DPO/CISO: Управление комплаенсом

Three-Stream Compliance: разделение потоков ИСПДн, КИИ и ГИС

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

Three-Stream Compliance: разделение потоков ИСПДн, КИИ и ГИС

Руководство по раздельному учету и независимой оценке комплаенса по трем ключевым регуляторным контурам: защита персональных данных (ИСПДн), безопасность критической информационной инфраструктуры (КИИ) и государственные информационные системы (ГИС).

Почему регуляторные потоки нельзя смешивать

В российских организациях одна и та же информационная система часто попадает сразу под несколько законодательных актов. Однако смешивание их мер в единый показатель грубо нарушает методологию комплаенса:

Регуляторный поток	Ключевой НПА и регулятор	Ответственность за нарушения	Особенность контура
ИСПДн (Персональные данные)	152-ФЗ, ПП РФ № 1119, Приказ ФСТЭК № 21 (Роскомнадзор, ФСТЭК)	Ст. 13.11 КоАП РФ (штрафы до 18 млн ₽ за повторные утечки)	Фокус на правах субъектов, согласии, локализации баз и защите конфиденциальности.
КИИ (Критическая инфраструктура)	187-ФЗ, ПП РФ № 127, Приказ ФСТЭК № 239 (ФСТЭК 8-е упр., ФСБ / НКЦКИ)	**Ст. 274.1 УК РФ** (лишение свободы на срок до 10 лет)	Фокус на непрерывности процессов, ГосСОПКА, предотвращении компьютерных инцидентов.
ГИС (Государственные ИС)	149-ФЗ, Приказ ФСТЭК № 117 от 11.04.2025 (ФСТЭК, Минцифры)	Предписания, приостановка эксплуатации, отзыв аттестата	Обязательная аттестация по требованиям безопасности, защита целостности и доступности.

Опасность «средней температуры»: Если система имеет 100% выполнения мер по ИСПДн, но 0% по КИИ, суммарная оценка 50% маскирует состав уголовного преступления по ст. 274.1 УК РФ. Архитектура Three-Stream Compliance делает каждый поток полностью автономным.

Как работает Three-Stream в Пульте DPO

1. **Поле stream в снимках комплаенса:** Каждая мера и снимок состояния привязаны к потоку (`ispdn`, `kii`, `gis`).
2. **Изолированная фильтрация мер:**
   - Меры ИСПДн (Приказ 21) фильтруются строго по рассчитанному `uz_level` (УЗ-1..4).
   - Меры КИИ (Приказ 239) фильтруются строго по категории значимости `kii_category` (1, 2, 3 категория).

    - Меры ГИС (Приказ 117) фильтруются строго по классу защищенности `gis_class` (K1, K2, K3).

3. **Автоподключение НПА:** При завершении классификации в соответствующем мастере система автоматически связывает ИТ-систему с нужным НПА и разворачивает стек мер.

Три KPI-карточки и вкладки управления

На странице «Комплаенс» ИТ-системы представлены 3 независимые карточки метрик:

- **ИСПДн (Приказ № 21):** статус уровня защиты (например, УЗ-3), процент выполнения и количество реализованных мер из применимых.
- **КИИ (Приказ № 239):** категория значимости (например, 2 категория либо «Критичность не рассчитана»), покрытие требований по эшелонам защиты.
- **ГИС (Приказ № 117):** класс защищенности (например, К2 либо «Класс не определен») и процент готовности к аттестации.

С помощью вкладок [Все меры], [ИСПДн], [КИИ], [ГИС] офицер безопасности может просматривать и настраивать применимость мер изолированно для каждого регулятора.

Секция «Контекст комплаенса» на Шаге 6

На финальном Шаге 6 паспорта системы блок «Контекст комплаенса» отображает текущее состояние всех 3 контуров. Если какой-либо контур не классифицирован, выводится аккуратный бейдж (например, «Класс не определен») и кнопка быстрого запуска соответствующего мастера.

Результат

Организация защищена от претензий всех трех регуляторов (РКН, ФСТЭК, ФСБ). При любой проверке вы мгновенно выгружаете раздельные доказательные базы без перемешивания требований.

М.П.

QR Consult — 2026