# **ЦЕНА ЗА ПЕРСОНАЛЬНЫЕ ДАННЫЕ: КАК НЕ ПОПАСТЬ НА МИЛЛИОНЫ**

Илья Романов Руководитель Отдела консалтинга

ilya.romanov@dialognauka.ru



# 💢 Штрафы – теперь по-взрослому

- Ж Неправомерная обработка до 300 тыс ₽, повторно до 500 тыс ₽
- **Г** 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 ₽



### **П** Данные РКН, а также иные источники

- Число инцидентов почти не изменилось
- 🖲 Утекают базы, а не записи по одному
- **∥** Цена ошибки миллионы ₽ и потеря доверия

### **Уголовная ответственность**

- О Незаконный сбор, передача, хранение ПДн до 4 лет лишения свободы
- О 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 ₽

Компании продолжают нарушать старые требования:

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

## **Х** Уведомлять Роскомнадзор не нужно

#### Почему так думают:

- Неправильное толкование закона
- Отрах привлечь внимание
- ♥ Мы обработчик, а не оператор

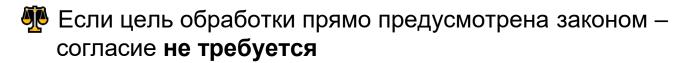
#### Реальность:

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

#### 💸 Штрафы за неуведомление:

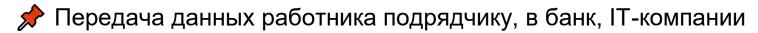
- > Должностные лица: 30–50 тыс. ₽
- > Юридические лица: 100–300 тыс. ₽

# **Х** Ошибка: Проблемы с согласиями



- Примеры: оформление по ТК, исполнение договора, сдача отчетности
- О Но в остальных случаях согласие обязательно
- Кандидаты, пропуска, внешние исполнители частые «зоны риска»





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. ₽** 



- Ф 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



### **Горматичающие 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



#### 5 шагов, которые работают



₽ Первое, с чего стоит начать

**ДиалОгНаука** 



### 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



Без понимания процессов не получится построить защиту

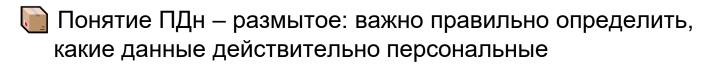


#### Определите:

- 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

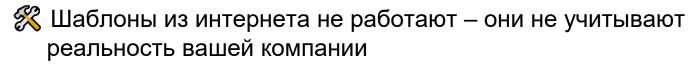
# Понять, что такое ПДн и ИСПДн



- ИСПДн тоже не всегда очевидно:
  - где границы?
  - как быть с облаками?
  - что включается в систему?
  - как это документировать?

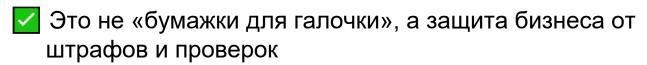


# Шаг 3. Аккуратнее с «шаблонами»



### 🗐 Нужно:

- разработать документацию под свои процессы
- уведомить РКН
- настроить процессы и их регулярно поддерживать



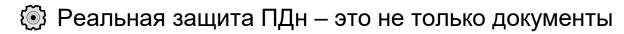
- Политика обработки ПДн на сайте обязательна
- Типовые нарушения:
  - нет политики вовсе
  - нет ссылки с главной страницы
  - не соответствует требованиям 152-ФЗ (очень часто)

- Ооокіе и метрика → всплывающее окно, отдельная цель
- В согласии указать:
  - цель, состав, передача третьим лицам
  - ссылку на политику
  - данные об операторе

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

**ΔυαΛΟΓΗανκα** 







- моделирование актуальных угроз
- 📐 адаптация под вашу ИТ-инфраструктуру
- регулярная оценка соответствия
- остоянное поддержание мер защиты
- ✓ Документы работают только тогда, когда они **свои** и **актуальные**

- 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

ilya.romanov@dialognauka.ru

