

Ревизия соблюдения законодательства о защите персональных данных: методика и последствия нарушений для репутации и бизнеса*

Audit Of Compliance With Legislation On The Protection Of Personal Data: Methodology And Consequences Of Violations For Reputation And Business

С. ДАВЛЕТШИНА, О. ЮЛДАШЕВ

Давлетшина Светлана Маратовна, канд. эконом. наук, доцент кафедры экономики предпринимательства Института экономики, управления и бизнеса (ИНЭБ) ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ). E-mail: garildar@mail.ru

Юлдашев Одилджон Олимджонович, студент кафедры экономики предпринимательства ИНЭБ УУНиТ. E-mail: yuldashev585@mail.ru

Аннотация. В статье рассматриваются теоретические и прикладные аспекты проведения ревизии соответствия законодательству о персональных данных на примере требований Федерального закона № 152-ФЗ и Регламента GDPR. Проведен анализ правовых и репутационных последствий нарушений с учетом изменений законодательства в 2023–2025 гг., в том числе введения оборотных штрафов и уголовной ответственности. На основе анализа судебной практики обосновывается вывод о необходимости интеграции регулярного комплаенса в систему управления рисками для предотвращения финансовых потерь и сохранения деловой репутации.

Ключевые слова: персональные данные, 152-ФЗ, GDPR, ревизия, экономическая безопасность, оборотные штрафы, репутационный ущерб, утечка данных, локализация данных, комплаенс, административная ответственность.

Abstract. This article examines the theoretical and practical aspects of conducting compliance audits with personal data legislation, using the requirements of Federal Law No. 152-FZ and the GDPR as examples. The legal and reputational consequences of violations are analyzed, taking into account legislative changes for 2023–2025, including the introduction of turnover-based fines and criminal liability. Based on an analysis of judicial practice, the conclusion is made regarding the need to integrate regular compliance into the risk management system to prevent financial losses and preserve business reputation.

Key words: personal data, Federal Law 152, GDPR, audit, economic security, turnover fines, reputational damage, data leakage, data localization, compliance, administrative liability.

Основные положения

1. В 2025 г. вступили в силу изменения в законодательстве о персональных данных (ПД), что требует перехода от разовых проверок к непрерывному комплаенсу.
2. Предлагаемая методика ревизии включает в себя четыре этапа: инвентаризация данных, юридический аудит, технический аудит защищенности и тестирование процессов реагирования.
3. Нарушение требований 152-ФЗ и GDPR влечет комплексные последствия: от оборотных штрафов (до 15 млн руб. и более) и уголовной ответственности для топ-менеджмента до потери клиентов и капитализации бизнеса.

Введение

В 2025 году вступили в силу нормы об обороте штрафов, кратно увеличилась сумма административной ответственности, а в Уголовном кодексе появилась статья 272.1, криминали-

* Ссылка на статью: Давлетшина С.М., Юлдашев О.О. Ревизия соблюдения законодательства о защите персональных данных: методика и последствия нарушений для репутации и бизнеса // Экономика и управление: научно-практический журнал. 2026. № 5. С. 116–121. DOI 10.34773/EU.2026.5.19.

зующая незаконный оборот ПД. Одновременно с этим Общий регламент по защите данных (GDPR) продолжает задавать стандарты для компаний, работающих на европейском рынке, предусматривая штрафы до 4 % от глобального оборота [7].

В этих условиях ревизия (аудит) соответствия перестает быть разовой формальностью и превращается в непрерывный бизнес-процесс. Ошибки в обработке данных, избыточное хранение информации или отсутствие актуальных согласий могут привести не только к многомиллионным штрафам, но и к полной утрате доверия контрагентов.

В современных условиях ПД выступают не только объектом правовой защиты, но и значимым экономическим активом организации. Чем выше уровень цифровизации бизнес-процессов, тем сильнее зависимость компании от качества сбора, хранения, передачи и уничтожения данных. Вследствие этого нарушения в сфере ПД становятся не частной юридической проблемой, а фактором стратегического риска, влияющим на стоимость бренда, устойчивость клиентских отношений и инвестиционную привлекательность компании.

Следует учитывать, что рост числа цифровых сервисов, платформ дистанционного обслуживания, маркетплейсов и облачных решений приводит к постоянному расширению периметра обработки ПД. При этом увеличение массивов данных не всегда сопровождается соответствующим развитием внутренних регламентов и средств защиты. Именно поэтому ревизия соблюдения законодательства должна быть ориентирована не только на формальное наличие документов, но и на проверку реального соответствия организационных и технических процессов установленным требованиям.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» к началу 2026 г. претерпел существенные изменения, связанные с усилением ответственности [4]:

– **оборотные штрафы.** Суммы взысканий теперь зависят от масштаба инцидента и могут достигать сотен миллионов рублей, что соизмеримо с годовыми бюджетами среднего бизнеса на информационную безопасность;

– **уголовная ответственность.** Статья 272.1 УК РФ введена за создание, использование и распространение вредоносных программ, а также за незаконный оборот ПД, полученных преступным путем. Максимальное наказание составляет до 10 лет лишения свободы.

– **локализация данных.** Требования об использовании баз данных, находящихся на территории РФ, сохраняются, а штрафы за их нарушение составляют до 18 млн рублей.

Методы

Рассмотрим следующую методику, базирующуюся на лучших практиках 2025-2026 гг. и включающую четыре ключевых этапа, которые должны проводиться с периодичностью не реже одного раза в год [2].

Этап 1: Инвентаризация и картирование данных (Data Discovery)

Первоначальным и методологически ключевым этапом аудита является комплексное обследование технической инфраструктуры организации с целью установления полного перечня мест хранения ПД. В отличие от документарного подхода, данный этап предполагает системное исследование информационной среды: идентификацию CRM-систем, платформ управления кадровым учётом, облачных сервисов (Google Workspace, МойОфис), сетевых файловых хранилищ, а также массивов документации на бумажных носителях. Все выявленные данные подлежат классификации по типологическому признаку (общие, специальные категории, биометрические) и по категориям субъектов (клиенты, сотрудники, посетители сайта). Эмпирический опыт проведения подобных аудитов свидетельствует о том, что именно на данном этапе выявляются так называемые «серые зоны» – неучтённые и нерегламентированные источники хранения ПД. В качестве характерного примера можно привести электронные таблицы, содержащие паспортные данные субъектов и бесконтрольно размещённые на локальных рабочих станциях административного персонала. В целях обеспечения исчерпывающей полноты инвентаризации рекомендуется применение специализированных инструментов автоматизированного

обнаружения данных (Data Discovery Tools), позволяющих идентифицировать неструктурированные хранилища, не охватываемые стандартными системами корпоративного учёта.

Этап 2: Юридический аудит документации.

На данном этапе проводится анализ локальных нормативных актов на соответствие букве закона. Проверяется наличие документации, ее доступность (опубликована ли на сайте), полнота и соответствие реальным процессам. Следующим шагом будет проверка форм согласий: нужно убедиться, что в них соблюдены принципы сознательности, информированности и конкретности. Особое внимание уделяется наличию отдельных согласий на разные цели обработки. Также проверяется, было ли направлено в Роскомнадзор уведомление о старте работы с ПД.

Этап 3: Технический аудит и анализ защищённости

Задача данного этапа – объективная оценка состояния информационной безопасности компании. В центре внимания – разграничение прав доступа персонала по принципу минимальной необходимости (least privilege). Отдельному контролю подлежит своевременность блокировки учётных записей уволенного персонала, поскольку статистически именно избыточность привилегий доступа является доминирующей причиной внутренних инцидентов утечки данных. Параллельно исследуется применение защищённых протоколов передачи данных (TLS/SSL) – в особенности при информационном обмене с контрагентами и использовании корпоративных мессенджеров.

В рамках технического аудита также проводится оценка наличия и корректности функционирования средств защиты: систем предотвращения утечек данных (DLP), межсетевых экранов уровня баз данных (DBF), инструментов криптографической защиты и механизмов маскирования персональных данных. Самостоятельным направлением является анализ договорной базы с внешними поставщиками услуг – облачными провайдерами, бухгалтерскими сервисами и иными контрагентами – на предмет наличия соглашений о конфиденциальности и соглашений об обработке персональных данных (Data Processing Agreement, DPA). Все выявленные в ходе аудита недостатки подлежат документированию в форме структурированных отчётов с присвоением каждому нарушению индивидуального идентификатора для последующего контроля устранения.

Этап 4: Тестирование процессов реагирования (DSAR & Breach Response).

Последний этап предполагает проверку того, как организация реагирует на запросы субъектов и инциденты. Он включает тестирование процедур ответа на запросы о доступе к данным (Subject Access Request), об их удалении («право на забвение») или приостановке обработки. Регламент GDPR требует ответа в течение 30 дней. Этап включает оценку готовности уведомить РКН о факте утечки (в установленные законом сроки: 24–72 часа для критичных инцидентов) и коммуникационной стратегии для пострадавших клиентов.

Результаты

Схематично предложенную методику по защите ПД можно представить в следующем виде (рисунок).

Результаты применения предложенной методики показывают, что наибольшее число нарушений выявляется не в сфере отсутствия базовых нормативных документов, а в области расхождения между формально утверждёнными правилами и фактической практикой обработки данных. Организации нередко разрабатывают политику обработки ПД и размещают её на сайте, однако внутренние процессы доступа, архивирования, передачи информации контрагентам и удаления данных остаются недостаточно регламентированными. Это указывает на наличие разрыва между декларативным и фактическим уровнями комплаенса.

С практической точки зрения наиболее уязвимыми зонами являются избыточный сбор данных, отсутствие чёткой дифференциации целей обработки, слабый контроль действий сотрудников и несвоевременное удаление информации после достижения цели обработки. Подобные недостатки создают условия не только для привлечения к административной ответственности, но и для формирования системных репутационных потерь. Чем дольше организация сохраняет такие

нарушения, тем выше вероятность того, что единичный инцидент перерастёт в полномасштабный кризис доверия.

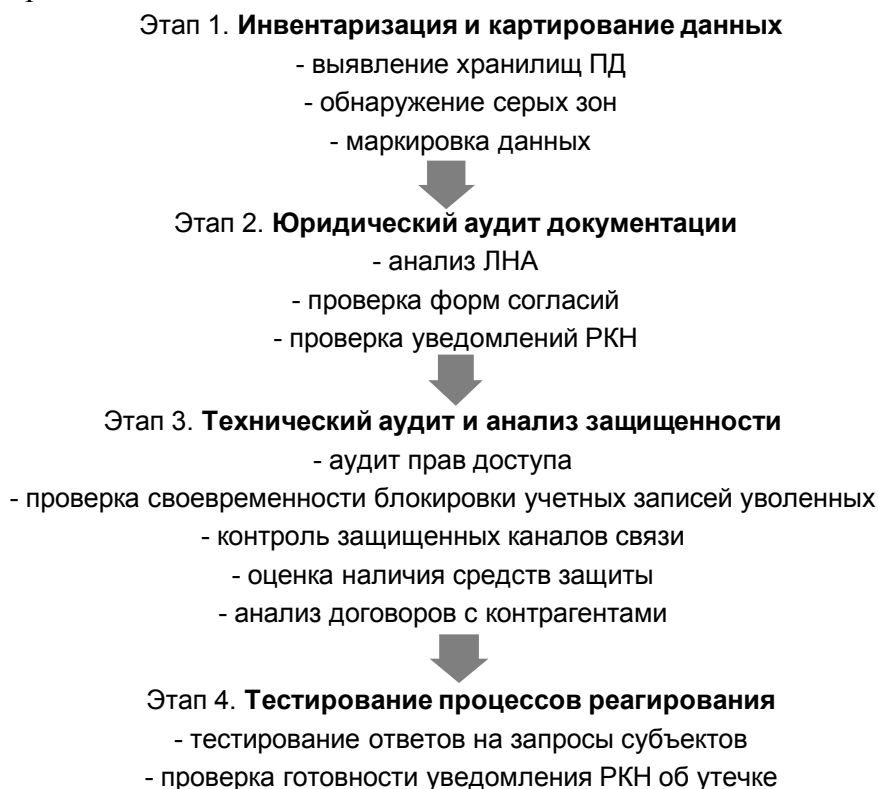


Схема предложенной методики для защиты персональных данных

Несоблюдение требований 152-ФЗ и GDPR влечет за собой комплексные последствия, которые делятся на прямые финансовые потери и косвенные репутационные издержки.

Рассмотрим прямые негативные последствия для юридических лиц при утечке ПД [5]:

1) утечка данных 1–10 тыс. человек – штраф до 5 млн руб., свыше 100 тыс. записей – до 15 млн руб. Повторные нарушения грозят оборотным штрафом (152-ФЗ);

2) до 20 млн евро или 4 % от годового мирового оборота, в зависимости от того, какая сумма больше (GDPR);

3) уголовная ответственность для IT-директоров и руководителей, чьи действия привели к созданию каналов незаконного оборота ПД (ст. 272.1 УК РФ).

Рассмотрим косвенные (репутационные) негативные последствия для юридических лиц при утечке ПД:

1) после громкой утечки клиенты массово уходят к конкурентам;

2) инвесторы и партнеры начинают сомневаться в надежности компании, что приводит к падению капитализации и удорожанию кредитов;

3) клиенты начинают ассоциировать бренд с потоком спама и мошеннических звонков, что формирует устойчивый негативный образ;

4) кибератаки, приводящие к утечкам, часто парализуют работу компании. Примером является компания «Винлаб», которая получила убытки около 250 млн рублей за день простоя после хакерской атаки в июле 2025 года ;

5) утечка коммерческой тайны или клиентских баз к конкурентам лишает компанию уникальных рыночных позиций;

6) крупные заказчики (западные или госкомпании) требуют подтверждения соблюдения GDPR/152-ФЗ. Отсутствие «чистого» аудита может стать причиной отказа в заключении контракта.

Обсуждение

Полученные результаты подтверждают гипотезу о том, что в условиях ужесточения регуляторных требований 2023–2026 гг. ревизия соответствия не может рассматриваться как разовая процедура. Выявленные «серые зоны» (например, бесконтрольное хранение таблиц с ПД на рабочих станциях) указывают на низкую культуру обращения с данными на уровне рядовых сотрудников, что не может быть устранено исключительно техническими средствами.

Реалии 2026 года диктуют необходимость перехода организаций от периодических проверок к модели непрерывного мониторинга соответствия требованиям законодательства. Внедрение SGRC-систем (платформ управления рисками и комплаенсом) обеспечивает автоматизацию сбора доказательной базы и оперативное отслеживание изменений в нормативно-правовом регулировании. Вместе с тем технические средства защиты не могут функционировать в отрыве от сформированной культуры информационной безопасности: систематическое обучение персонала способно предотвратить до 90 % потенциальных инцидентов, что подчёркивает приоритетность человеческого фактора в системе защиты персональных данных.

С научно-практической точки зрения полученные результаты свидетельствуют о качественной трансформации самой природы аудита в сфере персональных данных. Если прежде он воспринимался преимущественно как инструмент проверки формального исполнения регуляторных предписаний, то в современных условиях аудит интегрируется в систему корпоративного управления, органично встраиваясь в механизмы внутреннего контроля и риск-менеджмента. Это обуславливает необходимость переосмысления критериев его эффективности: результативность ревизии должна определяться не только количеством выявленных нарушений, но и способностью организации предупреждать повторные инциденты.

Необходимо поддерживать регулярность контрольных мероприятий, так как единовременная проверка не может служить гарантией того, что требования будут выполняться стабильно, учитывая постоянные изменения в цифровой среде, текучку кадров и законодательстве. В связи с этим методологически более обоснованной представляется модель непрерывного комплаенса, где мониторинг, обучение персонала, обновление документации и отработка инцидентов идут в одном цикле.

Заключение

Изложенное позволяет заключить, что ревизия соответствия законодательству о ПД не может быть сведена к разовой проверке – она должна быть институционализирована в качестве непрерывного бизнес-процесса. Системная интеграция регулярного мониторинга с применением SGRC-платформ, технических средств защиты информации и циклического обучения персонала представляет собой единственно состоятельный подход к минимизации комплаенс-рисков в условиях динамично меняющейся регуляторной среды.

Принципиально важно рассматривать аудит ПД не исключительно как правовой инструмент, но и как механизм экономической защиты организации, поскольку такой подход обеспечивает раннее выявление уязвимостей, снижает частоту применения регуляторных санкций, предотвращает финансовые потери из-за операционных сбоев и поддерживает репутационный капитал в отношениях с клиентами, деловыми партнёрами и инвесторами.

По проведенному анализу можно сделать вывод, что у ревизии ПД, встроенной в архитектуру управления и имеющую твердую поддержку со стороны топ-менеджмента, результат на порядок выше. В компаниях, где внедрена подобная модель, соответствие Федеральному закону № 152-ФЗ и GDPR становится естественной частью стратегии, позволяющей организации отвечать на современные цифровые и правовые угрозы.

Литература

1. Зилькарнаев Р.А., Давлетшина С.М. Риски и перспективы внедрения цифровых технологий при проведении ревизий // Экономика и менеджмент: новые вызовы и возможности:

сборник научных трудов III Международной научно-практической конференции, Ростов-на-Дону, 11 июня 2025 г. Ростов-на-Дону: ООО «ДГТУ-ПРИНТ», 2025. С. 239–242.

21. Ключевые этапы аудита персональных данных: практическое руководство [Электронный ресурс]. URL: <https://www.audit-it.ru/articles/soft/a115/1127564.html>

3. Козлов Е.В. Значение эволюции методов контроля и ревизии для укрепления экономической безопасности предприятия / Е.В. Козлов, С.М. Давлетшина // Youth Bulletin of the USA-TU. 2025. No. 2(33). DOI 10.54708/22259309_2025_23356.

4. Мансурова Ю.Т. Регрессионная модель определения уровня коррупции в Российской Федерации / Ю.Т. Мансурова, Д.И. Хамидуллина // Экономика и управление: научно-практический журнал. 2023. № 6(174). С. 141–145. DOI 10.34773/EU.2023.6.25.

5. Персональные данные: новая уязвимость в условиях цифровой экономики / РБК Компании [Электронный ресурс]. URL: <https://companies.rbc.ru/news/dj7lXAJwVh/personalnyie-dannyye-novaya-uyazvimost-v-usloviyah-tsifrovoj-ekonomiki/>

6. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/

7. Privacy-итоги 2025 [Электронный ресурс]. URL: <https://comply.ru/tpost/f3oed3k001-privacy-itogi-2025>

8. Regulation (EU) 2016/679 (General Data Protection Regulation) / European Union [Electronic resource]. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

DOI: 10.34773/EU.2026.5.20

К вопросу о внедрении технологий искусственного интеллекта для рассмотрения обращений граждан в органах Роспотребнадзора*

On the Issue of Artificial Intelligence Technologies Implementation to Consider Citizens' Appeals in the Rospotrebnadzor Organization

Л. СПИРИНА, Р. КРАСНОВА

Спирина Лиана Иршатовна, канд. экон. наук, доцент кафедры стратегического управления Института экономики, управления и бизнеса (ИНЭБ) ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ). E-mail: liana_spirina@mail.ru

Краснова Регина Анваровна, магистрант кафедры стратегического управления ИНЭБ УУНиТ. E-mail: atamindarova93@gmail.com

***Аннотация.** В статье рассматривается проблема повышения эффективности работы с обращениями граждан в условиях цифровой трансформации деятельности органов государственной власти. Актуальность обусловлена наличием дисбаланса между растущим потоком электронных обращений граждан и ограниченными кадровыми ресурсами органов государственной власти. Цель исследования разработать мероприятия по оптимизации административных процессов посредством внедрения технологий искусственного интеллекта для автоматизации классификации, маршрутизации и подготовки ответов на типовые обращения.*

* Ссылка на статью: Спирина Л.И., Краснова Р.А. К вопросу о внедрении технологий искусственного интеллекта для рассмотрения обращений граждан в органах Роспотребнадзора // Экономика и управление: научно-практический журнал. 2026. № 5. С. 121–126. DOI 10.34773/EU.2026.5.20.