжений и DLP-систем.

2. Разработка и внедрение регламента действий при инцидентах, включающего четкий порядок уведомления Роскомнадзора в установленные сроки.

3. Регулярный инструктаж сотрудников, работающих с персональными данными, о новых размерах ответственности и правилах безопасности.

Проведенный анализ позволяет сделать вывод о том, что законодательные изменения 2025 г. в Законе о персональных данных существенно трансформируют правовое поле для всех операторов. Основной тенденцией является резкое увеличение стоимости нарушений,

будь то несоблюдение процедурных требований (оформление согласия, уведомление регулятора) или непринятие адекватных мер безопасности, приведшее к утечке.

Новые правовые риски носят комплексный финансовый, регуляторный и репутационный характер. В этих условиях пассивная или формальная позиция оператора становится невозможной. Для соблюдения обновленного законодательства необходимы активные и целенаправленные действия: проведение внутреннего аудита процессов обработки данных, пересмотр всей документации, модернизация ИТ-инфраструктуры и внедрение эффективных систем защиты.

Таким образом, для минимизации новых правовых рисков операторам следует незамедлительно приступить к реализации комплекса организационно-технических мер, ориентированных на полное приведение своей деятельности в соответствие с актуализированными требованиями Закона. Развитие законодательства в этой сфере, вероятно, будет продолжено в направлении усиления контроля и ответственности, что делает задачу построения устойчивой и законной системы работы с персональными данными одной из ключевых для любого субъекта экономической деятельности.

## БИБЛИОГРАФИЯ

1. Бадюков В. Ф., Докучаев М. Н. Риски цифровой экономики: особенности и перспективы развития киберстрахования в России // *Страховое право*. — 2021. — № 1 (90). — С. 42–44.
2. Булочников С. Ю. О правотворчестве и правовых новациях в части защиты от утечек персональных данных // *Новизна. Эксперимент. Традиции*. — 2025. — № 1. — С. 6–15.
3. Петрова К. А. Защита конфиденциальности данных и прав личности в цифровой среде: правовое регулирование и практические механизмы // *Научные записки молодых исследователей*. — 2025. — № 2. — С. 46–53.
4. Согласие на обработку персональных данных с 1 сентября 2025 года: новые правила оформления и штрафы до 700 тыс. руб. за их нарушение // URL: <https://www.garant.ru/article/1862510/>.
5. Чернышов К. Д. Актуальные подходы к обработке персональных данных: анализ и развитие законодательства // *Вестник науки*. — 2025. — Т. 2. — № 1 (82). — С. 431–435.
6. Швыряев П. С. Утечки конфиденциальных данных: главный враг внутри // *Государственное управление. Электронный вестник*. — 2022. — № 91. — С. 226–241.
7. Шичанин М. Штрафы за утечку персональных данных повысят до 15 млн руб.: к чему еще готовиться бизнесу? // URL: <https://www.garant.ru/article/1746375/>.

*Материал поступил в редакцию 8 октября 2025 г.*

#### REFERENCES (TRANSLITERATION)

1. Badyukov V. F., Dokuchaev M. N. Riski tsifrovoy ekonomiki: osobennosti i perspektivy razvitiya kiberstrakhovaniya v Rossii // Strakhovoe pravo. — 2021. — № 1 (90). — S. 42–44.
2. Bulochnikov S. Yu. O pravotvorchestve i pravovykh novatsiyakh v chasti zashchity ot utechk personalnykh dannykh // Novizna. Eksperiment. Traditsii. — 2025. — № 1. — S. 6–15.
3. Petrova K. A. Zashchita konfidentsialnosti dannykh i prav lichnosti v tsifrovoy srede: pravovoe regulirovanie i prakticheskie mekhanizmy // Nauchnye zapiski molodykh issledovateley. — 2025. — № 2. — S. 46–53.
4. Soglasie na obrabotku personalnykh dannykh s 1 sentyabrya 2025 goda: novye pravila оформleniya i shtrafy do 700 tys. rub. za ikh narushenie // URL: <https://www.garant.ru/article/1862510/>.
5. Chernyshov K. D. Aktualnye podkhody k obrabotke personalnykh dannykh: analiz i razvitie zakonodatelstva // Vestnik nauki. — 2025. — T. 2. — № 1 (82). — S. 431–435.
6. Shvyryaev P. S. Utechki konfidentsialnykh dannykh: glavnyy vrag vnutri // Gosudarstvennoe upravlenie. Elektronnyy vestnik. — 2022. — № 91. — S. 226–241.
7. Shichanin M. Shtrafy za utechku personalnykh dannykh povysyat do 15 mln rub.: k chemu eshche gotovitsya biznesu? // URL: <https://www.garant.ru/article/1746375/>.