DPO/CISO: Управление комплаенсом

Расчет уровня защищенности ПДн (УЗ-1..4) по ПП РФ № 1119

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

Расчет уровня защищенности ПДн (УЗ-1..4) по ПП РФ № 1119

Пошаговое определение уровня защищенности персональных данных (УЗ-1, УЗ-2, УЗ-3, УЗ-4) при их обработке в информационных системах в соответствии с требованиями Постановления Правительства РФ № 1119 и Приказа ФСТЭК России № 21.

Основа классификации ИСПДн

Постановление Правительства РФ № 1119 устанавливает исчерпывающий математический алгоритм расчета требуемого уровня защиты на основе 4 параметров:

1. Тип актуальных угроз безопасности (1, 2 или 3 тип).
2. Категория обрабатываемых персональных данных (специальные, биометрические, общедоступные, иные).
3. Отношение субъектов к оператору (сотрудники или лица, не являющиеся сотрудниками).
4. Объем базы данных субъектов (до 100 000 субъектов или более 100 000).

Что вам понадобится

- Право доступа: Аналитик или Руководитель организации
- Раздел: Пульт DPO → ИТ-система → Шаг 1 → блок «ИСПДн»
- Ориентировочное время: 5–7 минут

Шаг 1: Определение типа актуальных угроз

В соответствии с моделью угроз определите тип угроз для вашей системы:

- **1-й тип угроз:** актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (ОС, гипервизоры).
- **2-й тип угроз:** актуальны угрозы, связанные с наличием недокументированных возможностей в прикладном программном обеспечении.
- **3-й тип угроз:** актуальны угрозы, не связанные с недокументированными возможностями в системном или прикладном ПО (наиболее распространенный случай при использовании сертифицированных СЗИ и закрытии сетевого периметра).

Шаг 2: Выбор категорий обрабатываемых персональных данных

Отметьте обрабатываемые категории ПДн:

- **Специальные категории:** расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь, судимость (ст. 10 152-ФЗ).
- **Биометрические данные:** физиологические и биологические характеристики, используемые оператором для установления личности субъекта (ст. 11 152-ФЗ).
- **Общедоступные данные:** ПДн, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта.
- **Иные категории:** стандартные персональные данные (ФИО, паспортные данные, контакты, снилс, инн, финансовые сведения).

Шаг 3: Определение круга субъектов и объема

Укажите, чьи данные обрабатываются:

- Только сотрудники организации (субъекты состоят в трудовых отношениях).
- Физические лица, не являющиеся сотрудниками (клиенты, пользователи мобильного приложения, пациенты).

Затем выберите объем: **до 100 000 субъектов** или **более 100 000 субъектов**.

Шаг 4: Итоговая матрица защищенности (УЗ-1 .. УЗ-4)

Калькулятор автоматически вычисляет нормативный уровень защищенности:

Уровень защиты	Когда назначается	Требования Приказа ФСТЭК № 21
УЗ-1	1-й тип угроз, либо спецкатегории более 100 тыс. не-сотрудников при 2-м типе	Максимальный состав мер, сертифицированные СЗИ 4-го класса и выше
УЗ-2	2-й тип угроз для большинства систем, либо спецкатегории при 3-м типе угроз	Повышенный уровень мер, строгий контроль доступа, аудит событий
УЗ-3	3-й тип угроз для иных категорий данных свыше 100 тыс. субъектов	Базовый корпоративный стандарт защиты, межсетевые экраны, антивирусная защита
УЗ-4	3-й тип угроз для общедоступных данных или до 100 тыс. сотрудников	Минимальный объем организационных и базовых технических мер

Результат

Уровень защищенности зафиксирован в паспорте системы. Фреймворк Приказа ФСТЭК России № 21 автоматически фильтрует

применимые меры именно под ваш уровень УЗ, исключая избыточные требования.

М.П.

QR Consult — 2026