DPO/CISO: Управление комплаенсом

Реагирование на утечки данных: регламент 24ч/72ч по 152-ФЗ и НКЦКИ

Раздел: DPO/CISO: Управление комплаенсом · Опубликовано 13.11.2026 · Обновлено 13.11.2026

Реагирование на утечки данных: регламент 24ч/72ч по 152-ФЗ и НКЦКИ

Порядок действий офицера безопасности и юридической службы при выявлении инцидента компрометации персональных данных: жесткие регламенты Роскомнадзора (24 часа и 72 часа), уведомление НКЦКИ и автоматическая генерация документов.

Новые требования ст. 21 Федерального закона № 152-ФЗ

Законодательство РФ устанавливает строжайшие временные рамки для операторов персональных данных с момента выявления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн:

Временной норматив	Обязательное действие	Адресат
В течение 24 часов	Направление первичного уведомления об инциденте: описание произошедшего, предполагаемые причины, предполагаемый вред, принятые меры и контакты ответственного лица.	Роскомнадзор (через портал или систему взаимодействия)
В течение 72 часов	Направление результатов внутреннего служебного расследования инцидента, а также сведений о лицах, действия которых стали причиной компрометации.	Роскомнадзор
Немедленно (до 24 часов)	Информирование о компьютерном инциденте на объекте КИИ через каналы ГосСОПКА.	НКЦКИ (ФСБ России)

Что вам понадобится

- Право доступа: Аналитик или Руководитель организации
- Раздел: Пульт DPO → Организация → Центр реагирования (Data Breach Center)
- Ориентировочное время: оперативно при инциденте

Шаг 1: Фиксация инцидента и запуск таймеров SLA

В момент обнаружения утечки или получения сообщения от ИБ-мониторинга откройте Центр реагирования и нажмите **«Зарегистрировать инцидент»**. Система зафиксирует точный timestamp инцидента и запустит **живые таймеры обратного отсчета (SLA 24ч и SLA 72ч)** с цветовой индикацией критичности дедлайна.

Шаг 2: Оценка масштаба и классификация

Укажите затронутые ИТ-системы, примерный объем скомпрометированных записей (до 1000, до 10 000, свыше 100 000) и категории данных (паспортные данные, платежные реквизиты, телефоны, пароли). Система автоматически рассчитает уровень тяжести инцидента.

Шаг 3: Назначение комиссии по расследованию

Нажмите «Сформировать комиссию». Система предложит состав (председатель комиссии, ответственный за ИБ, юрист, системный администратор) и сформирует **Приказ о создании комиссии по расследованию инцидента информационной безопасности**.

Шаг 4: Генерация первичного уведомления в РКН (24 часа)

До истечения первых суток нажмите кнопку **«Сформировать уведомление в РКН (24ч)»**. Сервис создаст официальное уведомление установленной формы, готовое к подписанию руководителем и отправке в территориальный орган Роскомнадзора.

Шаг 5: Проведение расследования и отчетность 72 часа

Комиссия фиксирует вектор атаки (фишинг, уязвимость веб-приложения, инсайдер) и принятые меры по локализации. Нажмите **«Сформировать итоговый отчет в РКН (72ч)»** и **«Акт служебного расследования»** — система сформирует закрывающий пакет юридических документов.

Результат

Организация полностью соблюдает регламенты ч. 3.1 ст. 21 152-ФЗ, исключая риски оборотных штрафов и претензий со стороны регулятора.

Совет: Всегда храните сгенерированные уведомления с отметками об отправке и квитанциями доставки в реестре инцидентов организации.

М.П.

QR Consult — 2026