ДЭКС ИНТЕГРАЦИЯ
системный интегратор

О соблюдении требований по защите информации, содержащейся в информационных системах, государственных органов и государственных учреждений в 2026 году

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Приказ ФСТЭК России №117 – что изменилось

Новые требования к защите информации в государственных и иных информационных системах

Приказ ФСТЭК России №117 от 11.04.2025 пришел на смену Приказу ФСТЭК России № 17 и вводит новые требования к защите информации

Область действия требований существенно расширена: приказ №117 распространяется не только на ГИС, но и на более широкий круг информационных систем государственных органов, учреждений и предприятий

Приказ ФСТЭК России №117 – это переход к более комплексной и современной модели защиты информации

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

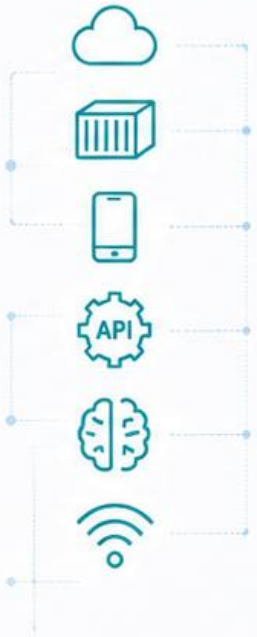
Приказ ФСТЭК России №117 – что изменилось

БЫЛО Приказ ФСТЭК России №17

- Фокус на государственных информационных системах
- Ориентация на более традиционную ИТ-инфраструктуру
- Акцент преимущественно на наборе мер защиты
- Меньше внимания постоянным процессам ИБ и современным технологиям

17 → 117

СТАЛО Приказ ФСТЭК России №117



- Расширена область действия требований
- Охватывается более широкий круг информационных систем
- Акцент на постоянно действующих процессах защиты информации
- Учитываются современные технологии: облака, контейнеризация, мобильные устройства API, ИИ, IoT
- Требования сильнее зависят от архитектуры конкретной ИС

Приказ ФСТЭК России №117 – это переход от набора отдельных мер защиты к более комплексной системе постоянно действующих процессов информационной безопасности

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Ключевые процессы защиты информации по Приказу ФСТЭК России №117

Защита информации рассматривается как система постоянно действующих процессов, а не как набор отдельных мер

Управление и конфигурации

- ВУ – Выявление и оценка угроз безопасности
- КК – Контроль конфигураций информационных систем
- КУ – Управление уязвимостями
- КО – Управление обновлениями

Доступ и устройства

- ЗУ – Обеспечение защиты информации при использовании конечных устройств
- МУ – Обеспечение защиты при применении мобильных устройств
- УД – Обеспечение защиты информации при удаленном доступе пользователей к информационным системам
- БД – обеспечение защиты информации при беспроводном доступе к информационным системам
- ПД – Обеспечение защиты информации при предоставлении пользователям привилегированного доступа

Мониторинг и контроль

- МБ – Обеспечение мониторинга информационной безопасности
- ПК – Проведение периодического контроля уровня защищенности информации, содержащейся в информационной системе
- ОО – Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании

От отдельных мер – к постоянно действующей системе процессов информационной безопасности

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Ключевые процессы защиты информации по Приказу ФСТЭК России №117

Защита информации рассматривается как система постоянно действующих процессов, а не как набор отдельных мер

Защита инфраструктуры и данных

- ОД – Обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа
- ФЗ – Обеспечение физической защиты информационных систем
- НФ – Обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций

Разработка и технологии

- БР – Обеспечение разработки безопасного программного обеспечения
- ИИ – Обеспечение защиты информации при использовании искусственного интеллекта

Люди и взаимодействие

- УЗ – Повышение уровня знаний и информированности пользователей по вопросам защиты информации
- ЗП – Обеспечение защиты информации при взаимодействии с подрядными организациями

От отдельных мер – к постоянно действующей системе процессов информационной безопасности

Основные меры защиты информации по Приказу ФСТЭК России №117

Доступ

ИАФ — Идентификация и аутентификация

УПД — Управление доступом

Платформы

ЗСВ — Защита виртуализации и облачных вычислений

ЗКО — Защита технологий контейнерных сред и их оркестрации

Приложения и сервисы

ЗЭП — Защита сервисов электронной почты

ЗВТ — Защита веб-технологий

ЗПИ — Защита программных интерфейсов взаимодействия приложений (API)

Устройства

ЗКУ — Защита конечных устройств

ЗМУ — Защита мобильных устройств

Эти меры формируют базовый контур защиты

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Основные меры защиты информации по Приказу ФСТЭК России №117

Мониторинг и обнаружение

РСБ	Регистрация событий безопасности
АВЗ	Антивирусная защита
СОВ	Обнаружение и предотвращение вторжений на сетевом уровне
ЗОО	Защита от компьютерных атак, направленных на отказ в обслуживании

Сеть и коммуникации

МСЭ	Сегментация и межсетевое экранирование
ЗКС	Защита каналов связи и сетевого взаимодействия
ЗБД	Защита точек беспроводного доступа
ЗИВ	Защита технологий «Интернета вещей»

Эти меры формируют базовый контур защиты

Современные технологии в требованиях Приказа ФСТЭК России №117

Приказ №117 учитывает технологии, которые стали стандартной частью современной ИТ-инфраструктуры и новых технологических сред

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

От чего зависит набор требований

Конкретный набор процессов и мер определяется особенностями ИС

01 Архитектура и технологический стек
- Компоненты и сегменты
- Внешние взаимодействия
- Используемые технологии

02 Информационные потоки
- Как данные обрабатываются
- Где хранятся
- Куда передаются

03 Обрабатываемая информация
- Категории и чувствительность данных
- Критичность для процессов
- Последствия нарушения безопасности

04 Актуальные угрозы
- Сценарии атак
- Уязвимые компоненты
- Возможные последствия

Определение применимых требований Приказа №117

На основе анализа особенностей информационной системы

→ **Требования к защите**

Определяются применимые требования Приказа №117 для конкретной ИС

→ **Меры защиты**

Выбираются необходимые организационные и технические меры

→ **Реализация**

Определяются средства, технологии и способы выполнения выбранных мер

Сначала анализ информационной системы – затем определение требований, выбор мер и способов их реализации

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Что необходимо сделать организации

Переход к требованиям Приказа №117 – это последовательная работа

01 Анализ и проектирование

- Аудит имеющихся информационных систем
- Оценка уровня защищенности
- Определение применимых процессов и мер
- Выявление недостающих средств защиты

02 Подготовка и реализация

- Актуализация организационной и технической документации
- Формирование требований к системе защиты информации
- Подбор необходимых технических решений
- Закупка, настройка и интеграция средств защиты информации

03 Эксплуатация и контроль

- Организация постоянно-действующих процессов информационной безопасности
- Проведение мониторинга
- Управление уязвимостями и обновлениями
- Обучение сотрудников
- Проведение периодического контроля защищенности
- Сопровождение и актуализация системы защиты

Соответствие Приказу ФСТЭК России №117 – это не разовая установка средств защиты, а построение постоянной действующей системы защиты информации

Начинать следует с аудита информационной системы и определения применимости требований

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Приказ ФСБ России №117 – что изменилось

Новые требования к защите информации с использованием средств криптографической защиты информации

Приказ ФСБ России №117 от 18.03.2025

- Устанавливает требования к защите информации с использованием СКЗИ
- Пришел на смену приказу ФСБ России №524 от 24.10.2022
- Вступил в силу 6 апреля 2025 года

Приказ ФСБ России №117 актуализировал требования, к применению средств криптографической защиты информации и расширил круг информационных систем, для которых необходимо учитывать требования ФСБ

Главное изменение – не создание новой системы криптографической защиты, а расширение сферы применений и уточнение порядкам использования СКЗИ

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Приказ ФСБ России №117 – расширил область применения требований

Новые требования к защите информации с использованием средств криптографической защиты информации

БЫЛО

Государственные информационные системы (ГИС)

Требования к применению СКЗИ были ориентированы прежде всего на ГИС

№524 → №117

СТАЛО

ГИС | ИС госорганов | ИС госучереждений | ИС ГУП

Требования распространяются также на информационные системы государственных органов, государственных учреждений и государственных унитарных предприятий

Основное изменение – требования по применению СКЗИ охватывают более широкий круг информационных систем

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Когда необходимо применять СКЗИ?

Требование НПА

- Необходимость криптографической защиты прямо установлена нормативными требованиями

Передача информации

- Информация передается за пределы контролируемой зоны

СКЗИ

Защита носителей

- Невозможно исключить несанкционированный доступ к носителям другими средствами

Электронная подпись

- Требуется использование электронной подписи и признание электронных документов равнозначными бумажным

СКЗИ применяются там, где криптографическая защита необходима для обеспечения установленного уровня безопасности информации

ДЭКС ИНТЕГРАЦИЯ
системный интегратор

Применений СКЗИ должно быть обосновано

Актуальные угрозы
Угрозы определяют необходимость криптографической защиты информации

01 Модель угроз

- Определяется, какие угрозы актуальны для информационной системы
- Оцениваются возможные сценарии нарушения безопасности
- Обосновывается необходимость криптографической защиты

02 Техническое задание

- Фиксируются требования к защите информации
- Определяется необходимость применения СКЗИ
- Задаются требования к реализуемым мерам защиты

03 Технический проект

- Отражается выбранный способ реализации криптографической защиты
- Определяется место СКЗИ в архитектуре системы
- Учитываются условия эксплуатации и взаимодействия с другими компонентами ИС