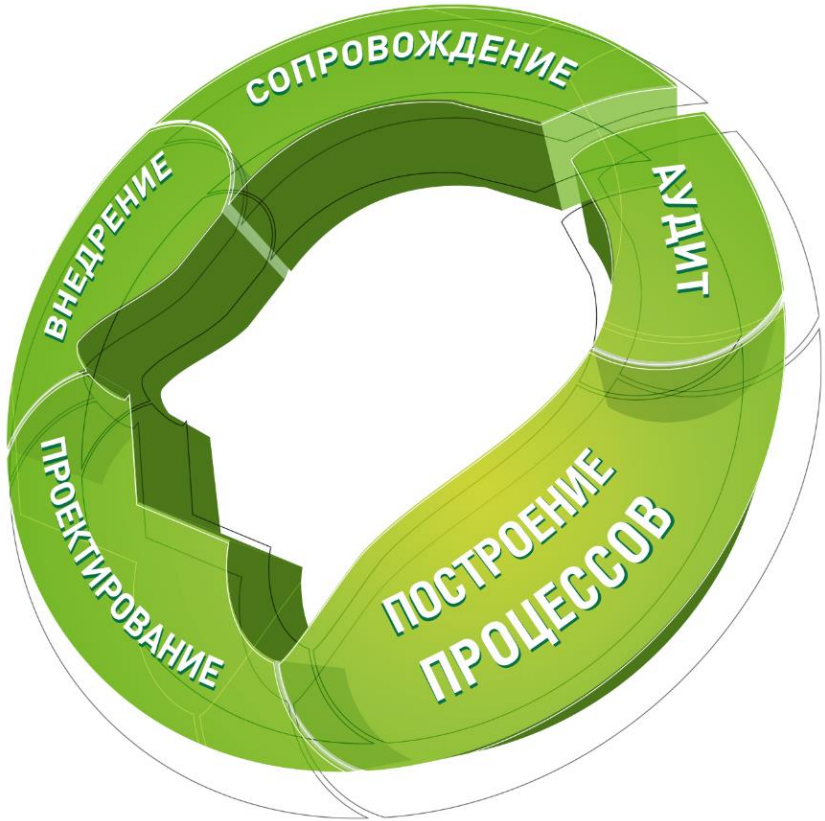
ПЕРСОНАЛЬНЫЕ ДАННЫЕ БЕЗ ШТРАФОВ:
ЧТО ПО-ПРЕЖНЕМУ ЛОМАЕТСЯ И КАК ЭТО ЧИНИТЬ?

Илья Романов
Руководитель Отдела консалтинга

ДиалогНаука

Направления деятельности

- 152-ФЗ и GDPR
- Объекты КИИ (187-ФЗ)
- Положения Банка России
- ГОСТ 57580
- PCI DSS
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



Ключевые Заказчики

Штрафы – теперь по-взрослому

❌ Неправомерная обработка – до 300 тыс ₽, повторно – до 500 тыс ₽

📪 Нет уведомления в РКН – до 300 тыс ₽

🚨 Нет уведомления об утечке – до 3 млн ₽

💧 Утечки:
– обычные ПДн – до 15 млн ₽
– спецкатегории – до 15 млн ₽
– биометрия – до 20 млн ₽
– повторно – до 3% выручки или до 500 млн ₽

Утечек больше, чем кажется

📊 **Данные РКН, а также иные источники**

- 📌 Число инцидентов почти не изменилось
- 📈 Объем утекших в 2025 году данных вырос в **2,5–5 раз**
- 🔒 Утекают базы, а не записи по одному
- 🔥 Цена ошибки – миллионы ₽ и потеря доверия

 Уголовная ответственность

- 🚫 Незаконный сбор, передача, хранение ПДн – до **4 лет лишения свободы**
- 👶 Несовершеннолетние, биометрия, спецкатегории – до **5–7 лет**
- 💰 Крупный ущерб, группа лиц – до **1 млн ₽ штрафа** или **6 лет тюрьмы**
- 🌍 Трансграничная передача – до **8 лет**
- 💥 Тяжкие последствия или организованная группа – до **10 лет и 3 млн ₽**

Правила не новы – а ошибки все те же

Компании продолжают нарушать старые требования:

- Мифы, заблуждения – повторяются из года в год
- Рассмотрим типовые ошибки, которые совершают даже крупные организации

❌ Уведомлять Роскомнадзор не нужно

Почему так думают:

- ⚖️ Неправильное толкование закона
- 😱 Страх привлечь внимание
- 🤝 Мы – обработчик, а не оператор

Реальность:

📄 **Уведомление обязательно** для всех операторов ПДн, за исключением единичных случаев, предусмотренных законом.

💸 **Штрафы за неуведомление**:

- Должностные лица: **30–50 тыс. ₽**
- Юридические лица: **100–300 тыс. ₽**

❌ Ошибка: Проблемы с согласиями

⚖️ Если цель обработки прямо предусмотрена законом – согласие **не требуется**

📄 Примеры: оформление по ТК, исполнение договора, сдача отчетности

🚫 Но в остальных случаях – согласие **обязательно**

👥 Кандидаты, пропуска, внешние исполнители – частые «зоны риска»

Согласие в письменной форме

- Передача данных работника подрядчику, в банк, IT-компании
- Биометрия, здоровье, убеждения
- Типовая ошибка: нет письменного согласия → нарушение
- Штраф: до **300 тыс. ₽**, повторно – до **500 тыс. ₽**

- Проверьте формы согласий – большинство из них могут быть невалидны в глазах РКН

Ошибка: ПДн хранят вечно

Закон требует уничтожать ПДн:
– после достижения цели
– при отзыве согласия
– при отсутствии законных оснований

Нужны подтверждающие документы (Приказ РКН от 28.10.2022 № 179):
– Акт об уничтожении с деталями
– Выгрузка из журнала ИСПДн

Отсутствие процедуры = **нарушение**
Штраф – до **300 тыс. ₽**, повторно – до **500 тыс. ₽**

Уведомление об утечках

Оператор обязан сообщить РКН:
– о самом инциденте
– о результатах внутреннего расследования

Что включают уведомления:
– дата, причина, характеристики ПДн
– предполагаемый вред
– меры по устранению
– виновные лица и ИС, где все случилось

Штраф за молчание – до **3 млн ₽** для юрлица

Смягчающие факторы: в 10 раз меньше

Штраф за утечку может быть снижен в **10 раз**, если выполнены три условия:

1. Траты на ИБ за 3 года – не менее **0,1% выручки**
2. Документально подтверждена защита ПДн в ИСПДн
3. Нет отягчающих обстоятельств по КоАП

Все должно быть задокументировано и актуально

✅ Как не попасть под раздачу

5 шагов, которые работают

- 📋 Не «для галочки», а для защиты
- 💡 Первое, с чего стоит начать

Шаг 1. Назначьте ответственных

📌 Два ключевых направления:
– за **обработку ПДн**
– за **защиту ПДн** (можно совместить, но роли разные)

🔍 Обязанности ответственного за организацию обработки:
– контроль за соблюдением требований
– информирование сотрудников
– работа с запросами субъектов ПДн

❗ Отсутствие ответственных =
нарушение + высокие риски других нарушений

Шаг 2. Начните с обследования

🔍 Без понимания процессов не получится построить защиту

📌 Определите:
– какие ПДн вы реально обрабатываете
– для каких целей
– кто и как их обрабатывает
– где они хранятся, куда передаются, зачем и почему

❗ Перечень целей – это основа всей дальнейшей работы

Понять, что такое ПДн и ИСПДн

- Понятие ПДн – размытое: важно правильно определить, какие данные действительно персональные
- ИСПДн – тоже не всегда очевидно:
  – где границы?
  – как быть с облаками?
  – что включается в систему?
  – как это документировать?
- Ошибки на этом этапе ведут к нарушениям

Шаг 3. Аккуратнее с «шаблонами»

🛠 Шаблоны из интернета не работают – они не учитывают реальность вашей компании

📋 Нужно:
– разработать документацию под свои процессы
– уведомить РКН
– настроить процессы и их регулярно поддерживать

✅ Это не «бумажки для галочки», а защита бизнеса от штрафов и проверок

Шаг 4. Сайты – Политика

📄 Политика обработки ПДн на сайте – обязательна

⚠️ Типовые нарушения:

– нет политики вовсе
– нет ссылки с главной страницы
– не соответствует требованиям 152-ФЗ (очень часто – отсутствие конкретики по целям обработки)

✅ Политика должна быть доступной, актуальной и отражать реальные процессы

Шаг 4. Сайты – Согласия

🍪 Cookie и метрика → всплывающее окно, отдельная цель

📊 Google Analytics и прочие = трансграничка (уже нельзя!)

📌 В согласии указать:

– цель, состав, передача третьим лицам
– ссылку на политику
– данные об операторе

❗ Согласие – это не «галочка в форме», а документ

Шаг 5. Техническая защита

⚙ Реальная защита ПДн – это не только документы

👷 Нужны работающие процессы:

- моделирование актуальных угроз
- 📐 адаптация под вашу ИТ-инфраструктуру
- 🧪 регулярная оценка соответствия СрЗИ и общая оценка эффективности СЗПДн
- 🔄 постоянное поддержание мер защиты (мониторинг, обновление, контроль, техподдержка,…)

✅ Документы работают только тогда, когда **они свои и актуальные**

Корректные, обоснованные документ:

позволяютыва

Шаг 5. Техническая защита

Средства защиты информации, корректные и актуальные документы и процессы – обязательные условия для:

- ✅ снижения вероятности утечек
- ✅ снижения вероятности штрафов и санкций

Главное – действовать, а не бояться

- 📌 Требования давно известны, но теперь они подкреплены серьёзными санкциями
- 💡 Важны не только «бумажки», но и системная, комплексная работа с рисками
- ✅ Даже небольшие шаги уже значительно снижают угрозы

Вопросы?

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: info@DialogNauka.ru