



ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ

# ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ 152-ФЗ

Новые изменения в штрафах —  
что нас ждет?

Александра Остапова  
Старший аналитик УЦСБ







# Спикеры



**Модератор**  
Ксения Кузнецова

---

Руководитель группы в направлении аудитов  
и соответствия требованиям ИБ



**Спикер**  
Александра Остапова

---

Старший аналитик направления аудитов  
и соответствия требованиям ИБ





# План вебинара

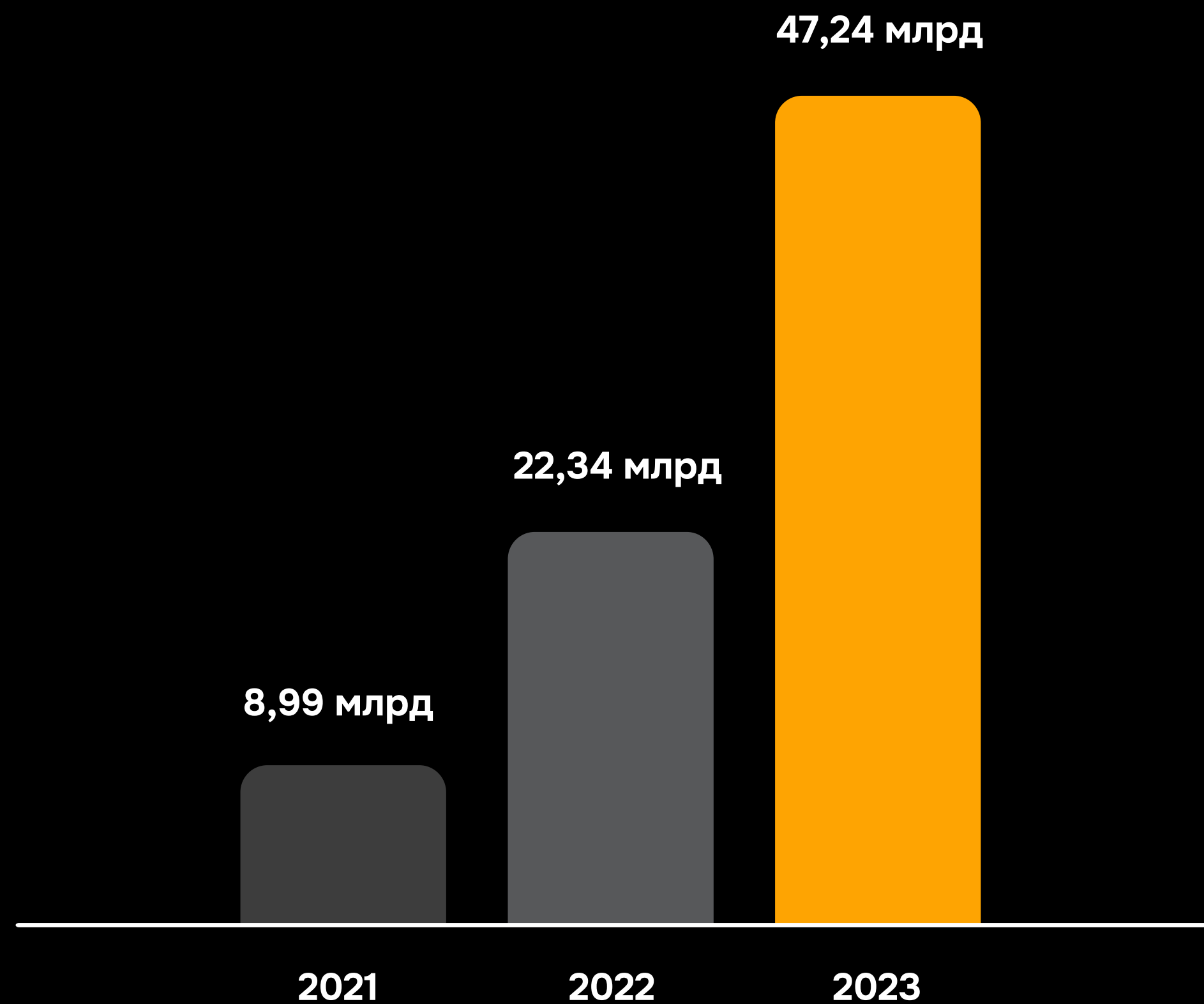
- 01** Статистика утечек данных
- 02** Ретроспектива
- 03** Изменения в КоАП РФ
- 04** Что делать операторам ПДн?
- 05** Ответы на актуальные вопросы





# Статистика утечек данных в мире

Количество утекших ПДн в мире



## Мир

- Количество утечек ПДн за 2023 год выросло более чем на **60%**
- На одну утечку в среднем пришлось **4,04 млн.** записей ПДн
- Зарегистрировано **1024 крупных утечек** данных, каждая из которых включает не менее **1 млн.** записей ПДн

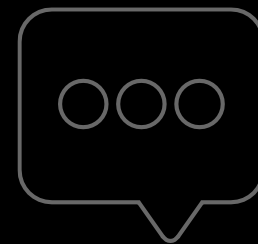
## Россия

- Роскомнадзор зафиксировал **168 фактов** утечек ПДн
- Судами рассмотрено **87 протоколов**, составленных Роскомнадзором
- Общая сумма штрафов более **4,6 млн.** рублей
- Средний штраф – **60 тыс.** рублей





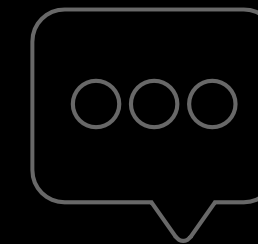
# Привлечение к ответственности в России



Вчера в свободный доступ были выложены данные заказов и покупателей предположительно сети винных магазинов [winestyle.ru](https://winestyle.ru). 📌

В текстовом файле, содержащем 1,154,694 строки, находятся: имена, телефоны (427 тыс. уникальных), адреса эл. почты (407 тыс. уникальных), адреса доставки, содержимое, даты и стоимость заказов, IP-адреса.

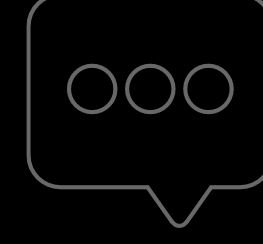
Данные датируются 23.10.2024.



Несколько дней назад в свободный доступ были выложены текстовые файлы, содержащие дампы нескольких таблиц из базы данных предположительно сайта [shop.mgnl.ru](https://shop.mgnl.ru) - интернет-магазина сети супермаркетов «Магнолия». 📌

Опубликованная информация содержит:

- 🌿 ФИО (часто это автосгенеренные последовательности в формате П<номер телефона>)
- 🌿 адрес доставки
- 🌿 адрес эл. почты (245,931 уникальный адрес, часто это автосгенеренные последовательности в формате <номер телефона>@shop.mgnl.ru)
- 🌿 номер телефона (252,209 уникальных номеров)
- 🌿 хешированный пароль
- 🌿 состав, стоимость и дата заказа
- 🌿 купон на скидку



В конце августа этого года, хакеры выложили в открытый доступ резервную копию (в формате *Norton Ghost*) базы данных 1С с информацией о клиентах и сотрудниках предположительно сети фитнес-клубов «World Class». 🔥

Нам удалось проанализировать таблицы из этой базы, содержащие данные примерно 2,2 млн юридических и физических лиц (активных, неактивных и потенциальных клиентов) и 10,1 тыс. сотрудников. 📌

В таблицах с клиентами находится:

- 🌿 ФИО (или название организации)
- 🌿 адрес
- 🌿 телефон (1,9 млн уникальных номеров)
- 🌿 адрес эл. почты (712 тыс. уникальных адресов)
- 🌿 дата рождения
- 🌿 пол
- 🌿 паспортные данные (не для всех)
- 🌿 частичный номер банковской карты (не для всех)
- 🌿 банковские реквизиты (для юрлиц)
- 🌿 информация о записях на индивидуальные тренировки, посещениях клубов и т.п.
- 🌿 ссылка на фотографию (на сервере [solutions.worldclass.ru](https://solutions.worldclass.ru))



# Ретроспектива

**2017**

Расширение составов правонарушений в области обработки и защиты ПДн

**2021**

Предложение Роскомнадзора обязать операторов компенсировать моральный вред жертвам утечек

**2024**

Принятие поправок в КоАП РФ об ужесточении ответственности и введению оборотных штрафов

**2020**

Предложение Минюста России по значительному увеличению штрафов за утечку ПДн

**2022**

Инициатива Минцифры России по введению оборотных штрафов за утечки ПДн



# Терминология

- **ПДн** – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)
- **Операторы** – это любые организации, которые обрабатывают ПДн, а также определяют **цели их обработки**, состав необходимых для обработки ПДн и операции, совершаемые с ПДн
- **Утечка ПДн** – это неправомерная передача (предоставление, распространение, доступ) ПДн лицам, не имеющим разрешения на доступ



# Область действия изменений

Принятый закон распространяется на:

- **должностных лиц**, под которыми понимаются должностные лица государственных или муниципальных органов либо некоммерческих организаций
- **юридических лиц**, под которыми понимаются юридические лица, не являющиеся государственными или муниципальными органами, либо некоммерческой организацией
- **индивидуальных предпринимателей**
- **граждан**





# Изменения в КоАП РФ

- 01** Увеличение штрафов за незаконную обработку ПДн
- 02** Введение новых составов правонарушений за:
  - отсутствие уведомления в Роскомнадзор о намерении осуществлять обработку ПДн
  - отсутствие уведомления в Роскомнадзор об утечке ПДн
  - утечки иных\* категорий ПДн
  - утечки специальных или биометрических категорий ПДн
  - повторные утечки ПДн
- 03** Введение новых составов правонарушений за нарушение порядка обработки и обеспечения безопасности биометрических ПДн в ЕБС

\* и разрешенных субъектом ПДн для распространения, если легитимность обработки таких ПДн была нарушена



# **Увеличение штрафов за незаконную обработку ПДн**





# Незаконная обработка ПДн

Норма	Содержание нарушения	Для кого	Было (рублей)	Стало (рублей)
ч. 1 ст. 13.11	Обработка ПДн в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработка ПДн, несовместимая с целями сбора	Граждане Должностные лица Юридические лица	2 тыс. – 6 тыс. 10 тыс. – 20 тыс. 60 тыс. – 100 тыс.	10 тыс. – 15 тыс. 50 тыс. – 100 тыс. 150 тыс. – 300 тыс.
ч. 1.1. ст. 13.11	Повторное совершение административного правонарушения, предусмотренного ч. 1 ст. 13.11	Граждане Должностные лица Юридические лица	4 тыс. – 12 тыс. 10 тыс.– 50 тыс. 50 тыс.– 100 тыс. (для ИП) 100 тыс. – 300 тыс.	15 тыс. – 30 тыс. 100 тыс. – 200 тыс. 300 тыс. – 500 тыс.



# **Новые составы правонарушений при обработке ПДн**





# Отсутствие уведомления о намерении осуществлять обработку ПДн

Норма	Содержание нарушения	Для кого	Стало (рублей)
ч. 10 ст. 13.11	Невыполнение и (или) несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора о намерении осуществлять обработку ПДн  <i>ч. 1 ст. 22 152-ФЗ</i>	Граждане Должностные лица Юридические лица	5 тыс. – 10 тыс. 30 тыс. – 50 тыс. 100 тыс. – 300 тыс.

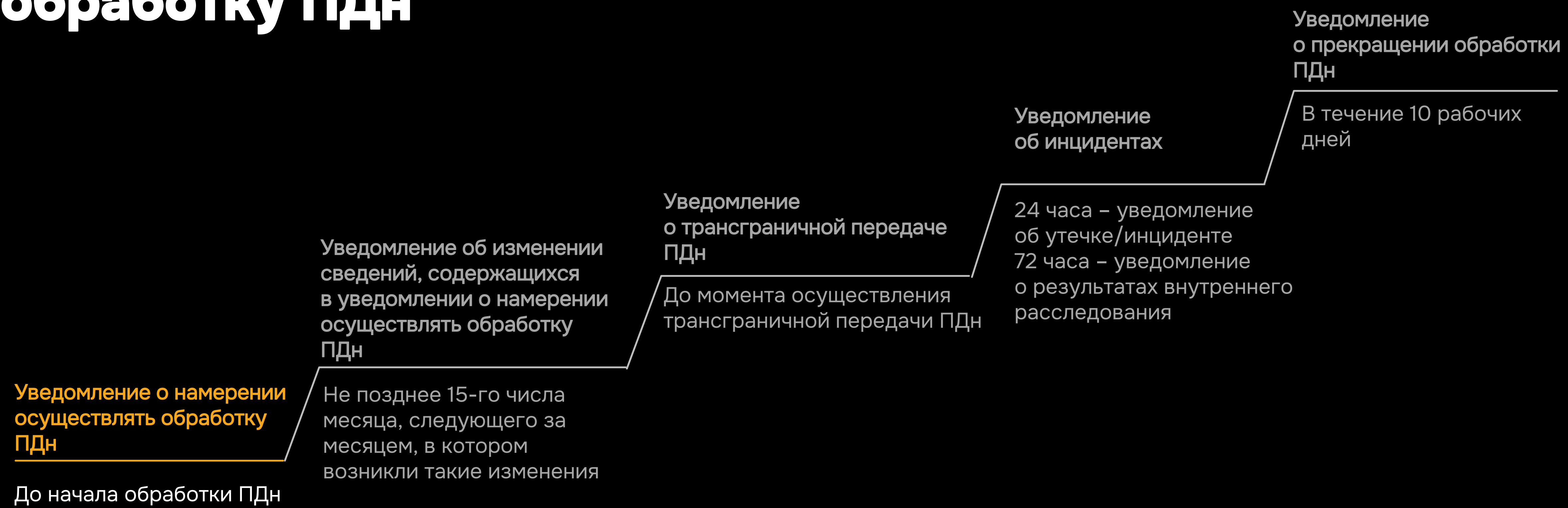


# Опрос слушателей





# Отсутствие уведомления о намерении осуществлять обработку ПДн





# Отсутствие уведомления об обработке: что нужно знать?

Уведомлять Роскомнадзор не нужно, если оператор осуществляет обработку ПДн (п.2 ст. 22 152-ФЗ):

- без использования средств автоматизации
- в случаях, предусмотренных законодательством о транспортной безопасности
- включенных в государственные автоматизированных информационные системы или в государственные информационные системы ПДн, созданные в целях защиты безопасности государства и общественного порядка

В иных случаях необходимо подать уведомление о намерении осуществлять обработку ПДн для включения в Реестр операторов ПДн.

Направить уведомление в Роскомнадзор можно одним из следующих способов:

- в бумажном виде
- в электронном виде с использованием усиленной квалифицированной электронной подписи
- в электронном виде с использованием средств аутентификации Госуслуг



Важно: уведомлять Роскомнадзор необходимо не только о начале обработки ПДн, но и об изменениях в порядке обработки или о ее прекращении (в течение 10 рабочих дней с даты внесения изменений или прекращения обработки) (ч.7 ст.22 152-ФЗ). Формы уведомлений представлены на сайте Роскомнадзора.



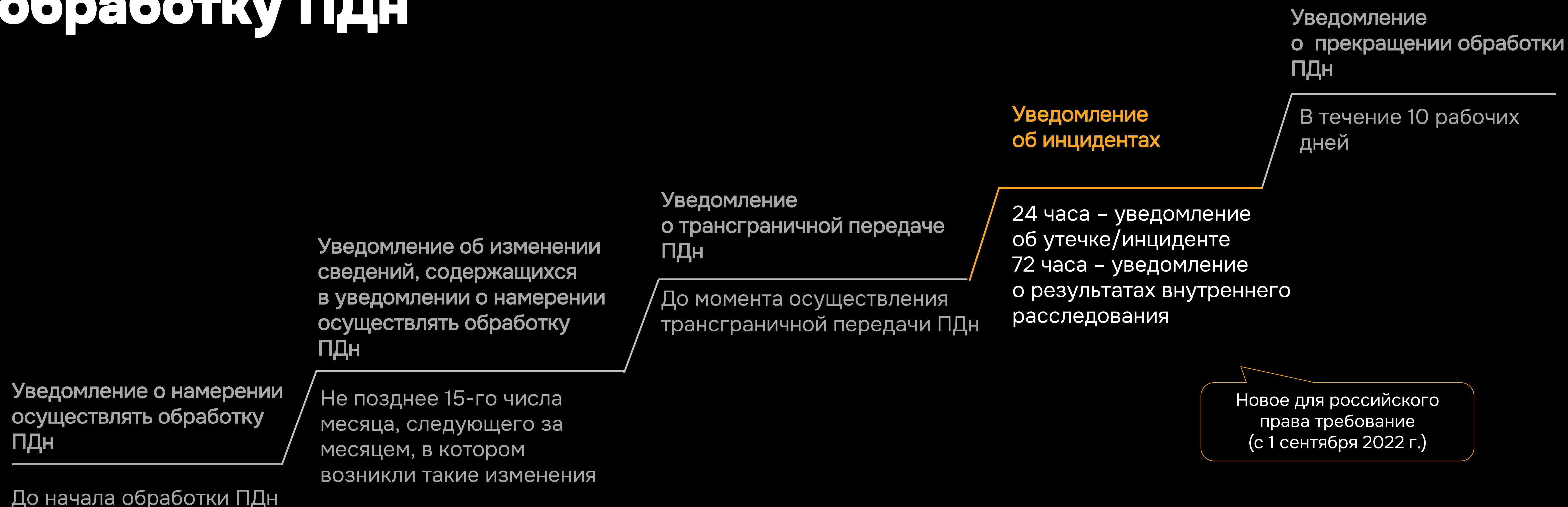


# Отсутствие уведомления об утечке ПДн

Норма	Содержание нарушения	Для кого	Стало (рублей)
ч. 11 ст. 13.11	Невыполнение и (или) несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора в случае установления факта неправомерной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн <i>ч. 3.1 ст. 21 152 ФЗ</i>	Граждане Должностные лица Юридические лица	50 тыс.– 100 тыс. 400 тыс.– 800 тыс. 1 млн. – 3 млн.



# Отсутствие уведомления о намерении осуществлять обработку ПДн





# Отсутствие уведомления об утечке ПДн: что нужно знать?

Оператор	Кого уведомлять	Как уведомлять	Когда уведомлять
Субъект КИИ	НКЦКИ	е-mail: <a href="mailto:incident@cert.gov.ru">incident@cert.gov.ru</a> тел.: <a href="tel:+79169010742">+7 (916) 901-07-42</a>  факс: <a href="tel:+749914464">7 (499) 144-64</a>  средства технической инфраструктуры	3 часа – уведомление об инциденте со значимым объектом КИИ (для субъекта КИИ)  24 часа – уведомление об утечке/ инциденте
Не субъект КИИ	Роскомнадзор (передает сведения в НКЦКИ)	<a href="#">Уведомления на сайте Роскомнадзора</a>	24 часа – уведомление об утечке/ инциденте  72 часа – уведомление о результатах внутреннего расследования



# Утечка иных\* категорий ПДн

В соответствии с ч. 12, 13, 14 ст. 13.11 КоАП РФ ответственность наступает за действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн. Размер штрафа зависит от объема неправомерно переданных ПДн, количества субъектов ПДн и идентификаторов

Норма	Градация объемов	Для кого	Штраф (рублей)
ч. 12 ст. 13.11	от 1 тыс. до 10 тыс. субъектов ПДн, от 10 тыс. до 100 тыс. идентификаторов	Граждане Должностные лица Юридические лица	100 тыс.– 200 тыс. 200 тыс. – 400 тыс. 3 млн. – 5 млн.
ч. 13 ст. 13.11	от 10 тыс. до 100 тыс. субъектов ПДн, от 100 тыс. до 1 млн. идентификаторов	Граждане Должностные лица Юридические лица	200 тыс. – 300 тыс. 300 тыс. – 500 тыс. 5 млн. – 10 млн.
ч. 14 ст. 13.11	более 100 тыс. субъектов ПДн, более 1 млн. идентификаторов	Граждане Должностные лица Юридические лица	300 тыс.– 400 тыс. 400 тыс. – 600 тыс. 10 млн. – 15 млн.

\* и разрешенных субъектом ПДн для распространения, если легитимность обработки таких ПДн была нарушена





# Утечка иных категорий ПДн: что нужно знать?

- **Идентификаторы** — уникальные обозначения сведений о физических лицах, необходимые для определения таких лиц (далее — идентификаторы).
- **Уникальное обозначение сведений** — любая запись в базе данных, прямо или косвенно относящаяся к субъекту ПДн



Важно верно идентифицировать категории ПДн



Важно легитимно обрабатывать ПДн, разрешенные субъектом ПДн для распространения



# Утечка специальных и биометрических категорий ПДн

Норма	Содержание нарушения	Для кого	Штраф (рублей)
ч. 16 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей специальную категорию ПДн	Граждане Должностные лица Юридические лица	300 тыс. – 400 тыс. 1 млн. – 1,3 млн. 10 млн. – 15 млн.
ч. 17 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей биометрические ПДн	Граждане Должностные лица Юридические лица	400 тыс. – 500 тыс. 1,3 млн. – 1,5 млн. 15 млн. – 20 млн.



## Утечка специальных или биометрических категорий ПДн: что нужно знать?

- **Специальные категории ПДн** – это данные касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости
- **Биометрические ПДн** – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн



# Обработка биометрических ПДн

## Неавтоматизированная обработка БПДн

- ➔ Обработка в рамках 152-ФЗ
- ➔ Идентификация **без использования** средств автоматизации (сравнивает человек)
- ➔ Ответственность – в ч. 17 ст. 13.11 КоАП

## Автоматизированная обработка БПДн

- ➔ Обработка в рамках 572-ФЗ
- ➔ Идентификация и (или) аутентификация **с использованием** средств автоматизации
- ➔ Ответственность – в ст. 13.11.3 КоАП





# Повторная утечка ПДн

Норма	Содержание нарушения	Для кого	Штраф (рублей)
ч. 15 ст. 13.11	Совершение административного правонарушения, предусмотренного ч. 12-14 ст. 13.11, лицами, которые ранее уже привлекались в соответствии с ч. 12-15, 16-18 ст. 13.11 КоАП РФ за действия (бездействие), повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн	Граждане Должностные лица Юридические лица	400 тыс. – 600 тыс. 800 тыс. – 1,2 млн. от 1% до 3%, но не менее 20 млн. и не более 500 млн.
ч. 18 ст. 13.11	Совершение административного правонарушения, предусмотренного ч. 16 или 17 ст. 13.11, лицом, которое ранее уже привлекалось в соответствии с ч. 12-18 ст.13.11 КоАП РФ к административной ответственности	Граждане Должностные лица Юридические лица	500 тыс. – 800 тыс. 1,5 млн. – 2 млн. от 1% до 3%, но менее 25 млн. и не более 500 млн.

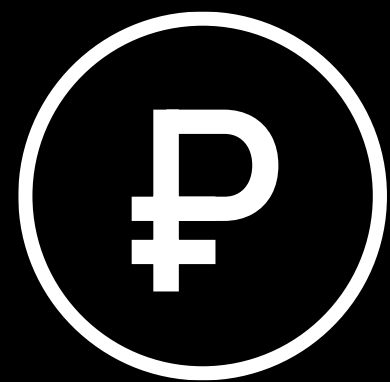


## Повторная утечка ПДн: что нужно знать?

- **Выручка оператора** – это совокупность размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение
- **В течение какого времени утечка считается повторной?**  
В соответствии с п. 2 ст. 4.6 КоАП РФ утечка считается «повторной» в течение одного года с момента уплаты административного штрафа



# Смягчающие обстоятельства

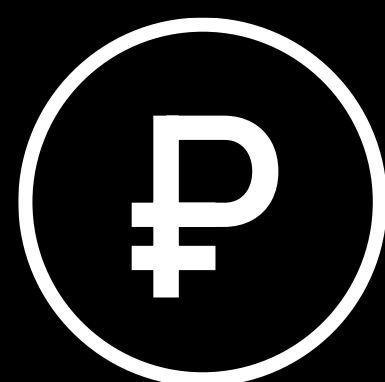


## Инвестиции в ИБ

Оператор за последние 3 года расходует не менее 0,1% годовой суммы выручки на мероприятия по обеспечению информационной безопасности



## Смягчающие обстоятельства



### Инвестиции в ИБ

Оператор за последние 3 года расходует не менее 0,1% годовой суммы выручки на мероприятия по обеспечению информационной безопасности



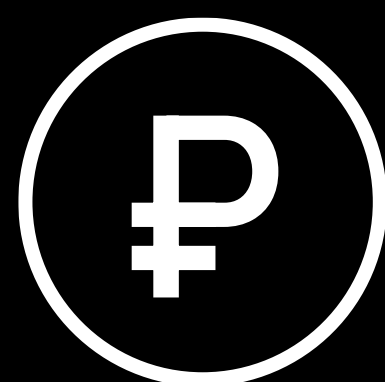
### Выполнение 152-ФЗ

Соблюдение требований к защите ПДн при их обработке в ИСПДн (с документальным подтверждением указанного факта, проведенного в течение 12 месяцев)



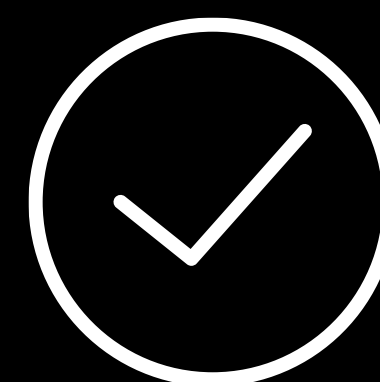


## Смягчающие обстоятельства



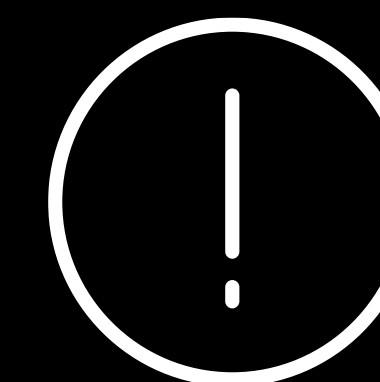
### Инвестиции в ИБ

Оператор за последние 3 года расходует не менее 0,1% годовой суммы выручки на мероприятия по обеспечению информационной безопасности



### Выполнение 152-ФЗ

Соблюдение требований к защите ПДн при их обработке в ИСПДн (с документальным подтверждением указанного факта, проведенного в течение 12 месяцев)



### Отсутствие отягчающих обстоятельств

Прошлая ответственность за нарушение требований к обработке ПДн. Оператор ранее не привлекался к ответственности по ч.1-11 ст.13.11, а также ст. 13.6, 13.12 КоАП РФ



# **Новые составы правонарушений при обработке ПДн в ЕБС**



# Защита биометрических ПДн в ЕБС

Норма	Содержание нарушения	Для кого	Штраф (рублей)
ч. 2 ст. 13.11.3	Нарушение порядка обработки БПДн в ЕБС, порядка обработки БПДн, векторов ЕБС в ИС гос. органов, ЦБ РФ, организаций, прошедших аккредитацию и осуществляющих аутентификацию на основе БПДн физических лиц, либо требований к информационным технологиям и техническим средствам, предназначенным для обработки БПДн, векторов ЕБС в целях проведения идентификации и (или) аутентификации	Должностные лица Юридические лица	100 тыс. – 300 тыс. 500 тыс. – 1 млн.
ч. 3 ст. 13.11.3	Непринятие организационных и технических мер по обеспечению безопасности БПДн при их обработке в ЕБС, ее взаимодействию с иными ИС либо непринятие организационных и технических мер по обеспечению безопасности БПДн при их обработке в иных ИС, обеспечивающих аутентификацию с использованием БПДн физических лиц, в том числе в ИС аккредитованных гос. органов	Должностные лица Юридические лица	300 тыс. – 500 тыс. 1 млн. – 1,5 млн.
ч. 4 ст. 13.11.3	Обработка БПДн, векторов ЕБС для аутентификации физических лиц в ИС гос. органов, организаций, ИС ЦБ РФ без аккредитации либо в случае, если аккредитация приостановлена или прекращена	Должностные лица Юридические лица	500 тыс. – 1 млн. 1 млн. – 2 млн.



# Обработка биометрических ПДн

## Неавтоматизированная обработка БПДн

- ➔ Обработка в рамках 152-ФЗ
- ➔ Идентификация **без использования** средств автоматизации (сравнивает человек)
- ➔ Ответственность – в ч. 17 ст. 13.11 КоАП

## Автоматизированная обработка БПДн

- ➔ Обработка в рамках 572-ФЗ
- ➔ Идентификация и (или) аутентификация **с использованием** средств автоматизации
- ➔ Ответственность – в ст. 13.11.3 КоАП





# Мероприятия по снижению рисков утечек ПДн

## 01 Провести **аудит процессов организации обработки и обеспечения безопасности** ПДн:

- Определить цели, перечень ПДн, состав ПДн, операции над ПДн, условия обработки и третьих лиц, кому передаются ПДн
- Определить (важно назначить) ответственного за организации обработки ПДн
- Провести оценку эффективности системы защиты ПДн
- Заполнить форму уведомления о намерении осуществлять обработку ПДн и направить её в Роскомнадзор
- Осуществить контроль за соответствием информации, зафиксированной в уведомлении о намерении осуществлять обработку ПДн, действительности и, по мере необходимости, направить уведомление об изменениях в Роскомнадзор

## 02 Выстроить **процесс реагирования на инциденты**:

- Регламентировать процесс реагирования на инциденты
- Подготовить условия для мониторинга инцидентов информационной безопасности и обеспечить реагирование на них или подключиться к корпоративному центру мониторинга
- Обеспечить информирование Роскомнадзора в случае утечки ПДн

## 03 Повышать **осведомленность** пользователей в вопросах обеспечения безопасности ПДн



# Опыт УЦСБ

↗ 17

лет на рынке

↗ 1000

профессионалов в штате

↗ 4000

реализованных проектов

## УСЛУГИ ПО ЗАЩИТЕ ПДН



Аудит процессов  
обработки и защиты ПДн



Разработка организационно-  
распорядительной документации



Проектирование СЗПДн



Оценка эффективности СЗПДн



Моделирование угроз  
безопасности ПДн



Аттестация ИСПДн, ЦОД



Тестирование на  
проникновение



Обучение антифишингу



ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ

# Кейсы





## Кейс 1 – утечка

**Первая ситуация:** в сети опубликована «расширенная» версия БД юридического лица, которая фигурировала в утечке ранее.

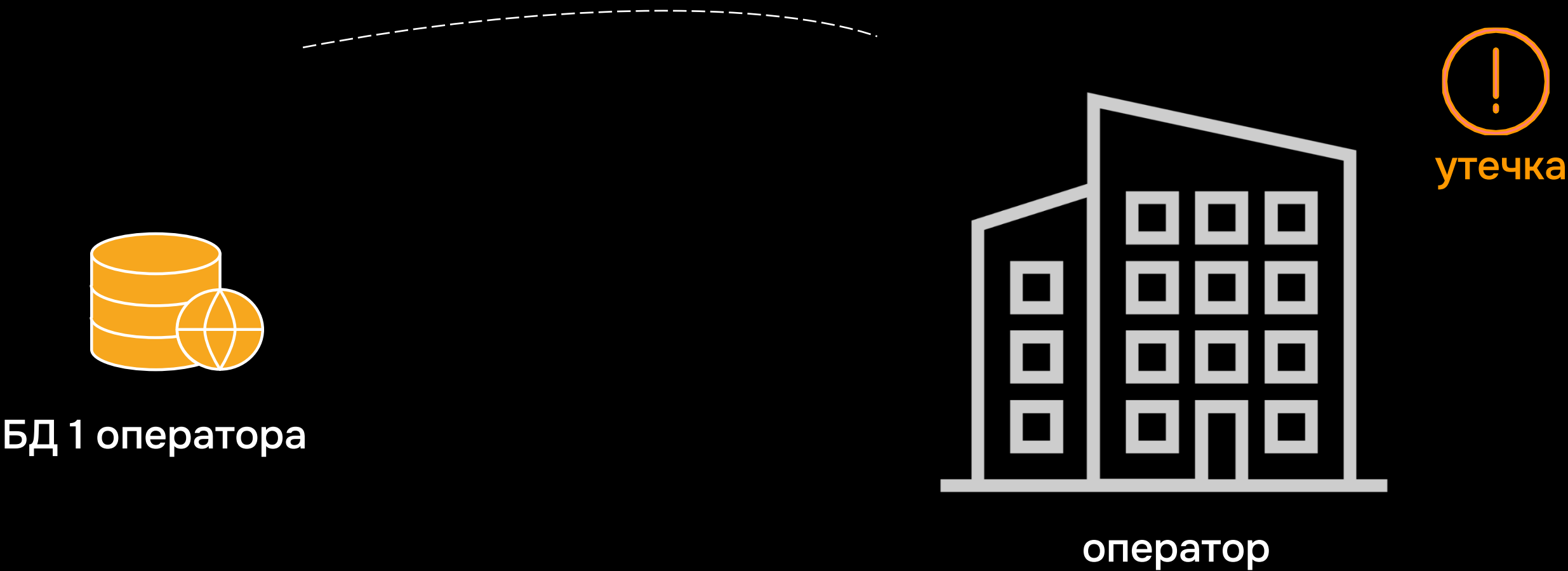
**Вторая ситуация:** опубликована БД, которая фактически является объединённой с БД другого юридического лица.

Что следует делать оператору?





# Кейс 1 – утечка







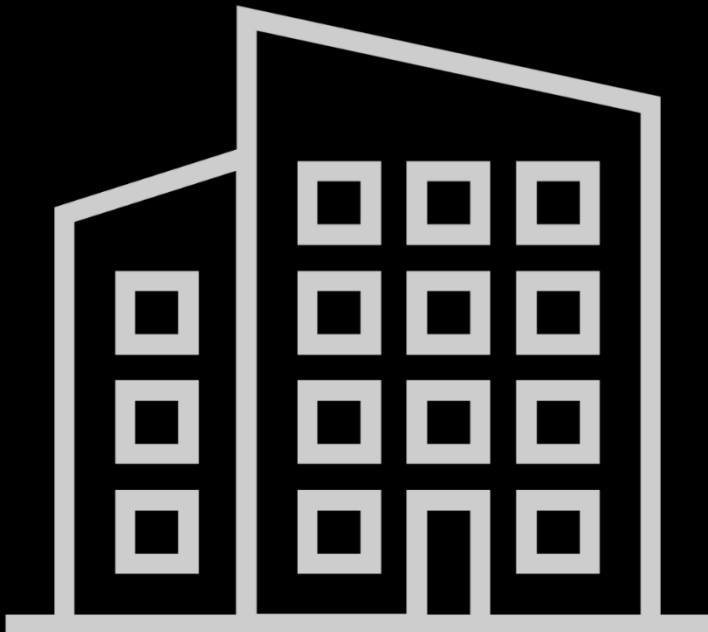
# Кейс 1 – утечка



БД 2 из интернета  
(не оператора)



БД 1 оператора



оператор



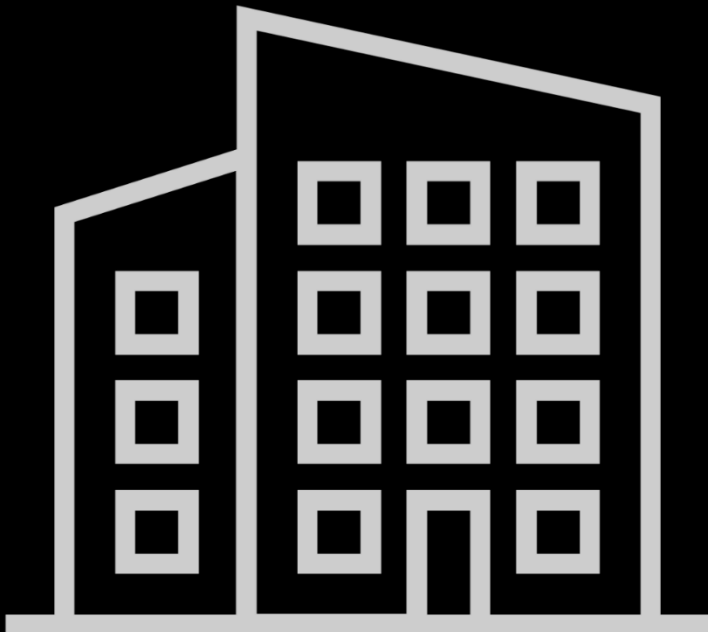
утечка



# Кейс 1 – утечка



БД 1 оператора +  
БД 2 из Интернета



оператор



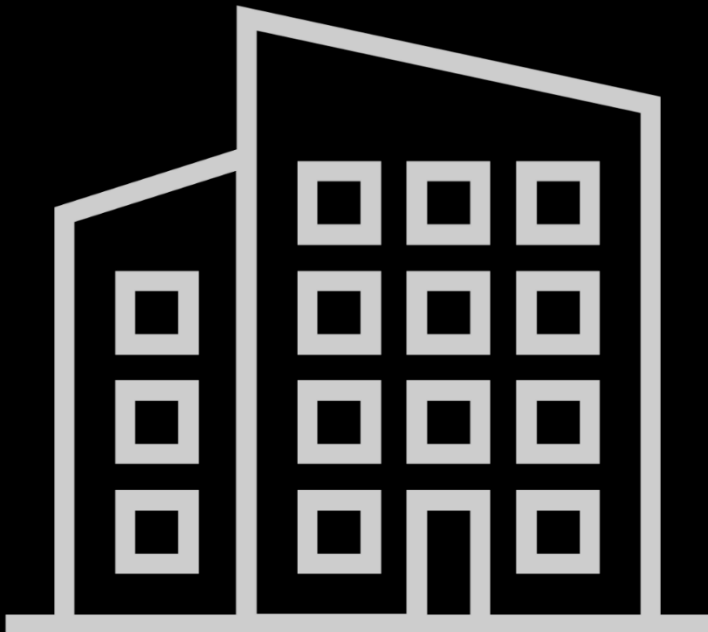
утечка



# Кейс 1 – утечка



БД 1 оператора +  
БД2 из Интернета



оператор



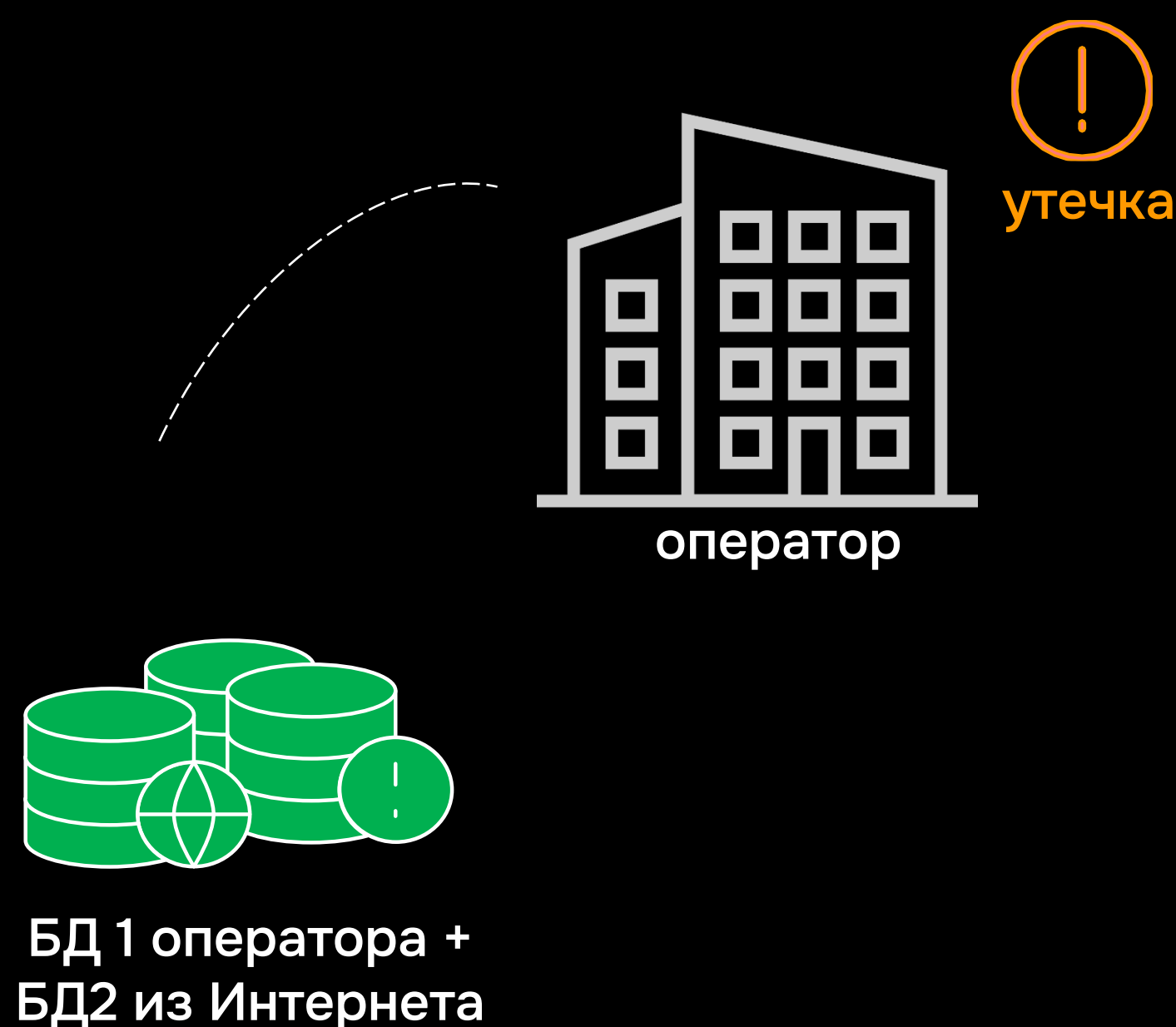
утечка



Ответственность за БД1 или за БД2?



## Кейс 1 – утечка



Оператору нужно будет **доказать**, предоставить:

1. Результаты регистрации утечки ПДн (уведомление)
2. Результаты расследования инцидента (уведомление)
3. Свидетельства: переписки, выгрузки, копии образов и т.д.



## Кейс 2 – обработчик

Утечка произошла у лица, действующего в рамках поручения на обработку ПДн.

Как в данном случае будет распределяться ответственность?

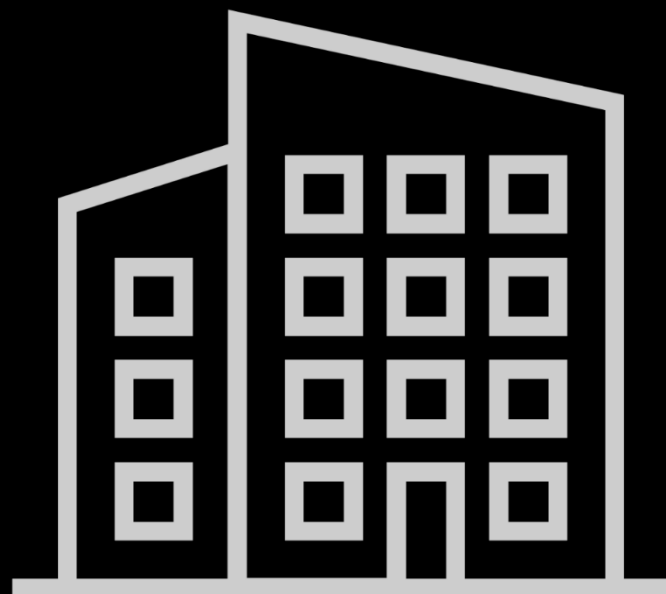






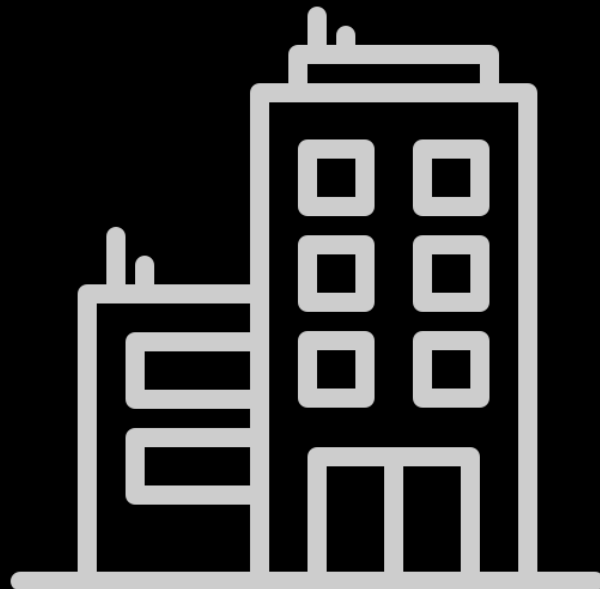
# Кейс 2 – обработчик

Кто понесет  
ответственность?



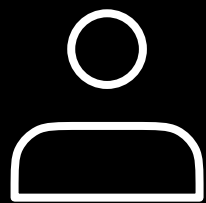
оператор

передача ПДн



лицо, действующее по  
поручению оператора

согласие



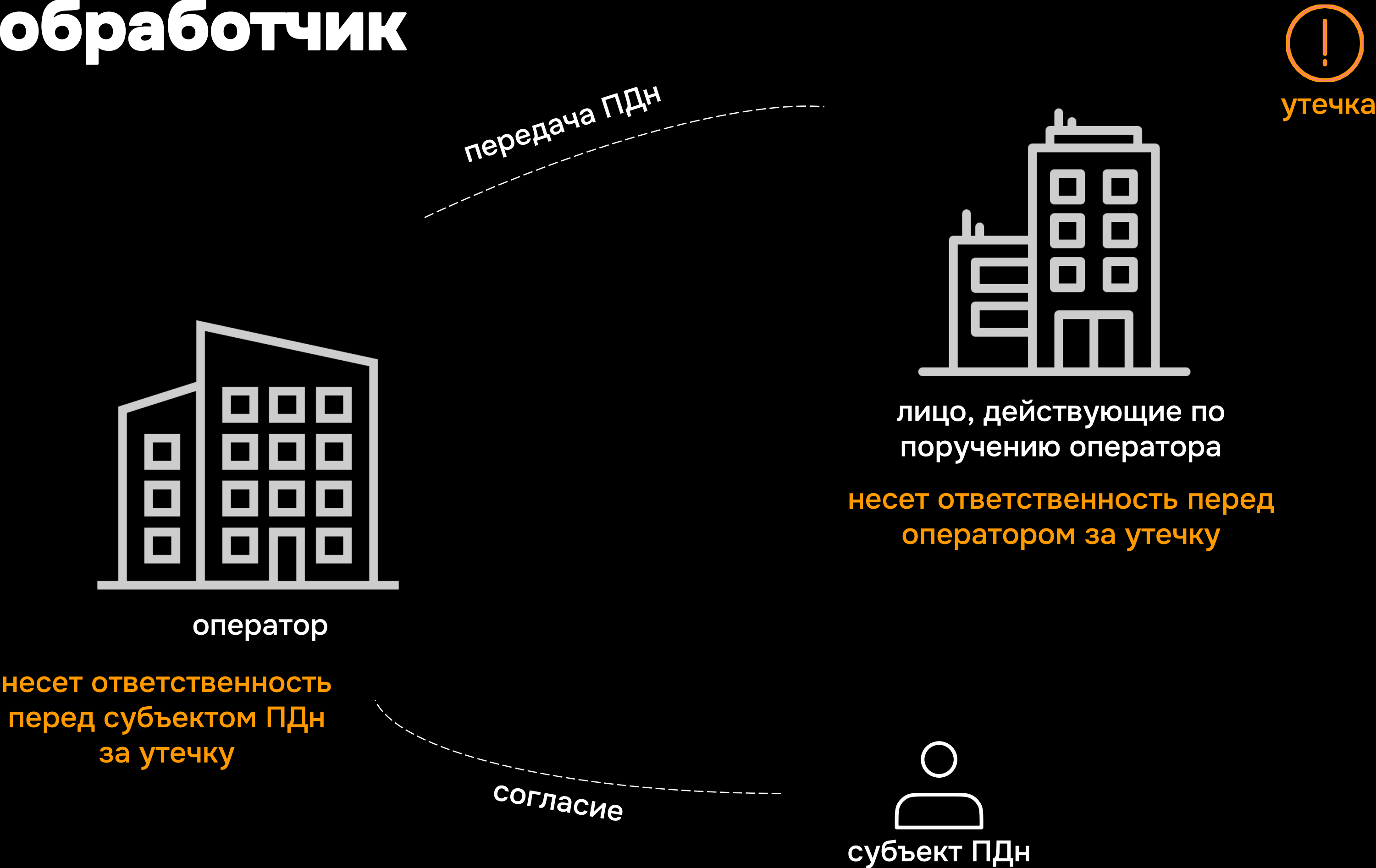
субъект ПДн



утечка



# Кейс 2 – обработчик



## Кейс 2 – обработчик. До инцидента



### Мероприятия до инцидента:

1. Проверка контрагентов на предмет соответствия требованиям по защите ПДн
2. Корректно оформленное **поручение на обработку** (оно должно содержать все нормы, которые предусмотрены для него в ст. 6 152-ФЗ: информацию об обработке и обязанности лица, обрабатывающего ПДн по поручению)
3. Наличие законных **оснований** на обработку ПДн

## Кейс 2 – обработчик. После инцидента



Мероприятия после инцидента:

- 1. Реагирование на инцидент** по результатам внутреннего расследования (направление уведомления об инцидентах, оценка вреда субъектам, расторжение договора с подрядчиком, принятие технических мер, проведение внутреннего расследования и т.д)
- 2. Митигация последствий утечки** (принятие мер по ограничению доступа к публичным дампам, мониторингу их публикаций в общедоступных источниках, усиление контроля за запросами субъектов, чьи данные были скомпрометированы)
- 3. Минимизация рисков повторения утечки** в будущем (внедрение/пересмотр принимаемых мер безопасности, пересмотр существующих договоров с 3ми лицами, повторные ознакомления работников с требованиями ЛНА, их обучение)



**ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ**

# QA-сессия





Николай

Вопрос № 1

Какая техническая информация  
считается ПДн, а какая нет?  
Например, IP-адрес?



Тимур

Вопрос № 2

Является ли учетная запись  
AD ПДн, если в ней кроме  
ФИО есть номер телефона  
и электронная почта?



Сергей

Вопрос № 3

Адрес электронной почты сам  
по себе является ПДн? Есть  
различия между личным  
и служебным адресом?





Александр

Вопрос № 4

Как Роскомнадзор узнает  
об утечках?



Елена

Вопрос № 5

Что Роскомнадзор считает  
фактом утечки?



Дмитрий

Вопрос № 6

Где посмотреть утечки?





Иван

Вопрос № 7

Может ли генеральный директор или ответственный за обработку ПДн привлечен к административной ответственности?



Дарья

Вопрос № 8

Если в организации выделено несколько ролей, ответственных за обеспечение безопасности ПДн, кто будет нести ответственность?







ЦЕНТР  
КИБЕРБЕЗОПАСНОСТИ



Филипп

Вопрос № 9

Разве штрафы всё ещё не стоят  
дешевле организации ИБ  
для ПДн?





# ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

**Александра Остапова**

[cybersec@ussc.ru](mailto:cybersec@ussc.ru)

[+7 \(343\) 379-98-34](tel:+73433799834)

[sec.ussc.ru](https://sec.ussc.ru)



[cybersec@ussc.ru](mailto:cybersec@ussc.ru)

