Штрафы выросли, 152-ФЗ прежний:

топ ошибок в персональных данных и как их предотвратить

Илья РОМАНОВ,
руководитель отдела консалтинга АО «ДиалогНаука»

Вопросы, связанные с защитой персональных данных, всегда остаются в центре внимания. Теперь же, с 30 мая, вступают в силу изменения, которые в разы увеличивают размеры штрафов за недочеты в области ПДн. Парадокс в том, что сами требования законодательства остаются прежними, но большинство компаний до сих пор либо вовсе их не соблюдают, либо ограничиваются «бумажным» выполнением.
В результате любые нарушения, которые ранее могли привести к небольшим штрафам, теперь станут серьезной финансовой угрозой – вплоть до многомиллионных санкций. В этой статье мы рассмотрим, на какие новые цифры стоит ориентироваться, за что именно будут штрафовать, какие ошибки чаще всего делают операторы персональных данных и как перестроить работу, чтобы избежать проблем с регулятором.

Новые штрафы и уголовная ответственность: что изменится?

Главное изменение – существенный рост сумм в Кодексе об административных правонарушениях (КоАП). Если раньше, скажем, за неподачу уведомления об обработке персональных данных организация могла заплатить лишь 5 тыс. руб., то теперь максимальный размер штрафа возрастает до 300 тыс. Это более чем в 60 раз превышает первоначальную сумму.

Кроме того, впервые явно прописана ответственность за утечки персональных данных. Если нарушение безопасности и последующая утечка стали результатом действий (или бездействия) оператора, а Роскомнадзор в рамках разбирательства выяснит, что необходимые меры защиты не были приняты, штрафы могут достигать 15–20 млн руб. При повторной утечке речь идет об оборотных штрафах до 3% выручки или суммах до 500 млн руб. Это рекордные для отечественного законодательства цифры, сопоставимые с зарубежными нормами (например, в GDPR такие штрафы существуют давно).

Повышенное внимание законодатель уделяет:

- несовершеннолетним (обработка их данных рассматривается с особой строгостью);
- биометрии (распространение или утечка таких данных несет исключительно высокие риски);
- трансграничной передаче (пересылка информации за рубеж также относится к зоне особого контроля).

Наконец к административной добавляется уголовная ответственность. За незаконный сбор, передачу и хранение персональных данных теперь возможно лишение свободы до четырех лет. В первую очередь это коснется тех, кто умышленно продает базы данных, торгует личной информацией.
Но по логике права нормы могут применяться и к иным ситуациям – здесь многое зависит от судебной и правоприменительной практики, которая будет формироваться.

Несмотря на серьезность штрафов, есть определенные условия, которые позволяют снизить сумму до десяти раз. По КоАП для этого нужно:

- затрачивать на информационную безопасность не менее 0,1% выручки за последние три года;
- документально подтвердить, что в течение последнего года оператор должным образом обеспечивал защиту персональных данных;

- не иметь отягчающих обстоятельств, предусмотренных КоАП.

Эти пункты не только важны как средство смягчения санкций, но и реально повышают уровень защищенности:

- инвестиции в ИБ подразумевают внедрение современных средств защиты и привлечение квалифицированных специалистов;
- формализованные процессы позволяют контролировать все этапы обработки данных, своевременно выявлять уязвимости и оперативно реагировать на инциденты;
- актуальные документы (регламенты, модели угроз, журналы проверок) помогают постоянно держать фокус на безопасности и служат надежным доказательством добросовестности оператора при проверках.

В результате организация не только уменьшает вероятность крупных штрафов, но и создает более безопасную среду, сокращая риски реальных инцидентов, будь то утечки, компрометации или человеческие ошибки. Из вышеизложенного можно сделать вывод, что теперь соблюдение требований 152-ФЗ стало в разы критичнее. Но какие именно ошибки чаще всего приводят к санкциям?

Типичные ошибки операторов

Усиление ответственности по КоАП и Уголовному кодексу заставило многие организации «переосмыслить» давно существующие нормы по персональным данным, хотя в самом 152-ФЗ никаких принципиальных новшеств не появилось.

При этом практика проектов по приведению в соответствие с законом дает интересную картину: независимо от сферы (банк, страхование, ритейл, промышленность, государственные или муниципальные структуры) проблемы повторяются.

Большинство нарушений связано с одними и теми же ошибками: от запоздалой подачи уведомлений в Роскомнадзор до отсутствия формализованной процедуры уничтожения данных. Разберем самые распространенные из них и поясним, как избежать этих штрафных ловушек.

Не подается (или неверно подается) уведомление в Роскомнадзор

Отговорки и заблуждения бывают разными:

- «Мы не оператор, а обработчик». По закону «обработчиков» в отрыве от «операторов» не существует: тот, кто фактически обрабатывает ПДн, и есть оператор;
- «Привлечем лишнее внимание». Реестр операторов огромен – появление еще одной компании не делает вас «мишенью». Зато отсутствие уведомления – прямой повод для штрафа;
- «Мы попадаем под исключения». На практике таких исключений крайне мало, и большинство компаний в них не вписываются.

Чтобы избежать санкций, важно:

- назначить ответственного за подачу уведомления и поддержание данных в актуальном виде;
- инвентаризировать процессы: какие данные собираете, для каких целей, кому передаете;
- своевременно обновлять уведомление при появлении новых видов обработки.

Раньше за отсутствие уведомления штраф был символическим (до 5 тыс. руб.), теперь – до 300 тыс. И в дополнение – до 50 тыс. для должностных лиц. Кажется, есть повод пересмотреть риски.

Ошибки в согласиях на обработку персональных данных

Согласия и раньше были «болевой точкой» для многих операторов, но с ростом штрафов малейшее отступление от правил может обернуться весьма ощутимыми санкциями. По логике 152-ФЗ согласие нужно только тогда, когда нет прямого законного основания (например, Трудового кодекса или гражданско-правового договора). Однако на практике путаются даже в таких, казалось бы, очевидных моментах.

1. Неверное определение оснований

- Ошибочный отказ от согласия. Некоторые компании решают, что Трудовой кодекс «покрывает» любую передачу данных работников третьим лицам (например, аутсорсинговой бухгалтерии), забывая, что если передача выходит за рамки прямых требований закона, согласие обязательно.
- Напротив, избыточное согласие. Другие компании берут «универсальные» согласия на «каждый чих», включая случаи, где по закону в этом нет необходимости (например, при обычных процедурах кадрового учета). В итоге в документах накапливаются нестыковки, а субъектов персональных данных бессмысленно пугают кипой лишних бумаг.

2. Неверная форма согласия

- Общая форма вместо «письменной». Закон четко говорит, что при обработке специальных категорий, а также биометрии и медицинских данных требуется согласие в письменном виде, с полным перечнем обязательных реквизитов (ФИО, адрес субъекта, цель обработки, состав данных и т. д.). Часто эту норму игнорируют либо делают одно «универсальное» согласие на все случаи.
- Недостаточность реквизитов. Если по закону форма согласия должна содержать конкретные сведения и подпись субъекта, то «просто росписи в каком-нибудь журнале» недостаточно. Роскомнадзор при проверках особенно внимательно смотрит, соответствует ли «бумага» требованиям ст. 9 152-ФЗ.

3. Необновленные согласия

- Операторы забывают, что согласие – это документ, который должен отражать конкретную цель и объем обработки. Когда цели меняются (например, начинают использовать данные и для маркетинга, и для передачи новым подрядчикам), нужно получать новое согласие или вносить корректировки.

- Если у субъекта меняется фамилия, адрес или иные реквизиты, то согласие в его прежнем виде также может не соответствовать действительности и требовать обновления.

4. Риски «согласия ради согласия»

- Для многих компаний согласие остается формальным документом, составленным «на всякий случай». Но при реальной проверке может выясниться, что цели описаны «в общем и целом», без конкретики, а сроки хранения данных не указаны.
- Если же дело дойдет до суда или иного разбирательства, размытая формулировка согласия, не соответствующая фактическим действиям, только усугубит ситуацию.

Все эти недоработки теперь могут привести к штрафу до 300 тыс. руб. Причем Роскомнадзор уделяет согласиям особое внимание, потому что это один из самых наглядных показателей того, как оператор подходит к соблюдению 152-ФЗ на практике.

Как действовать грамотно?

1. Определяйте нужду в согласиях правильно: если есть прямое законное основание (Трудовой кодекс, гражданско-правовой договор и т. д.), то согласие не нужно. Но если задействуются специальные категории (например, биометрические данные) либо происходит передача третьим лицам, не прописанная напрямую в законе, без согласия не обойтись.

2. Следите за формой и содержанием: в ряде случаев, особенно при работе со специальными категориями ПДн, согласие нужно только в письменном виде. Убедитесь, что там есть все реквизиты, указанные в законе, и что формулировки максимально точны.

3. Актуализируйте согласия: как только меняются цели, условия или объем данных, документы нужно пересматривать. Иначе оператор официально обрабатывает одни данные «по бумаге», а фактически – совсем другие.

Соблюдение всех этих рекомендаций существенно снижает риск штрафов и дает уверенность, что даже при детальном разбирательстве оператор сможет подтвердить законность обработки персональных данных.

Отсутствие или игнорирование процедуры уничтожения персональных данных

Закон прямо обязывает операторов уничтожать персональные данные, когда:

- цель обработки достигнута (например, услуга оказана или трудовые отношения расторгнуты);
- субъект отозвал согласие, а у компании нет других законных оснований продолжать обработку.

Причем такая операция должна быть документально подтверждена: нужны и акт об уничтожении, и запись в соответствующем журнале информационной системы. Однако на практике многие организации годами хранят базы с неактуальными записями, потому что «может пригодиться», «не до этого» или «не предусмотрена процедура».

Результат – фактическая незаконная обработка, ведь оператор с точки зрения закона не имеет права держать информацию, ставшую ненужной или утратившую правовое основание для использования. Отсутствие правил «цикла жизни» данных и формальных подтверждений об их уничтожении может обернуться штрафами до 300 тыс. руб., а в случае утечки такой «балласт» только усугубит ответственность.

Чтобы избежать подобных рисков, необходимо:

- разработать регламент (или включить соответствующий раздел в уже имеющиеся внутренние документы) с четкой процедурой удаления персональных данных по истечении сроков хранения или при отзыве согласия;
- назначить ответственных за контроль исполнения (обычно это лицо, ответственное за организацию обработки ПДн либо за защиту ПДн);
- вести акты и журналы по каждому факту уничтожения, указывая, какие именно сведения были удалены и на каком основании;
- периодически проводить ревизию: проверять, не копятся ли на серверах, рабочих станциях и внешних носителях избыточные данные, которые следовало давно уничтожить.

Такой комплексный подход не только убережет от штрафов, но и позволит компании оптимизировать работу с базами, снизить риски утечек и повысить прозрачность внутренних процессов.

Не подается уведомление об утечке

Сейчас операторы персональных данных обязаны уведомлять Роскомнадзор о факте утечки в течение 24 часов с момента обнаружения и в течение следующих 72 часов представлять результаты внутреннего расследования. За несоблюдение этих сроков или полное «умалчивание» инцидента предусмотрен штраф до 3 млн руб. для юридических лиц.

На практике многие компании сталкиваются с тем, что формального регламента на случай утечки у них нет: не определена четкая процедура, кто и на каком этапе решает, считать ли произошедшее «сбоем» или полноценной компрометацией, как быстро собирать доказательную базу и готовить официальное письмо в надзорные органы. При этом закон требует не только уведомить о факте утечки, но и подтвердить, что оператор предпринимал все разумные меры защиты, иначе случившееся квалифицируют как «бездействие».

Чтобы не попасть под санкции, необходимо заранее:

- зафиксировать регламент действий при утечке: кто отвечает за выявление, кто готовит документы и официальные уведомления, как оцениваются масштаб и критичность инцидента;
- описать и отработать процесс быстрого расследования: где и как будут собираться логи, журналы событий, акты проверок систем безопасности;

- назначить ответственных лиц с полномочиями оперативно взаимодействовать с руководством и при необходимости с Роскомнадзором.

Такой подход дает возможность при возникновении инцидента сразу же отреагировать по плану и уложиться в строгие сроки. Учитывая новые штрафы и ужесточение ответственности, многие компании сталкиваются с вопросом: «С чего начать, чтобы минимизировать риски?» Ответ прост – действовать системно. Вместо хаотичных мер, которые могут привести к новым ошибкам, стоит сосредоточиться на ключевых шагах, прописанных в законе, но часто игнорируемых.

Пять шагов, которые необходимо сделать каждому оператору

Чтобы комплексно подойти к выполнению требований, полезно начать с базовых мер, которые приносят 80% пользы при 20% усилий. Все они давно описаны в законодательстве и проверены практикой.

1. Назначьте ответственных лиц

По закону требуется:

- лицо, ответственное за организацию обработки ПДн. Оно контролирует соблюдение 152-ФЗ, организует обучение персонала, занимается взаимодействием по запросам субъектов;
- лицо (или подразделение), ответственное за защиту ПДн. Формально закон не всегда обязывает издавать отдельный приказ о его назначении (в отличие от обязательного ответственного за организацию обработки), однако на практике без такого работника или подразделения все меры по защите персональных данных будут «буксовать».

2. Проведите обследование процессов обработки

Определите:

- какие данные и для каких целей обрабатываются (с разбиением на каждую цель);
- откуда поступают данные, как хранятся и кому передаются;
- есть ли законные основания или нужны согласия;
- какие технические и организационные меры обеспечения безопасности применяются.

Без ясной картины по этим вопросам невозможно корректно выстраивать защиту и оформлять документы.

3. Разработайте (или актуализируйте) пакет документов

Важно:

- не полагайтесь на «волшебные» шаблоны из интернета. Они не учитывают специфику вашей инфраструктуры и требований;
- пакет должен включать политику и регламенты (в том числе политику обработки ПДн, инструкции для персонала), формы согласий (с учетом, когда нужна письменная, а когда достаточно электронной) и сопутствующие документы: акты, журналы, приказы, модели угроз и т. п.;
- все документы должны соответствовать фактическим процессам и регулярно обновляться.

4. Приведите в соответствие сайт

Проверьте следующее:

- политика обработки ПДн на сайте должна в деталях совпадать с уведомлением, которое подается в Роскомнадзор, и с реальной практикой;
- убедитесь, что при сборе cookies и других технических данных пользователь дает информированное согласие (всплывающие окна, чекбоксы и т. д.);
- проверяйте все формы обратной связи, чтобы они содержали правильную ссылку на согласие и соответствующую форму его выражения.

5.Обеспечьте техническую защиту

Учтите при реализации технической защиты:

- минимум: модель угроз, модель нарушителя, регламент по защите данных, журналы учета и контроля;
- технические меры: средства управления доступом, антивирусы, системы сетевой безопасности, резервное копирование, анализ защищенности и т. д.;
- важно не просто «разработать бумаги», а запустить реальные процессы аудита, проверки эффективности защитных мер, вести журналы и акты, чтобы всегда иметь доказательную базу для регулятора.

Выводы

Новые штрафы, доходящие до десятков миллионов рублей и даже оборотных санкций в 3% годовой выручки, моментально поднимают планку ответственности в вопросах персональных данных. Но если всмотреться глубже, окажется, что прежние требования никуда не делись. Самые частые нарушения давно известны: неоформленные согласия, неподача уведомлений, отсутствие грамотного процесса уничтожения данных, слабая техническая защита и «формальные» документы без фактического выполнения.

Внедрение четких регламентов, корректной документации и реальных мер защиты – не только путь к снижению рисков попасть под крупные штрафы, но и способ повысить уровень информационной безопасности в целом. Законодательство давно указывает, что приведение компании в соответствие требованиям в сфере персональных данных – это не разовая акция, а непрерывный процесс, в котором важны регулярный пересмотр и адаптация правил обработки ПДн и мер их защиты.

В итоге можно сказать: все, что мы обязаны делать сегодня, мы обязаны были делать и раньше. Но теперь надеяться на отсутствие серьезных последствий не приходится: сумма штрафов выросла настолько, что любая ошибка может оказаться фатальной для бюджета компании. Главное – не откладывать приведение к соответствию «на потом», а системно подходить к вопросам защиты персональных данных, опираясь на конкретные процессы, тщательную документальную базу и отлаженные технологические решения. ■