КСБ-СОФТ

117 приказ ФСТЭК РФ: от «бумажной» безопасности к непрерывной и практической защите. Новые реалии ИБ

Спикеры:

- **Екатерина Викторова** – заместитель начальника отдела аудита информационных систем
- **Александр Кочетков** – начальник отдела внедрения
- **Александр Кирий** – руководитель центра мониторинга SOCRAT

Модератор:

- **Евгений Хохлов** – продуктовый маркетолог

Обменивайтесь сообщениями во вкладке «Чат»

Запись вебинара направим всем участникам на указанный при регистрации e-mail

Задавайте вопросы во вкладке «Вопросы»

Канал в MAX «Мнение Интегратора»

Темы для обсуждения

- Новые требования и новые организации, подпадающие под действие приказа.
- Что делать с системами, аттестованными по-старому (17 приказу)?
- Какие СЗИ теперь обязательны?
- Мониторинг ИБ – необходимость.
- Просто новые меры или новый подход? Разберемся…

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Канал в MAX
«Мнение Интегратора»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

6000+
реализованных проектов

Портфолио КСБ-СОФТ

Новые ИС, попадающие под действие 117 приказа ФСТЭК России:

- ИС ГО, ГУ, ГУП*
- ЦОДы с размещением ИС ГО, ГУ, ГУП

а также:

- ИС подрядчиков (разработчиков и интеграторов)
- ИС организаций, получающих информацию из ГИС

* Определения в НПА:
ст. 123 ГК РФ
ст. 6 БК РФ
ст. 9.2 7-ФЗ «О некоммерческих организациях»
ч.1 ст. 2 174-ФЗ «Об автономных учреждениях»

Вопросы от участников:

*1. Просим разъяснить правовое и практическое содержание понятия «**иные информационные системы**» в контексте деятельности органов власти и организаций?*

*2. Какие критерии отнесения информационной системы к категории «**иная**»?*

*3. Объектами информационной инфраструктуры (не включая ГИС, объекты КИИ) в органах государственной власти и организаций часто являются такие ИС как «1С:Бухгалтерия», «1С: Зарплата и кадры», локальная вычислительная сеть, АРМ сотрудника и т.д.. Приведите развернутый пример отнесения к «**иным информационным системам**» конкретного объекта информационной инфраструктуры.*

*4. На каких **субъектов КИИ** распространяется 117 приказ ФСТЭК России?*

*5. Какая **административная ответственность** имеется за невыполнение требований приказа?*

Повышение административной ответственности за нарушение требований по технической защите информации (104-ФЗ от 23.05.2025)

Статья 13.12 КоАП РФ	Предыдущая редакция	Действующая редакция
Часть 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)	граждане – от 1,5 до 2,5 тыс. р. должностные лица – от 2,5 до 3 тыс. р. юридические лица – от 20 до 25 тыс. р.	граждане – **от 5 до 10 тыс. р.** должностные лица – **от 10 до 50 тыс. р.** юридические лица – **от 50 до 100 тыс. р.**
Часть 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну	должностные лица – от 3 до 4 тыс. р. юридические лица – от 20 до 30 тыс. р.	должностные лица – **от 20 до 50 тыс. р.** юридические лица – **от 50 до 100 тыс. р.**
Часть 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	граждане – 0,5 до 1 тыс. р. должностные лица – от 1 до 2 тыс. р. юридические лица – от 10 до 15 тыс. р.	граждане – **от 5 до 10 тыс. р.** должностные лица – **от 10 до 50 тыс. р.** юридические лица – **от 50 до 100 тыс. р.**
Часть 7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	граждане – от 1 до 2 тыс. р. должностные лица – от 3 до 4 тыс. р. юридические лица – от 15 до 20 тыс. р.	граждане – **от 10 до 20 тыс. р.** должностные лица – **от 20 до 50 тыс. р.** юридические лица – **от 50 до 100 тыс. р.**

Увеличен установленный ч. 1 ст. 4.5 КоАП РФ **срок давности** привлечения к ответственности за административные правонарушения, предусмотренные ст. 13.12 КоАП РФ, **до 1 года.**

В чем заключается ключевое отличие между 117 приказом ФСТЭК России и его предыдущей версией?

Изменение подхода

Переход от разовой организации защиты к процессу непрерывной безопасности

Новый приказ ФСТЭК предусматривает:

- Выявление и оценка угроз Кзи (1 раз в 6 мес.), Пзи (1 раз в 2 года)
- Управление уязвимостями (устранение в течение 24 ч. для критичного уровня) и управление обновлениями
- Непрерывный мониторинг ИБ и взаимодействие с ГосСОПКА
- Процессы ГОСТ Р 59547-2021. Мониторинг ИБ
- Процессы РБПО, в том числе ГОСТ 56939-2024
- Обеспечение непрерывности функционирования ИС (24 ч. на восстановление для ИС К1)
- Повышение уровня знаний (оценка 1 раз в 3 года либо после КИ)
- Контроль уровня защищенности (1 раз в 3 года либо после КИ)

Документов по ИБ стало больше

- Тенденция к **углубленной** проработке документов
- Количество документов **выросло на 25%**
- На разработку новых документов – **330 чел/ч** (2 мес.)*
- **Планы**

* Согласно проекту Типовых межотраслевых норм труда (норм времени) на работы по обеспечению защиты информации, разработанному Минтрудом России совместно с Минцифры России, ФСТЭК России и ФСБ России

Базовый комплект документов:

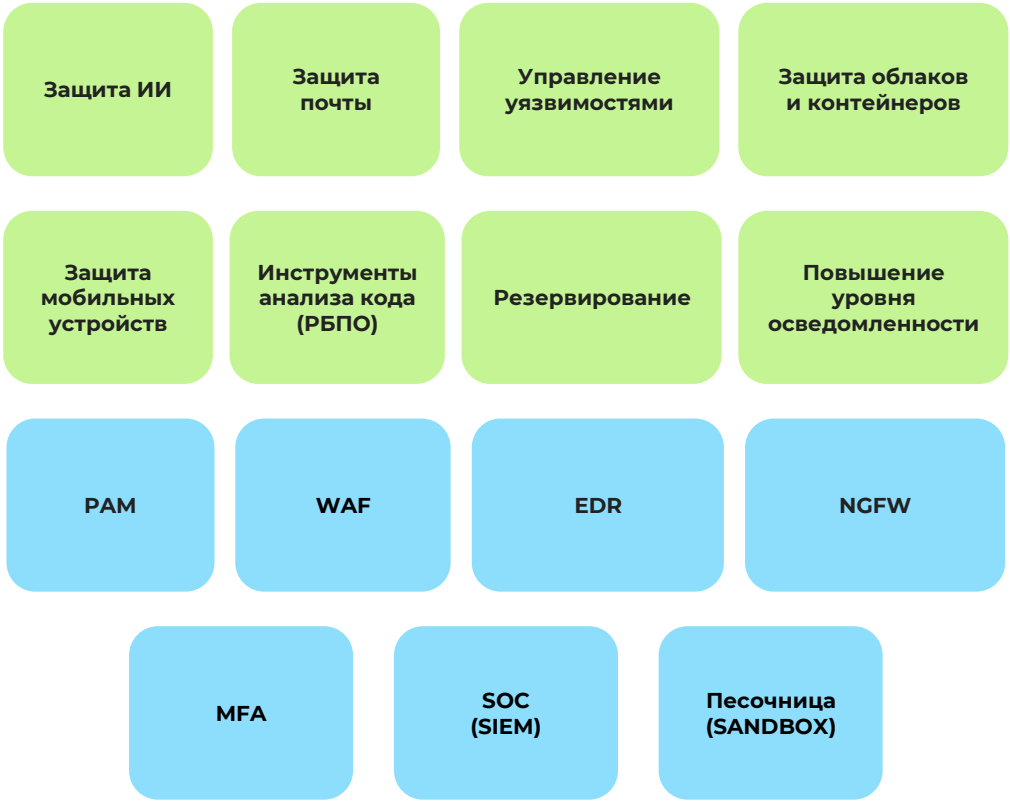
1. Политика защиты информации
2. Внутренние стандарты
3. Внутренние регламенты
4. Иные ОРД, технические документы о реализации процессов, решений
5. Эксплуатационная документация

Периодические взаимодействия с регуляторами:

- Последний в году, либо годовой отчет по **мониторингу**;
- Отчет в течение 5 р. д. по результатам **контроля уровня защищенности**
- В течение 5 р. д. показатель **Кзи и Пзи**
- Информирование НКЦКИ о выявленных **КА** и **КИ** (карточки)

Средств защиты стало больше

- Количество новых классов СЗИ ~ x2
- Сложность внедрения и сопровождения СЗИ ~ x3



Нужно ли переаттестовываться по новым требованиям при наличии действующего аттестата соответствия?

Выданные аттестаты ГИС считаются действительными после вступления в силу приказа № 117

- При модернизации ИС с повышение класса защищенности – переаттестация.
- Время на модернизацию системы защиты под новые требования – до даты проведения следующего периодического контроля
- Периодичность контроля не реже 1 раза в 3 года (поправки в Приказ ФСТЭК № 77)

Вопросы от участников:

«Что делать если на сегодня есть действующий контракт на аттестацию и система защиты спроектирована и внедряется по требованиям приказа № 17?»

«Контроль уровня защиты информации аттестованного по 17 приказу объекта информатизации делается по 17 приказу или уже по 117 приказу?»

Новые механизмы контроля: Кзи, Пзи

Кзи – до августа 2026 г.
Пзи – до марта 2028 г.

Кзи

- чем **раньше оценка**, тем больше времени на модернизацию СЗИ
- если при вторичной оценке частный показатель = 0, то вся группа показателей = 0
- результаты оценки Кзи и подтверждающие материалы направляются в ФСТЭК России
- Методика утверждена 11.11.2025

Статистика ФСТЭК, основные недостатки после оценки:

- отсутствие многофакторной аутентификации привилегированных пользователей
- наличие не устраненных критических уязвимостей на периметре и внутри информационной инфраструктуры
- наличие установленных по умолчанию паролей учетных записей привилегированных пользователей
- отсутствие мониторинга событий безопасности и реагирования на них
- непринятие мер по защите от распределенных атак, направленных на приведение систем в состояние «отказ в обслуживании»

Пзи

- достаточность и эффективность проведения мероприятий по защите информации

Новые механизмы контроля: Кзи, Пзи

Кзи – до августа 2026 г.
Пзи – до марта 2028 г.

Вопросы от участников

1. Орган власти является владельцем систем, а технически (обслуживание серверов, все привилегированные учетки) защищает оператор (другое ЮЛ), без оператора даже посчитать Кзи нельзя (некоторые пункты без них не посчитать), документы должны быть разработаны владельцем все-таки?

2. В случае, если владелец ГИС назначил оператором другое юридическое лицо, но в Положении и приказе о назначении оператора функции по обеспечению защиты информации не возложены, то кто отвечает за формирование КЗИ и в целом за реализацию требований 117?

3. Показатель рассчитывается для каждой ИС?

Новые механизмы контроля: Кзи, Пзи

Кзи – до августа 2026 г.
Пзи – до марта 2028 г.

Времени на модернизацию системы защиты информации не так много, как кажется

- Внедрение тяжелых решений – длительный и ресурсозатратный процесс
- Правильно подобранное решение – залог успеха

Для закрытия основных недостатков при оценке Кзи:

Проводить периодический анализ уязвимостей (1 человек):

- Критичные уязвимости на внешнем периметре, с даты публикации обновлений прошло более 30 дней
- Критичные уязвимости во внутреннем периметре, с даты публикации обновлений прошло более 90 дней

Организовать мониторинг и реагирование на инциденты ИБ (минимум 3 человека):

- Сбор событий безопасности
- Анализ событий безопасности

Важное из нового. Обновленные требования 117?

Квалификации персонала по ИБ и обучение пользователей

Ответственный за защиту информации:

- зам. руководителя с высшим образованием по направлению ИБ либо профессиональная переподготовка *(если организация попадает под действие Указа Президента РФ №250, 1272-ПП)*

Структурное подразделение (специалисты) по защите информации:

- **образование** по направлению ИБ либо переподготовка* (для 30% работников подразделения (специалистов))
- **развитие компетенций** по направлению ИБ (знание сети, ОС, понимание принципов атак и прочее)
- **навыки работы** с инструментами и решениями по ИБ
- **киберучения** для отработки навыков реагирования на КИ

Рядовые сотрудники:

- периодическое обучение **кибергигиене** (лекции, раздатка, примеры инцидентов)
- **тренировки** при помощи специализированных инструментов (AWR, обучающие площадки)
- **оценка знаний** раз в 3 года или после инцидента

*Перечень организаций, осуществляющих образовательную деятельность: https://fstec.ru/dokumenty/vse-dokumenty/perechni/perechen-organizatsij-osushchestvlyayushchikh-obrazovatelnuyu-deyatelnost

Подрядчик тоже обязан

Требования приказа распространяются теперь и на подрядчиков, которые оказывают услуги для оператора ГИС (требования определяются на усмотрение оператора)

Требования по взаимодействию с подрядными организациями

Организационные мероприятия:

- Договорная ответственность подрядчиков
- Список сотрудников подрядчика
- Запрет зарубежных программ для удаленного доступа

Процессы:

- Периодические пентесты
- Мониторинг инфраструктуры
- Управление уязвимостями

Технические решения:

- Необходимые классы решений: многофакторная аутентификация, антивирусная защита, управление доступом привилегированных пользователей, средства криптографической защиты, межсетевые экраны и т.д.
- Регистрация действий подрядчиков

Многофакторная аутентификация (MFA)

- Для удаленного доступа в информационную систему непривилегированных пользователей
- Для локального доступа в информационную систему привилегированных пользователей
- Актуально для всех типов пользователей и классов защищенности, кроме непривилегированных пользователей в системах

Внутренние и внешние пользователи

Внутренние

1. **работники оператора (обладателя информации), заказчика ИС, а также подведомственных ему государственных органов и организаций (при их наличии)**, выполняющие свои обязанности (функции) с использованием информации, информационных технологий и средств вычислительной техники ИС и которым в ИС присвоены учетные записи

2. **работники подрядных организаций**, привлекаемые на договорной основе для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации ИС, а также для выполнения работ, оказания услуг по защите информации

Внешние

все **пользователи ИС**, не указанные в качестве внутренних пользователей, получающие доступ к ИС со средств вычислительной техники, **не входящих в состав ИС** или для которых оператором ИС **не могут устанавливаться и контролироваться требования о защите информации**

Обеспечение непрерывности функционирования при возникновении нештатных ситуаций

- *Автоматизированная система*
- *Обеспечение восстановления в короткий срок*
- *Гарантия сохранности резервных копий*
- *Автоматическое создание резервных копий*
- *Резервирование из разных источников*

Расширение состава СЗИ.
Все новое – хорошо забытое старое?

На что обратить внимание в части использования сертифицированных СЗИ

- SIEM
- MDM
- Песочница (SANDBOX)
- MFA
- EDR
- Защита почты
- NGFW
- PAM

На что обратить внимание в части СЗИ

- Mail Security
- EDR

Средства защиты электронной почты (Mail Security)

- Необходимы для всех классов защищенности
- Антивирусная защита почты
- Защита от спама и фишинга

Средства обнаружения и реагирования на узлах (EDR)

- Обнаружение и реагирование на угрозы
- Необходимы для всех классов защищенности
- Источник событий для мониторинга на узлах

На что обратить внимание в части СЗИ

- SIEM
- SANDBOX

Система управления событиями безопасности (SIEM)

- Обязательно использование со второго класса защищенности
- Анализ событий со средств обнаружения вторжений, межсетевых экранов, средств защиты конечных устройств

Эмулятор среды функционирования ПО (Песочница (SANDBOX)

- Обязательно использование со второго класса защищенности
- Выявление вирусов и целевых атак путем запуска и анализа поведения подозрительных объектов

Универсальное решение?

- NGFW

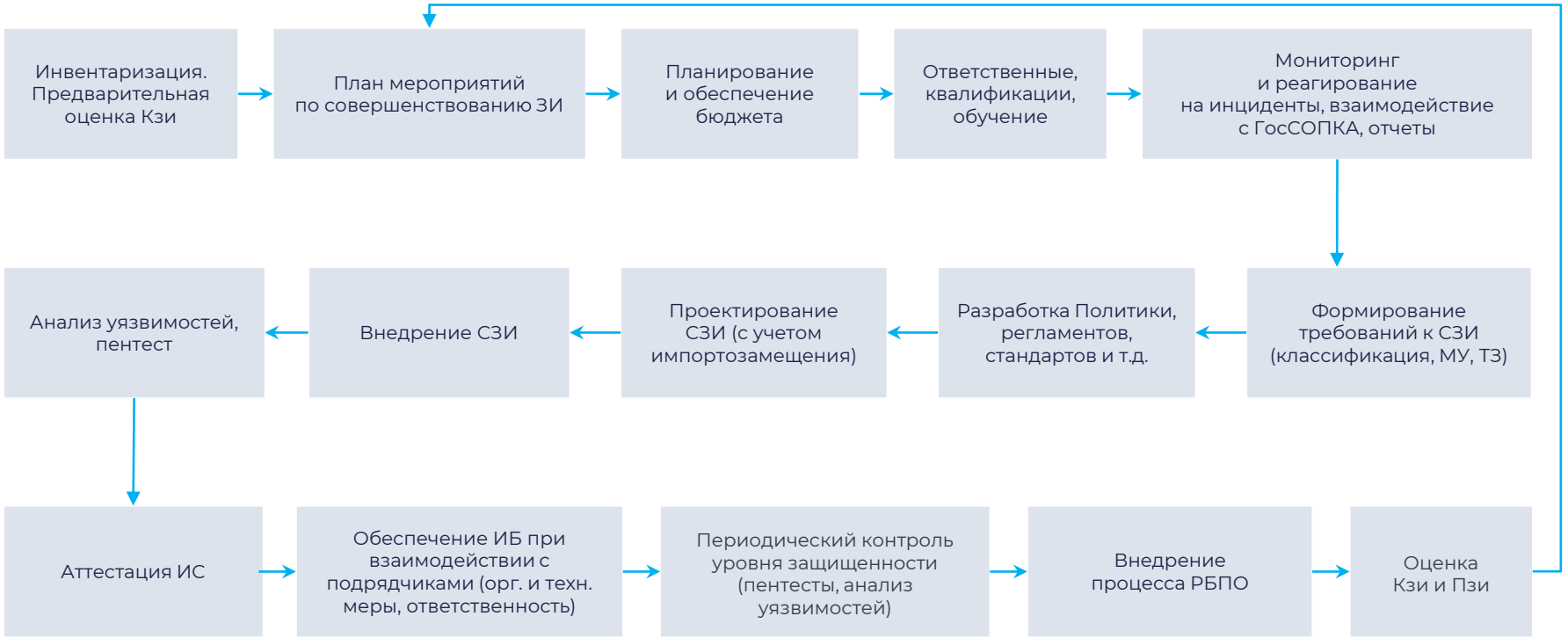
Многофункциональный межсетевой экран (NGFW)

- Возможность использования для всех классов защищенности

- Выполнение требований по контролю и управлению доступом, фильтрации трафика на сетевом и прикладном уровне, регистрации событий безопасности, сетевой антивирусной защите, сегментации сети, организации ДМЗ, защите каналов связи и сетевого взаимодействия, контролю подлинности соединений и обнаружению вторжений

Что делать дальше? С чего начать?

Дорожная карта



Работайте с нами!

8 800 3333-872

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9

127015, г. Москва,
Бутырская улица, 75

info@ksb-soft.ru

Сайт компании

Группа Вконтакте

Телеграм-канал
«Мнение Интегратора»

Канал в MAX
«Мнение Интегратора»