

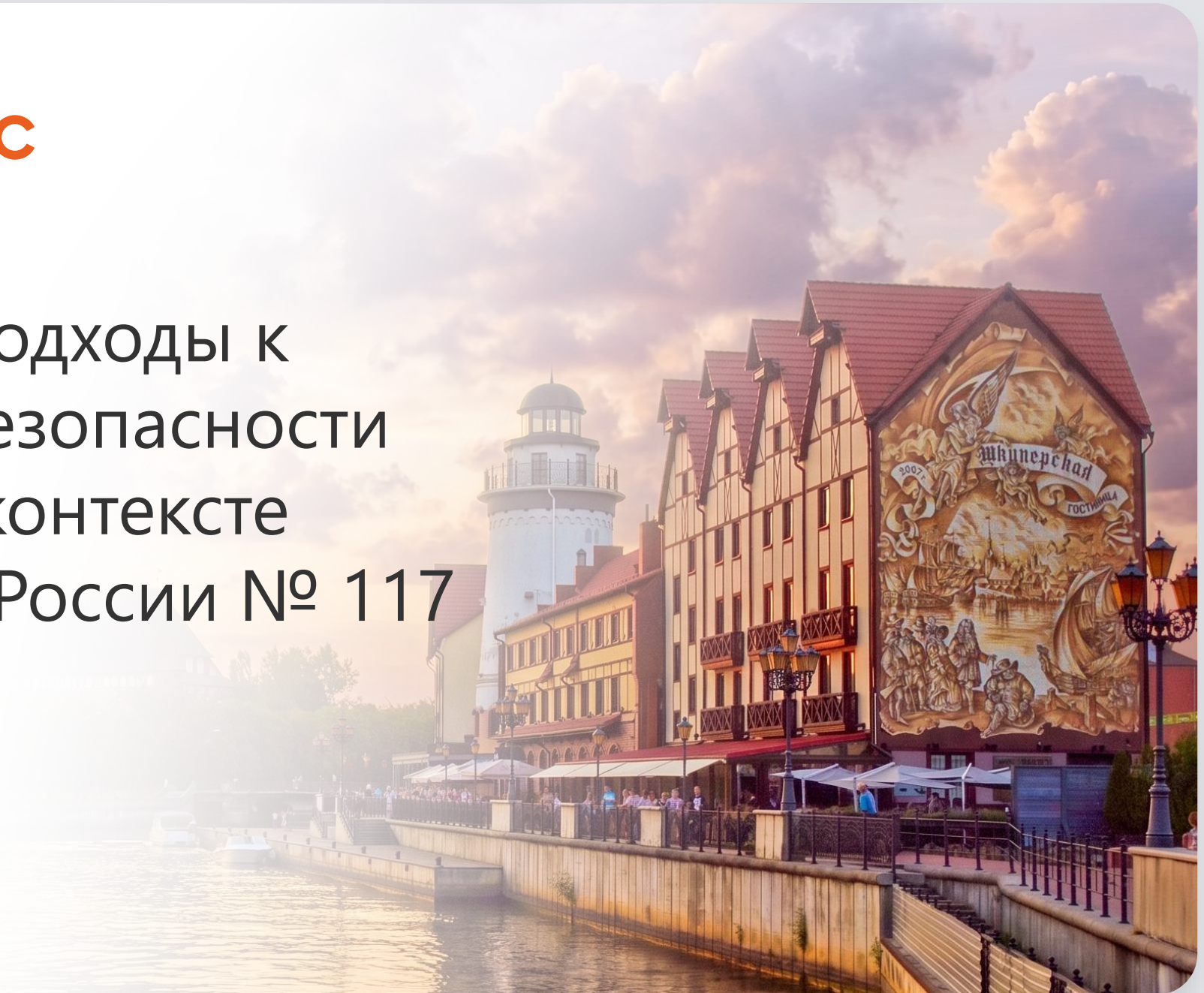


Современные подходы к обеспечению безопасности информации в контексте приказа ФСТЭК России № 117

СЕРГЕЕВ

Сергей Николаевич

Заместитель генерального директора

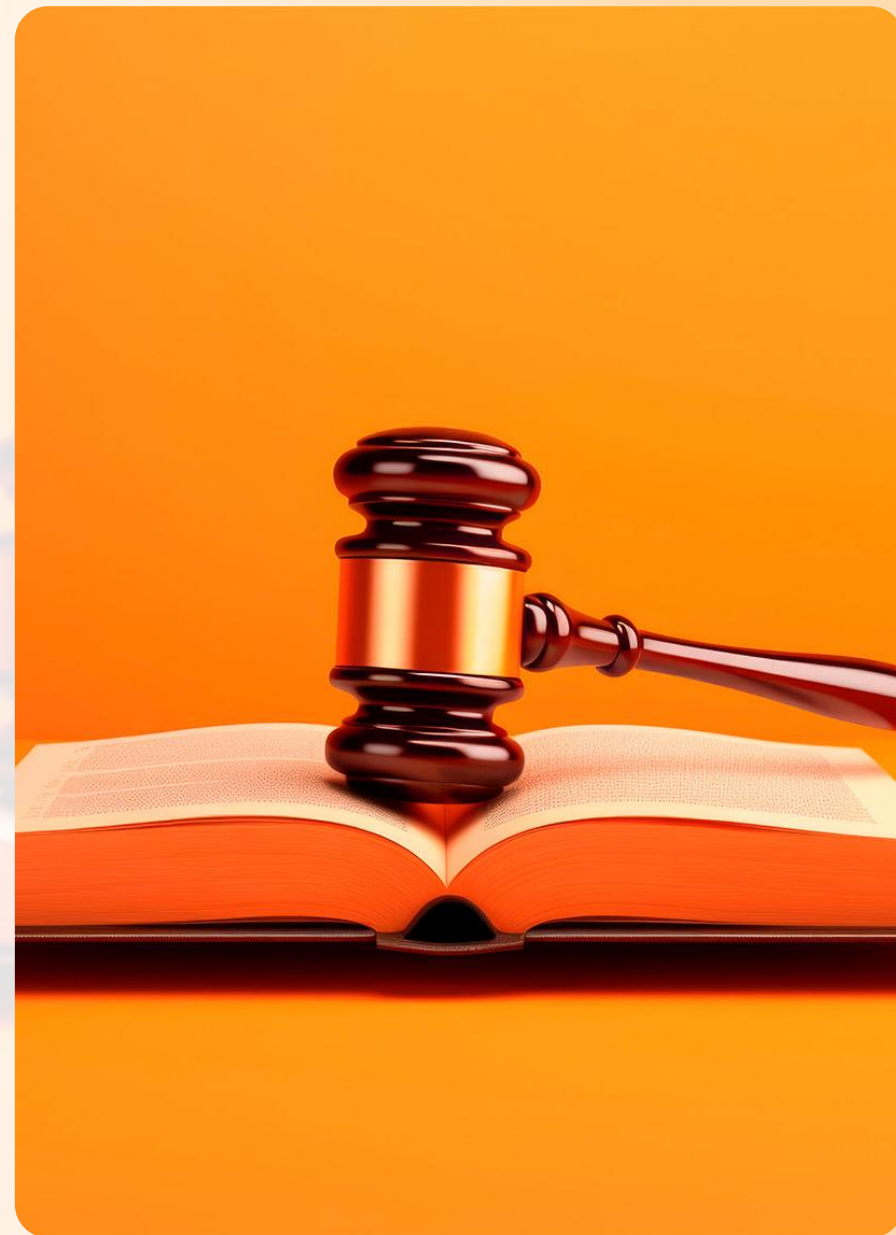


117 приказ ФСТЭК России

Основное

1. Вступил в силу 1 марта 2026 г.
2. Защите подлежат все ИС, даже если они не являются ГИС
3. Ориентирован на реальную и непрерывную защищенность
4. Методические рекомендации уже утверждены

Начинать действовать нужно было
уже вчера!



Общая проблематика



ОРД разработаны, но по 17 приказу ФСТЭК России



Нехватка имеющихся мощностей под «тяжелые» решения



Не все внутренние процессы по ИБ выстроены (управление уязвимостями и обновлениями ПО, мониторинг 24x7, взаимодействие с ГосСОПКА и т.д.)



Средства защиты информации внедрены, но без учета новых классов, требующихся 117 приказом (PAM, NGWF, EDR, SOC,...)



Штат ИБ недоукомплектован или отсутствует вовсе, на ИБ не хватает времени



Новые технологии = дополнительные усилия по обеспечению ИБ

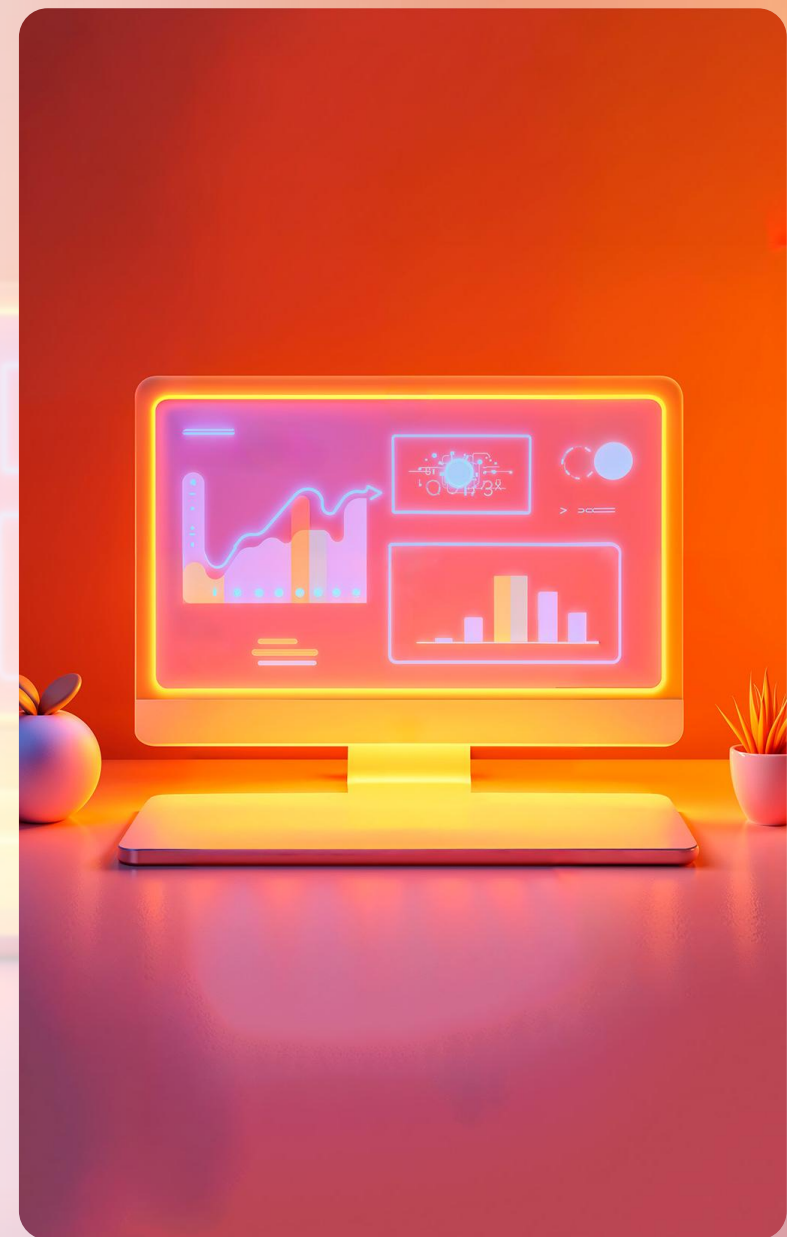
Тенденция к углубленной проработке документов

Документация по 17 приказу $\neq$ документации по 117 приказу

Строгая иерархия документов:

1. Политика защиты информации – фундамент
2. Стандарты (требования) – правила достижения целей из Политики
3. Регламенты (инструкции) – пошаговые описания процессов
4. ОРД и технические документы – матрицы доступа, назначение ответственных и т.д.

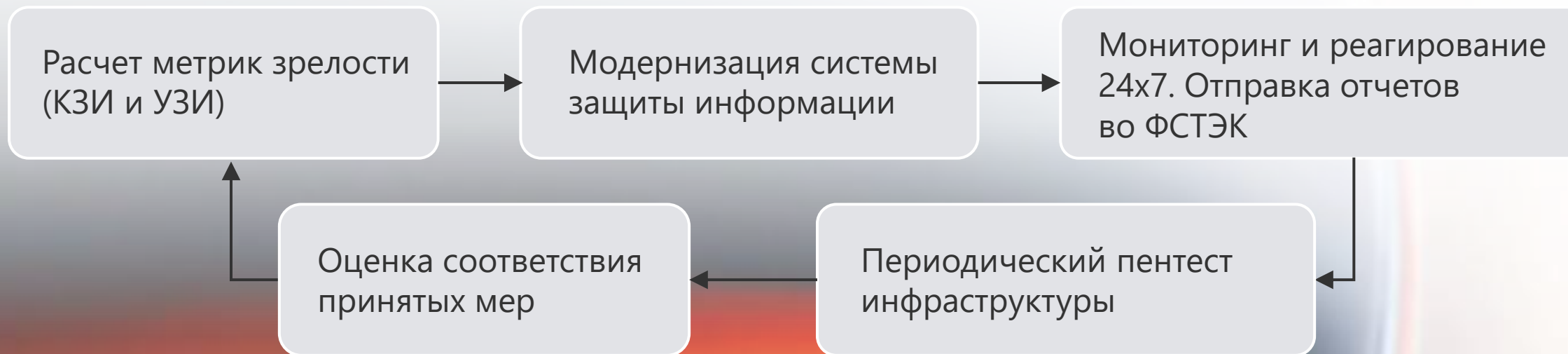
Начинать нужно с аудита бизнес-процессов и корректировки документов по новым требованиям



Непрерывные процессы вместо разовых аттестаций

Защита как циклический процесс

(PDCA – планируй, делай, проверяй, действуй)



Процесс должен быть непрерывным, оператор обязан постоянно анализировать состояние и планировать модернизацию

Практическая безопасность вместо бумажной

Регулятор смещает акцент на реальную защиту данных



Усиление защиты периметра

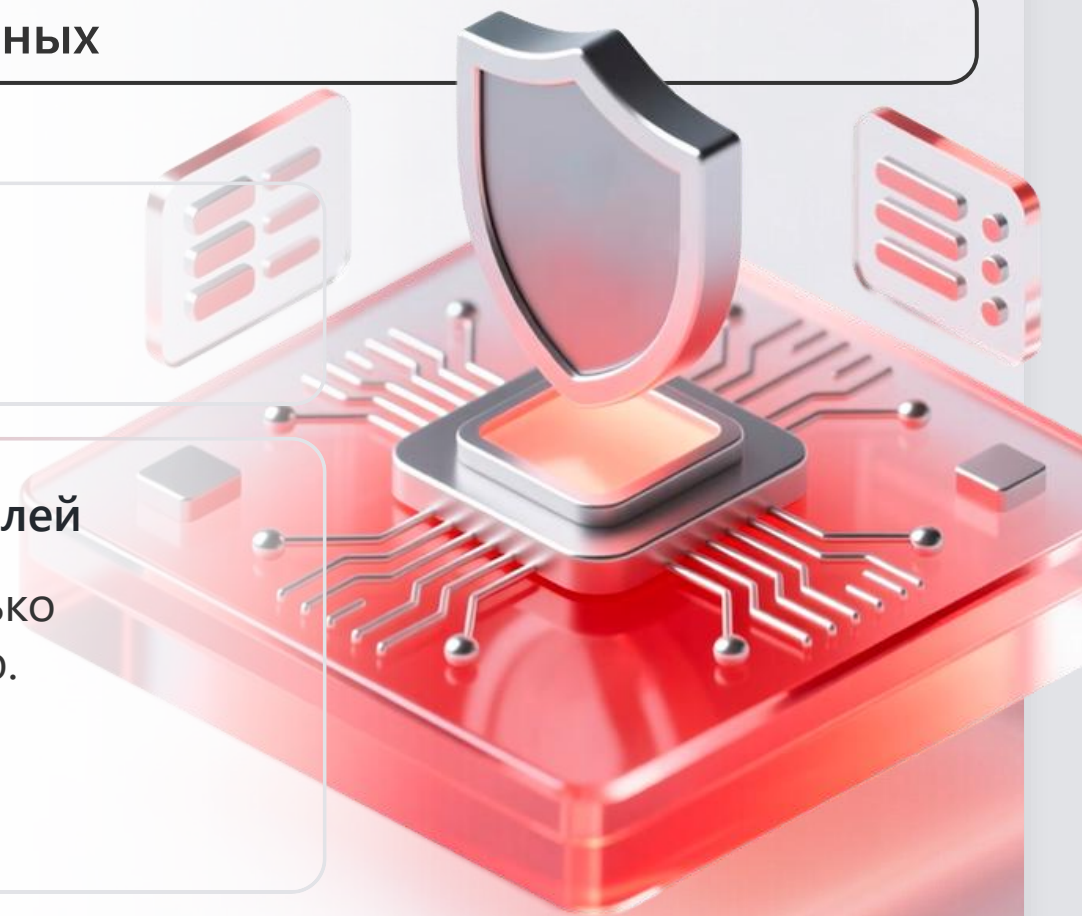
NGFW и WAF – теперь базовый минимум



Усиление механизмов идентификации пользователей

Для привилегированных пользователей доступ только через усиленную многофакторную аутентификацию.

Контроль доступа подрядчиков и фиксация всех их действий (PAM)



Практическая безопасность вместо бумажной

Регулятор смещает акцент на реальную защиту данных



Мониторинг 24x7

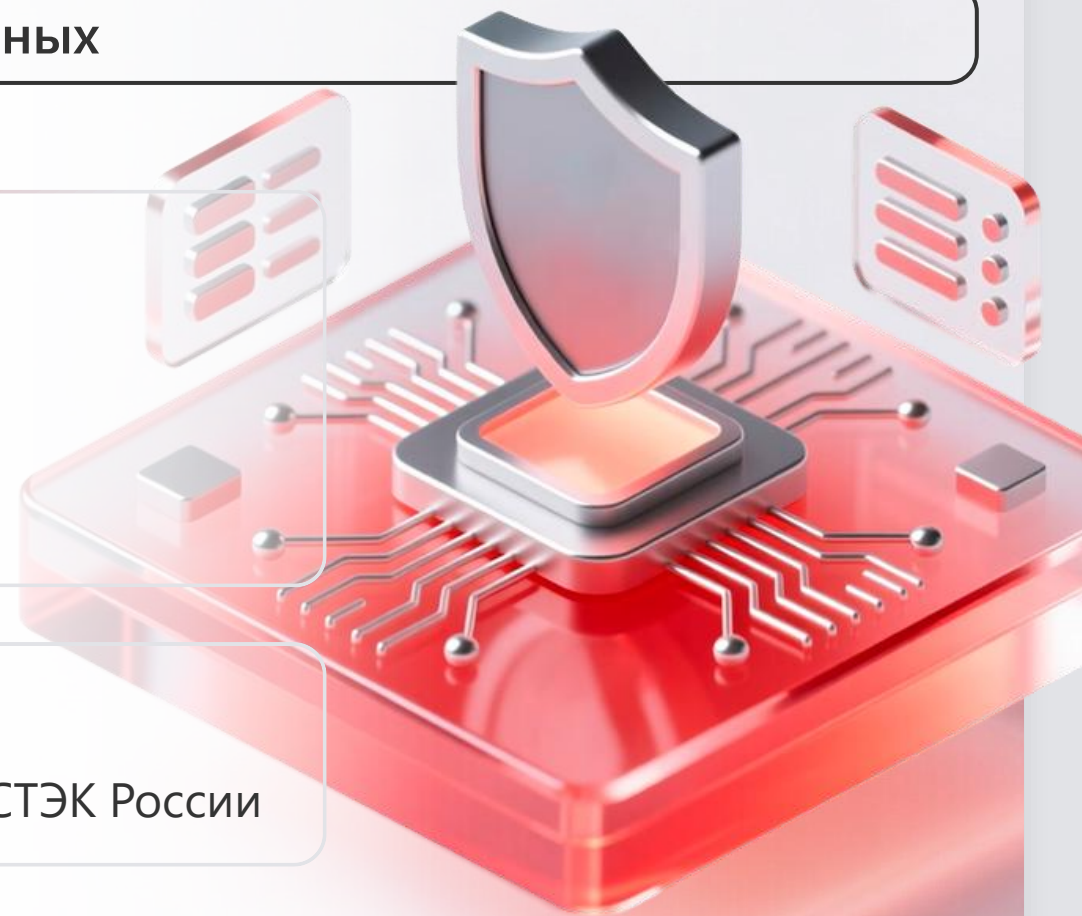
Приоритет быстрой отработки инцидентов.

Гибридная модель или сервисная – неважно, но мониторинг обязателен!



Контроль никто не отменял

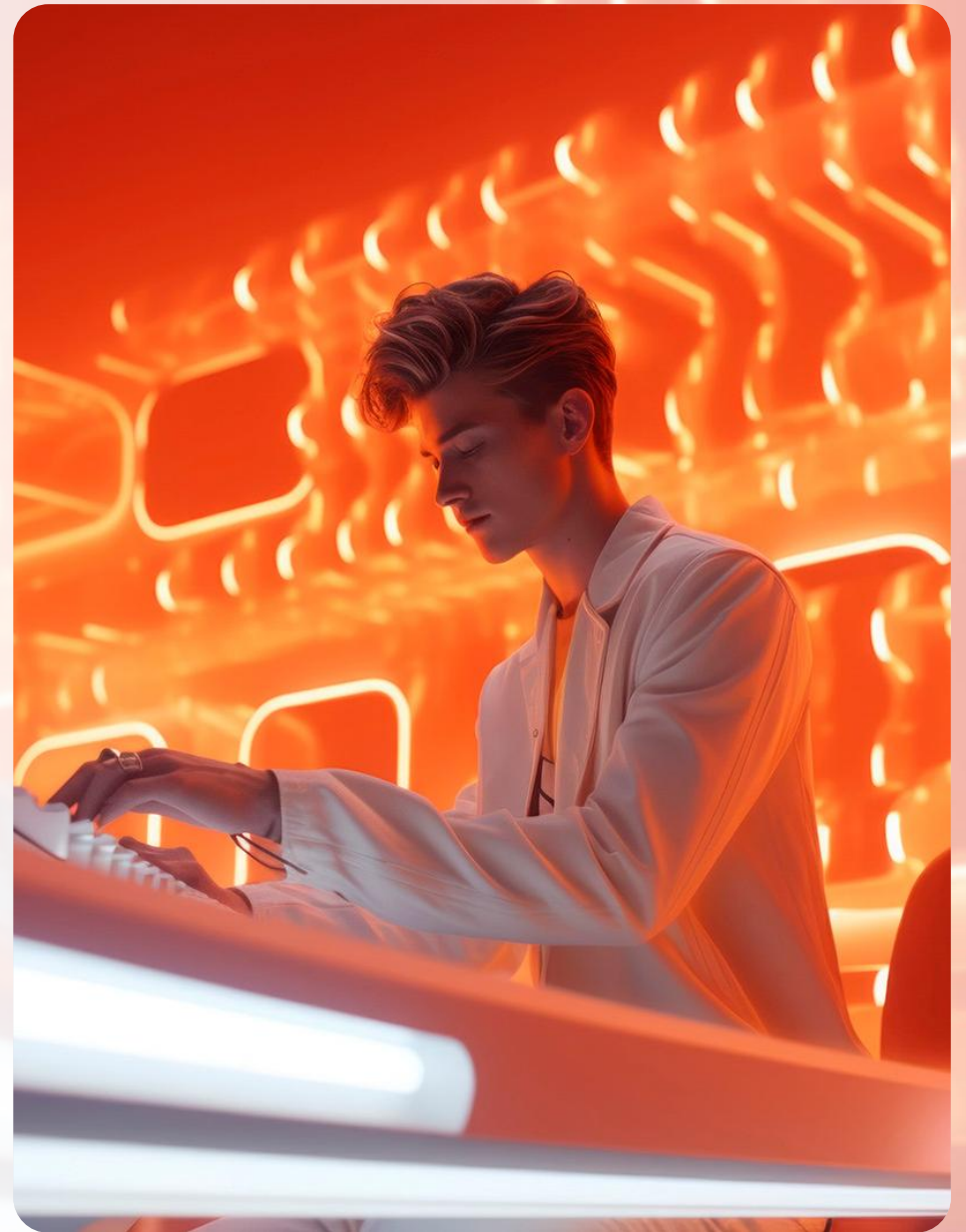
Итоговый отчет за год необходимо направить во ФСТЭК России



Безопасность невозможна без квалифицированных людей

- Не менее 30% сотрудников подразделения ИБ – с профильным образованием или переподготовкой
- Практическая подготовка: антифишинг, киберучения, лекции
- Оценка знаний пользователей

Наиболее эффективный
подход – сервисные контракты по ИБ



Оценка влияния на СКЗИ в продуктах «Кейсистемс»

Проблематика: контроль встраивания по умолчанию как процедура операторов конкретной инсталляции

Бизнес-цель: реализовать контроль встраивания на уровне разработчика

Текущий этап: консультации с испытательной лабораторией на предмет технического и регуляторного переноса контроля на уровень универсального криптомодуля

Дальнейшие шаги:

- Оценка воздействия на среду функционирования
- Заключение испытательной лаборатории

Функционирование СКЗИ должно быть штатное

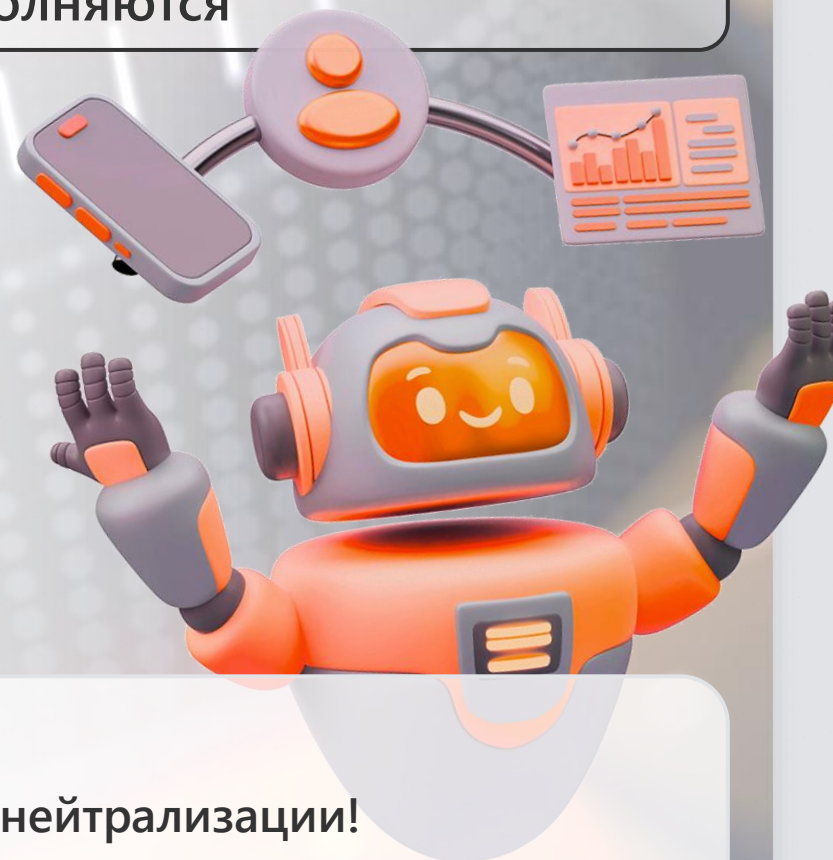
Защищать ИИ или нет?

Требования внесены в приказ ФСТЭК № 117 и постоянно дополняются

С чего необходимо начать:

- Выделенный сегмент
- «Базовый» набор СЗИ по 117 приказу (НСД, АВЗ, EDR)
- Усиленная многофакторная аутентификация к сегменту с ИИ
- Фильтрация входных и выходных данных к сегменту с ИИ (NGFW)
- Периодический анализ уязвимостей
- При размещении модели вне границ ИС – использование СКЗИ

- ❗ Контроль при выполнении значимых функций за оператором!
- ❗ Оценка угроз безопасности и включение требований в ТЗ для их нейтрализации!
- ❗ Специализированные средства защиты ИИ на подходе, но защищать нужно уже сегодня!

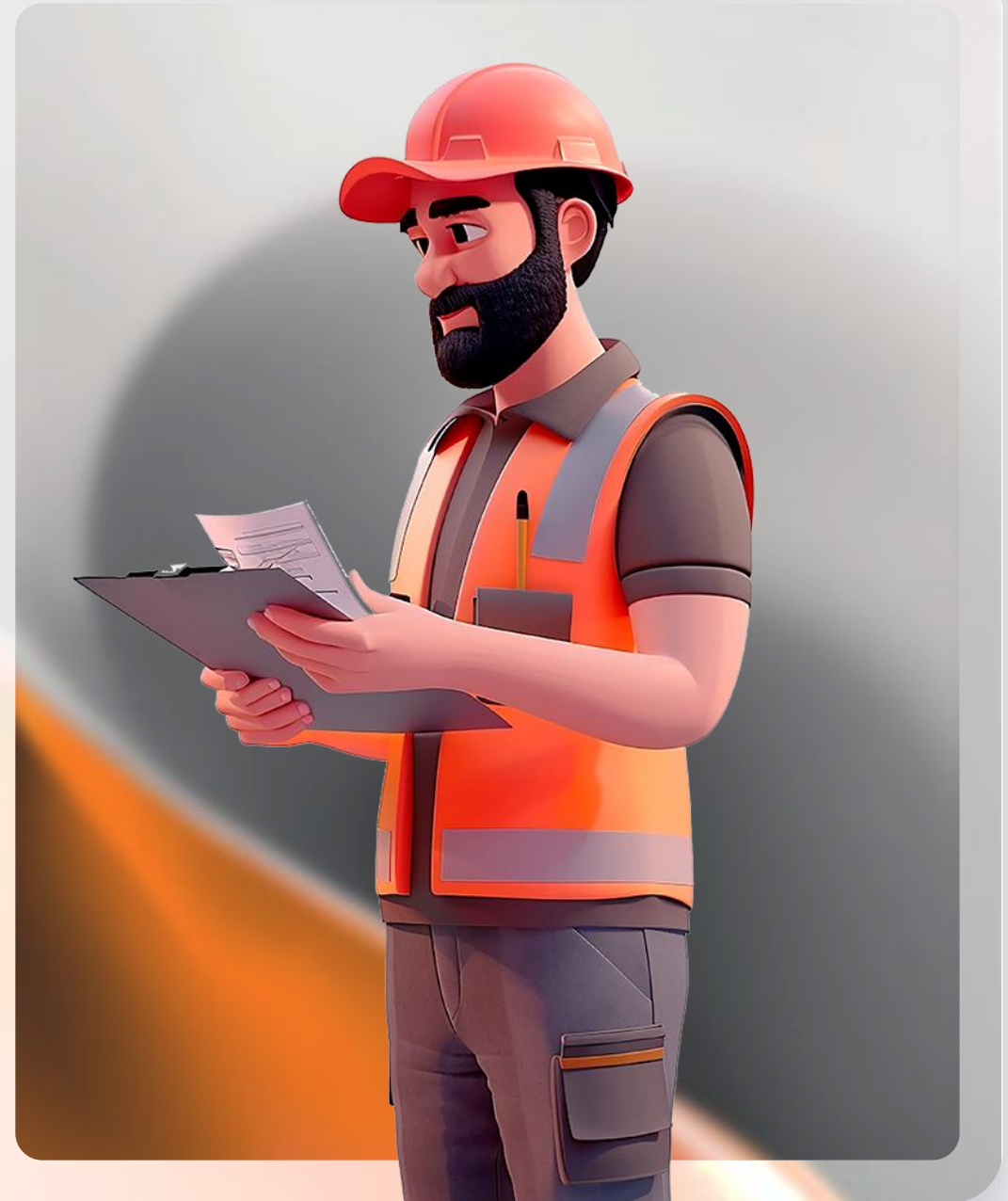


Подрядчик тоже обязан

Мероприятия при взаимодействии с подрядными организациями

- Договорная ответственность подрядчиков
- Управляемый доступ к инфраструктуре
- Выделенная защищенная ИС для подключения
- Регистрация действий подрядчиков
- Мониторинг инфраструктуры подрядчиков

❗ Поставщики подвергаются кибератакам
чаще своих клиентов



Типичные недостатки системы защиты



Отсутствие многофакторной аутентификации у админов



Критические уязвимости на периметре и внутри сети



Пароли по умолчанию у привилегированных учетных записей



Нехватка опыта противостояния современным угрозам у специалистов по ИБ



Нет мер защиты от DDoS-атак



Отсутствие SOC и регламентов реагирования

Изменения с 1 сентября 2026 г.

1. Показатель Пзи переименован на Узи
2. Оператор обязан устанавливать для подрядных организаций требования по расчету и оценке Узи
3. Удаленный доступ пользователей и доступ с мобильных устройств теперь разрешен с применением усиленной многофакторной аутентификации. До этого допускалось использовать только строгую

Изменения с 1 марта 2027 г.

1. До получения доступа к информационным системам подрядчик обязан провести оценку уровня зрелости
2. Направлять результаты оценки Узи во ФСТЭК России больше не нужно. Теперь ведомство отчитывается только о результатах оценки показателя защищенности Кзи

Способы контроля ИБ в цифрах

1. Не менее 30% работников подразделения по ЗИ должны быть обучены
2. Расчет Кзи – не реже 1 раза в 6 месяцев, Узи – не реже 1 раза в 2 года. Кзи направляется во ФСТЭК России не позднее 5 рабочих дней после дня его расчета
3. Устранять уязвимости в срок от 24 часов до 7 дней в зависимости от уровня опасности
4. При выявлении уязвимостей, которые отсутствуют в БДУ, отправлять их во ФСТЭК России не позднее 5 рабочих дней со дня их обнаружения
5. Ежегодно направлять отчет по мониторингу ИБ во ФСТЭК России
6. Интервалы восстановления инфраструктуры – от 24 часов до 4 недель, в зависимости от класса защищенности ИС
7. Не реже 1 раза в 2 года проводить проверки/тренировки по восстановлению информации из резервных копий
8. Оценка уровня знаний пользователей – не реже 1 раза в 3 года или после компьютерного инцидента
9. Контроль уровня защищенности информации в аттестованной системе должен проводиться не реже 1 раза в 3 года или после компьютерного инцидента. Результаты направляются во ФСТЭК России не позднее 5 рабочих дней после дня их получения

Не ждите плановой
проверки регулятора!



[Подробнее](#)

