

Ирина Алексеенко
DPO, адвокат

РЕАГИРОВАНИЕ НА УТЕЧКИ ОТ «А» ДО «Я»

«13» октября 2026 г.



Утечка — это гонка со временем



24 ч

**Первичное
уведомление**

с момента выявления
инцидента



72 ч

**Дополнительное
уведомление**

с результатами внутреннего
расследования



3 ч

**для значимых объектов
КИИ**

срок уведомления о
компьютерном инциденте

ПЛАН

- 1** Что и кому сообщать
- 2** Какие данные указывать
- 3** Как не получить штраф
- 4** Как подготовиться

Один инцидент — две системы: Роскомнадзор и НКЦКИ

КОМПЬЮТЕРНЫЕ



Неправомерные действия, реализуемые посредством компьютерной атаки



Наличие вреда не является обязательным признаком

Сообщаем в НКЦКИ

«ИНЫЕ»



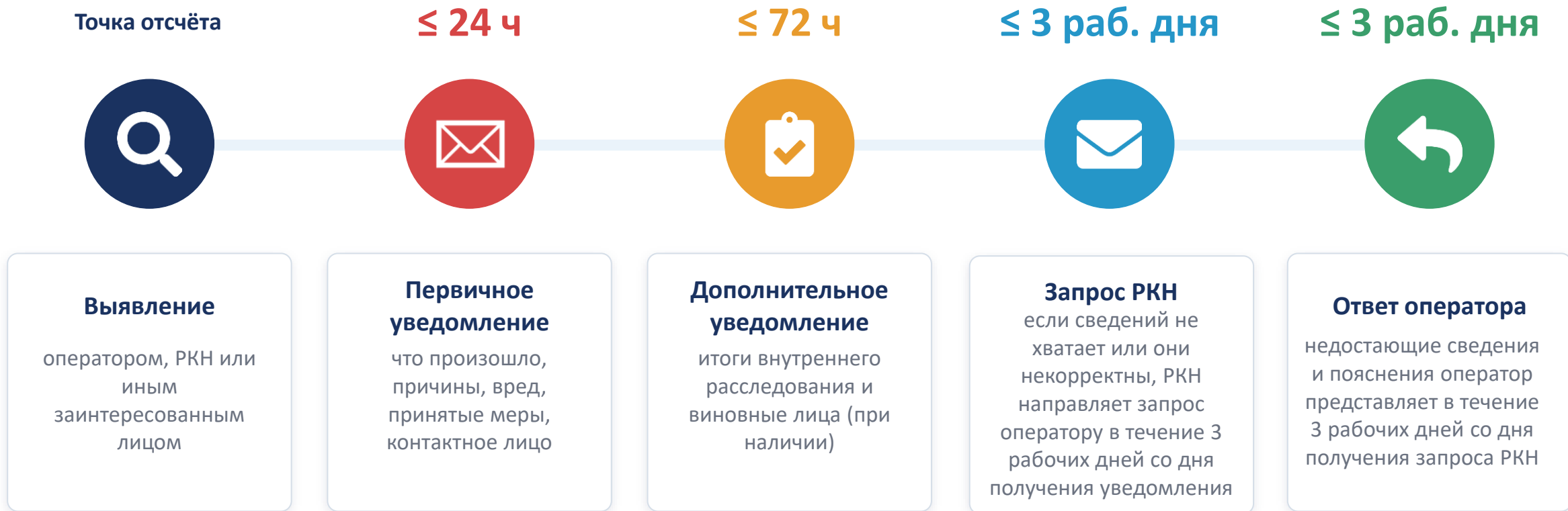
Неправомерные и случайные действия



Нарушены права субъектов и им причинён вред

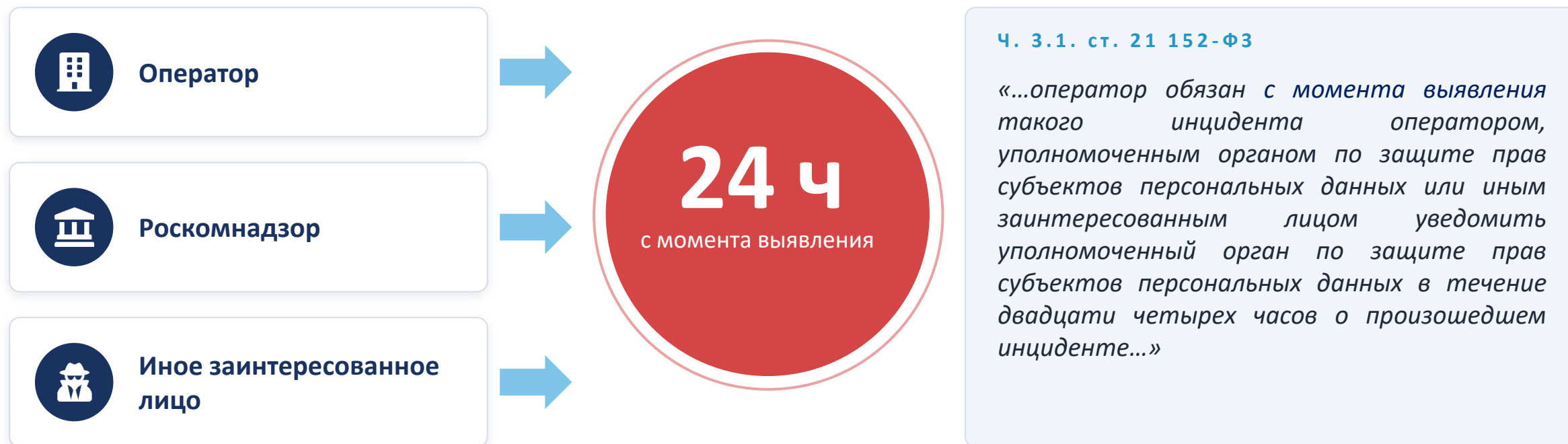
Сообщаем в Роскомнадзор

Хронология реагирования



 Не направили дополнительное уведомление — РКН направит требование, ответ на него нужно дать в течение 1 рабочего дня

Часики тикают: 24 часа - с момента выявления любым лицом



Если инцидент обнаружил Роскомнадзор: при публикации скомпрометированной базы, содержание которой указывает на её принадлежность оператору, РКН направляет требование представить уведомление

Два способа подачи уведомления

1 Документ на бумажном носителе



Адрес Роскомнадзора:
109992, г. Москва, Китайгородский пр., д. 7, стр. 2

2 Электронный документ



Портал персональных данных
Роскомнадзора

Первичное уведомление (24 ч)

Сведения об инциденте



Что произошло

дата и время выявления; содержание скомпрометированной базы и число записей (по желанию — актуальность и период сбора)



Предполагаемые причины

предварительные причины неправомерного распространения ПДн



Предполагаемый вред

предварительная оценка вреда субъектам и его последствий (п. 5 ч. 1 ст. 18.1 152-ФЗ, Приказ Роскомнадзора от 27.10.2022 №178)



Принятые меры

организационные и технические меры по устранению последствий (ст. 18.1, 19 152-ФЗ)



Контактное лицо

уполномоченное оператором на взаимодействие с РКН по инциденту

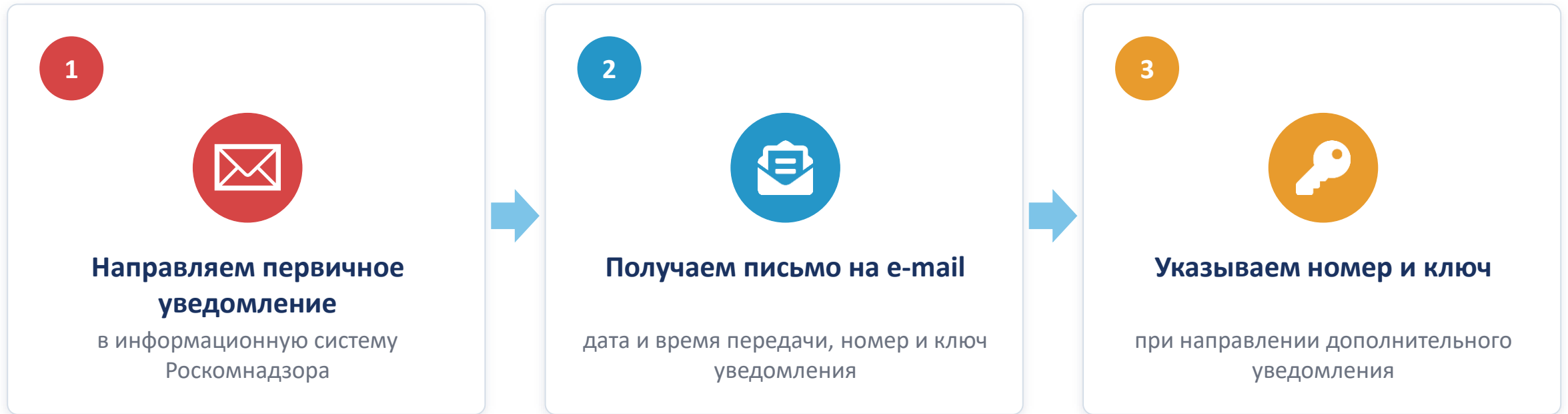
Данные оператора

- ФИО или наименование (полное и сокращённое)
- ИНН
- адрес регистрации / адрес ЮЛ
- e-mail для ответа РКН

Иные материалы

- источник информации об инциденте
- подтверждение принятых мер по устранению последствий инцидента (при наличии)

Алгоритм реализации подачи уведомлений



Сохраните номер и ключ уведомления: они понадобятся для дополнительного уведомления

Два уведомления — всегда

Если итоги расследования указали в первичном уведомлении, то дополнительное уведомление можно не направлять?

НЕТ



Оператор вправе указать итоги расследования в первичном уведомлении, если они есть на момент его направления



Это не освобождает от дополнительного уведомления в установленный законом срок



Не направили — РКН пришлёт требование представить итоги расследования; ответ — в течение 1 рабочего дня

Итоги расследования в первичном уведомлении не заменяют дополнительное уведомление

Дополнительное уведомление (72 ч)



Результаты внутреннего расследования

- причины нарушения прав субъектов и причинённый вред
- дополнительно принятые меры по устранению последствий (при наличии)
- решение о проведении внутреннего расследования с реквизитами



Лица, действия которых стали причиной (при наличии)

Работник оператора: ФИО и должность

Посторонние лица: ФИО физлица или ИП либо наименование организации; IP-адрес компьютера или устройства; предполагаемое местонахождение; иные сведения об инциденте

Ключевой признак персональных данных — возможность определить конкретного человека



Дело DLBI · А40-201075/25

«...необходимым квалифицирующим признаком ... является **способность данных, которые были опубликованы, определить конкретное лицо (субъекта персональных данных)**».

«Вместе с тем, скриншоты истца не свидетельствуют о том, что ответчик обрабатывал и публиковал данные, позволяющие определить конкретное лицо».

Проверка утечки

А наша ли база?



Утечка подтверждена

Направляем два уведомления

первичное — в течение 24 часов,
дополнительное — в течение 72
часов (ч. 3.1 ст. 21 152-ФЗ)



**База уже была
скомпрометирована**

Уведомление со ссылкой на прежнее

если характеристики базы полностью
соответствуют ранее
скомпрометированной, указываем
дату и номер ранее направленного
уведомления



Утечка не подтвердилась

Уведомление + акт расследования

если факт передачи ПДн не
подтверждён и (или) принадлежность
базы оператору не установлена — к
дополнительному уведомлению
прилагаем акт внутреннего
расследования

Помимо уведомлений: 5 шагов, которые усиливают позицию



Это не утечка: если ПДн не стали доступны третьим лицам (например, работник получил доступ вопреки ЛНА оператора), уведомлять Роскомнадзор не требуется

Компьютерные инциденты: но



Приказ ФСБ России от 13.02.2023 № 77

О порядке взаимодействия операторов с ГосСОПКА, включая информирование ФСБ России о компьютерных инцидентах с персональными данными



Регламент взаимодействия

НКЦКИ и владельцев информационных ресурсов РФ при информировании ФСБ о компьютерных инцидентах, реагировании и ликвидации последствий компьютерных атак



Методические рекомендации

по организации прямого взаимодействия с НКЦКИ



Приказ ФСБ России от 24.07.2018 № 367

Перечень информации, представляемой в ГосСОПКА, и порядок её представления

Кто обязан взаимодействовать с



Субъекты КИИ

ФЗ от 26.07.2017 № 187-ФЗ
«О безопасности критической информационной
инфраструктуры РФ»



Органы власти и стратегические организации

ФОИВ, высшие органы власти субъектов РФ, госфонды,
госкорпорации, стратегические предприятия и АО,
системообразующие организации — Указ Президента
РФ от 01.05.2022 № 250 «О дополнительных мерах по
обеспечению информационной безопасности
Российской Федерации»



Операторы персональных данных

ФЗ от 27.07.2006 № 152-ФЗ
«О персональных данных»



Провайдеры хостинга

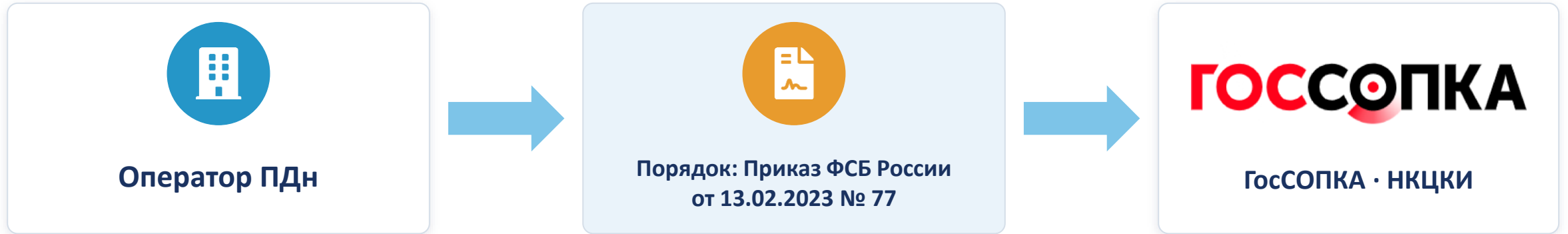
Приказ Минцифры России от 01.11.2023 № 936
"Об утверждении требований о защите информации
при предоставлении вычислительной мощности для
размещения информации в информационной системе,
постоянно подключенной к информационно-
телекоммуникационной сети "Интернет"



Иные организации

вправе взаимодействовать с
НКЦКИ добровольно

Взаимодействие с ГосСОПКА – обязанность оператора



Ч. 12 СТ. 19 152-ФЗ

Оператор обязан **обеспечивать взаимодействие с ГосСОПКА**, включая информирование о компьютерных инцидентах, повлёкших неправомерную передачу (предоставление, распространение, доступ) персональных данных — в порядке, определённом федеральным органом исполнительной власти в области обеспечения безопасности

Как уведомлять НКЦКИ



Уведомление через Роскомнадзор

«Иные» операторы

Заполняют первичное и дополнительное уведомление



РОСКОМНАДЗОР



Уведомление о факте неправомерной передачи ПДн



Уведомление о результатах внутреннего расследования



Дальше РКН передаёт информацию в НКЦКИ

Каналы связи с НКЦКИ

Субъекты КИИ / оператор подключён к ГосСОПКА



Средства автоматизированного обмена информацией на основе программного интерфейса (посредством API)



Личный кабинет субъекта ГосСОПКА в технической инфраструктуре НКЦКИ

В технической инфраструктуре НКЦКИ информации присваивается уникальный идентификатор КИ (ID)

«Иные» операторы



Электронная почта



Почтовые отправления (с электронными носителями информации) — дополнительный канал



Телефонная связь — дополнительный канал

Сотрудники НКЦКИ учитывают информацию в технической инфраструктуре, после чего передают отправителю ID

Факторы, минимизирующие ответственность



Правонарушение совершено впервые



Признание вины



Устранение нарушений



Статус МСП (ст. 4.1.2 КоАП РФ)



Признание компании потерпевшей стороной по уголовному делу



До инцидента приняты «необходимые и достаточные» технические и организационные меры (ЛНА, средства защиты информации)

3 условия одновременно

1

Расходы на ИБ — не менее 0,1 % годовой выручки

в течение трёх лет до выявления; мероприятия по обеспечению ИБ проведены лицензированными организациями или самим оператором при наличии лицензии (лицензия на деятельность по технической защите конфиденциальной информации)

2

Соблюдение требований к защите ПДн

при обработке в ИСПДн с документальным подтверждением в течение 12 месяцев до выявления нарушения

3

Отсутствие отягчающих обстоятельств

предусмотрены примечанием 5 к ст. 13.11 КоАП РФ



ШТРАФ

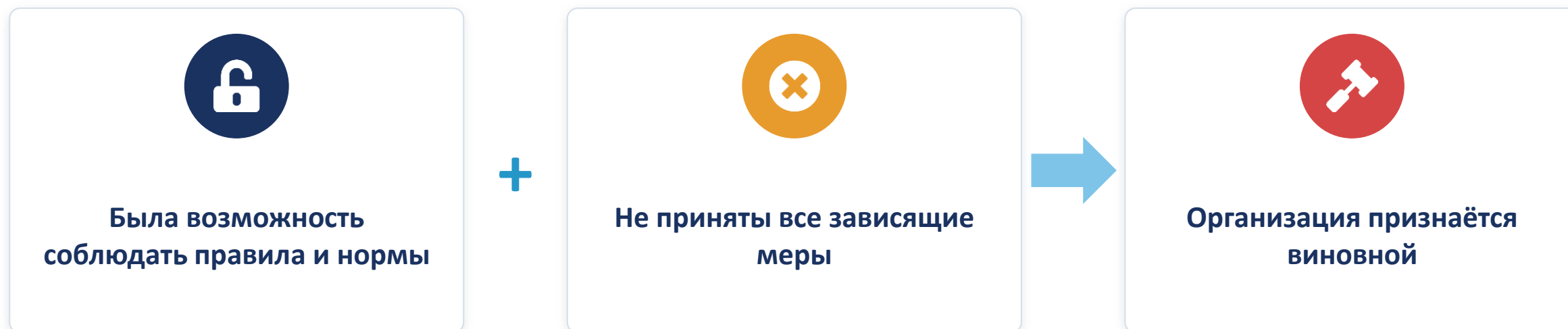
1/10

минимального размера штрафа по
статье

от 15 до 50 млн ₽

«Необходимые и достаточные меры»:

Вина организации — это упущенная возможность их принять



Юридическое лицо признается виновным в совершении административного правонарушения, если будет установлено, что у него имелась возможность для соблюдения правил и норм, за нарушение которых настоящим Кодексом или законами субъекта Российской Федерации предусмотрена административная ответственность, но данным лицом не были приняты все зависящие от него меры по их соблюдению (ч. 2 ст. 2.1. КоАП РФ).

Дело	Решение	Оценка
ОАО «РЖД» · А40-263206/2025	Отказ в привлечении	Утверждён порядок допуска к ИС, пароли ≤ 90 дней, регулярный аудит учётных записей, направлены обращение в НКЦКИ и сообщение о преступлении в ДЧ ГУМВД России, возбуждено УД
ООО ТД «АСК» · А27-27136/2025	Предупреждение	Впервые, признание вины, статус МСП, нет отягчающих обстоятельств, не повлекло причинение вреда или возникновение угрозы причинения вреда
ООО «Орион Телеком» · А19-25808/2025	Предупреждение	Пренебрежительное отношение к требованиям ИБ: некорректная конфигурация системы безопасности, использования ПО с критическими уязвимостями, неисполнения обязанности по деактивации учетных записей уволенных сотрудников и своевременной смене паролей. Суд 1 инстанции учёл статус МСП, совершение впервые, отсутствие отягчающих, принцип соразмерности административного наказания и дифференциацию публично-правовой ответственности
Yclients · А56-46276/2026	Предупреждение	Меры и невозможность их принять не доказаны Впервые
ООО «ПКР Аналитика» · А56-4733/2026	Предупреждение	Впервые
Минтруд · ВС РФ № 5-АД25-119-К2	Штраф 100 000 ₽	Не доказаны меры по ст. 18.1, 19, 22.1; инцидент подтверждён лишь после запроса
ООО «ЮКИДС» · А40-351064/25	Штраф 400 000 ₽	Штраф рассчитан по правилам для малых предприятий (ч. 2 ст. 4.1.2 КоАП)

Шаги до инцидента

- 1** Подготовить доверенность на лицо, уполномоченное на взаимодействие с Роскомнадзором
- 2** Утвердить комиссию по расследованию инцидента
- 3** Утвердить шаблоны документов: первичное уведомление; дополнительное уведомление; акт оценки вреда; решение о проведении внутреннего расследования; акт внутреннего расследования
- 4** Провести инвентаризацию ПДн: категории и количество субъектов, количество идентификаторов, качество ПДн (есть ли чувствительные ПДн), в какой ИСПДн какие ПДн
- 5** Составить карту передачи ПДн третьим лицам: кому передавали ПДн, какие обработчики получали доступ к ПДн
- 6** Аудит каналов подрядчиков, включая забытые
- 7** Собрать «тревожный чемоданчик»
- 8** Подготовить приказ о распоряжении ЭЦП на случай инцидента с персональными данными
- 9** Провести оценку вреда
- 10** Проводить на регулярной основе анализ информационных ресурсов на предмет наличия критических уязвимостей
- 11** Организовать резервное копирование и проводить тестирование восстановления из резервных копий

«Тревожный чемоданчик»: состав

Собрать в бумажном и электронном виде копии документов, подтверждающих исполнение обязанностей и принятие предусмотренных законом мер:

1



Информация о DPO — приказ или договор

2



ЛНА об обработке ПДн: политики и регламенты (в т. ч. о реагировании на инциденты) с листами ознакомления

3



Приказ об определении правил доступа к ПДн

4



Перечень ИСПДн

5



Список мер по обеспечению безопасности ПДн согласно ст. 19 152-ФЗ — доказательство качества системы безопасности

6



Документы о внутреннем контроле и (или) аудите соответствия обработки ПДн

7



Акт оценки вреда

8



Документы об обучении работников

Выводы

1

Два регулятора, два уведомления

РКН: 24 часа и 72 часа; компьютерные инциденты — НКЦКИ и ГосСОПКА

2

Срок идёт с момента выявления

любым лицом: оператор, РКН или иное заинтересованное лицо

3

Меры по исполнению требований 152-ФЗ

суды оценивают меры, принятые до инцидента

4

Доказательства собираем заранее

ЛНА, журналы, аудит учётных записей, «тревожный чемоданчик»

5

Факторы, минимизирующие ответственность

впервые, признание вины, статус МСП, признание потерпевшим по УД, наличие возбуждённого УД, устранение нарушений, отсутствие отягчающих обстоятельств

Утечка не так
страшна, если Вы к
ней готовы

