КСБ-СОФТ

positive technologies

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

Часть 3: Практическое руководство по выполнению требований к защите информации. Меры защиты, классы защищённости и инструменты реализации

Игорь Удиванов – технический писатель отдела аудита информационных систем

Владимир Яцюк – руководитель отдела поддержки продаж

Сергей Быков – модератор, заместитель начальника коммерческого отдела

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

- Ключевые изменения в методическом документе ФСТЭК от 12.04.2026.
- Базовый набор мер, адаптация и верификация мер защиты информационных систем.
- Что меняется в требованиях к средствам защиты информации?
- Как растёт сложность и глубина защиты вместе с классом защищенности информационной системы?
- Применяемые технологии и как они влияют на проектирование системы защиты информации.
- Решения Positive Technologies для реализации мероприятий и мер защиты информационных систем и содержащейся в них информации.

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

6000+
реализованных проектов

Канал в MAX
«Мнение Интегратора»

Портфолио КСБ-СОФТ

«Positive Technologies»

- Создаем продукты и решения
- Проводим аудиты безопасности
- Расследуем инциденты
- Исследуем угрозы

21 год

опыта исследований и разработок

300+

экспертов в нашем исследовательском центре безопасности

250+

аудитов безопасности корпоративных систем делаем ежегодно

200+

обнаруженных уязвимостей нулевого дня в год

ИС, ПОПАДАЮЩИЕ ПОД ДЕЙСТВИЕ 117 ПРИКАЗА ФСТЭК РОССИИ:

- Государственные информационные системы
- Муниципальные информационные системы
- ИС ГО, ГУ, ГУП
- ИС организаций, получающих информацию из ГИС
- ИС подрядчиков
- ЦОДы в которых размещаются ИС, попадающие под требования 117 приказа

Вебинар от 05.03.2026

ИЗМЕНЕНИЕ ПОДХОДА

- Переход от разовой организации защиты к процессу непрерывной безопасности
- 21 мероприятие по защите информации
- 17 мер по защите информации
- Оценка состояния защиты информации
- Реализация в информационных системах мер по их защите и защите содержащейся в них информации (пп. «у» п. 34)

МЕРОПРИЯТИЯ ПО РЕАЛИЗАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МЕР ПО ИХ ЗАЩИТЕ И СОДЕРЖАЩЕЙСЯ В НИХ ИНФОРМАЦИИ

Приказ ФСТЭК № 17	Приказ ФСТЭК № 117
❑ **Шаг 1.** Определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации	❑ **Шаг 1.** Реализация базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором (обладателем информации)
❑ **Шаг 2.** Адаптация базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы	❑ **Шаг 2.** Адаптация базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем
❑ **Шаг 3.** Уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации	❑ **Шаг 3.** Верификация адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление
❑ **Шаг 4.** Дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации	

ИЗМЕНЕНИЯ ТРЕБОВАНИЙ К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ

EDR	NGFW	SIEM	Песочница
WAF	Защита электронной почты	DLP	MDM
Сертифицированная ОС	Сертифицированная виртуализация	Сертифицированная СУБД	Средства анализа сетевого трафика на предмет наличия вторжений

ОСНОВНЫЕ ИЗМЕНЕНИЯ ПРОЕКТА МЕТОДИЧЕСКОГО ДОКУМЕНТА И УТВЕРЖДЕННОЙ ВЕРСИИ

EDR / система обнаружения вторжений уровня узла	NGFW	SIEM	Песочница
WAF	Защита электронной почты	DLP	MDM
Сертифицированная ОС / СЗИ от НСД	Сертифицированная виртуализация	Сертифицированная СУБД	Средства анализа сетевого трафика на предмет наличия вторжений

БАЗОВЫЙ НАБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Класс решений	Класс защищенности ИС		
	3 класс	2 класс	1 класс
Сертифицированные операционные системы или средства защиты информации от несанкционированного доступа	+	+	+
Многофункциональные межсетевые экраны (межсетевой экран, потоковый антивирус, обнаружение вторжений)*	+	+	+
Средство контроля и анализа защищенности	+	+	+
Средства антивирусной защиты	+	+	+
Средства криптографической защиты каналов связи	+	+	+
Система управления событиями безопасности информации	+	+	+
Средства обнаружения и реагирования на уровне узла или системы обнаружения вторжений уровня узла		+	+
Средства многофакторной аутентификации для всех типов пользователей		+	+
Программное обеспечение централизованного управления учетными записями		+	+

** красным цветом выделены классы решений, которые можно реализовать продуктами РТ*

NGFW

- Меры защиты:
  - СОВ.1
  - СОВ.2
  - МСЭ.1
  - МСЭ.2
  - МСЭ.3
  - ЗКС.1
  - ЗКС.2
  - ЗКС.3
  - АВЗ.3
- Показатель защищенности Кзи:
  - 3.1

PT NGFW

Самый производительный российский межсетевой экран нового поколения.

- Поддержка FW, IPS, URL-фильтрации, потокового антивируса и Threat Intelligence
- Использование более 8500 сигнатур от PT Expert Security Center
- Защита от эксплуатации уязвимостей, ботнетов, сетевых атак и вредоносного ПО
- Контроль доступа пользователей к веб-ресурсам и приложениям
- Блокировка опасных и вредоносных сайтов
- Предотвращение передачи зараженных файлов внутри инфраструктуры
- Производительность более 400 Гбит/с в режиме L7-фильтрации и более 100 Гбит/с с IPS и AV
- Собственная аппаратная платформа и модернизированный стек TCP/IP

SIEM

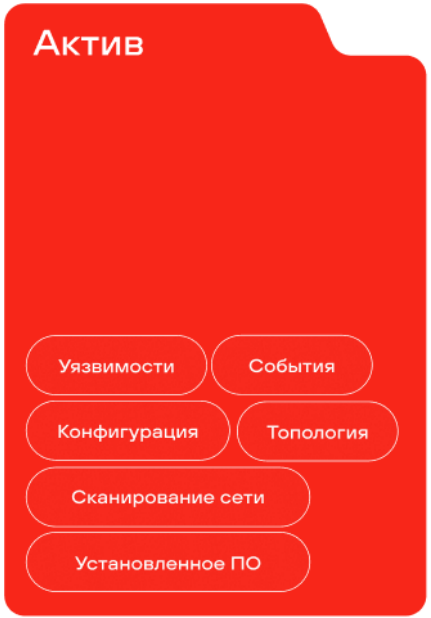
- Обеспечение мониторинга информационной безопасности (34 «л»)
- Показатель защищенности Кзи:
  - 4.2
  - 4.3
- Меры защиты:
  - РСБ.1
  - РСБ.2
  - РСБ.4
  - РСБ.5

Max Patrol SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз.

Сценарии использования:

- Сбор данных об инфраструктуре и отслеживание изменений в реальном времени
- Контроль полноты и качества сбора событий ИБ
- Единая точка мониторинга ИБ при высокой нагрузке
- Обнаружение сложных атак с помощью встроенной экспертизы и машинного обучения
- Валидация инцидентов ИБ с помощью ML-помощника
- Ускоренное расследование инцидента и реагирование из единого окна



Средства анализа защищенности

- Управление уязвимостями (34 «в»)
- Показатель защищенности Кзи:
  - 2.1
  - 2.3
  - 3.2
  - 3.3
- Меры защиты :
  - ЗКО.8

Max Patrol VM

Системы управления уязвимостями нового поколения.

- Автоматическое обнаружение IT-активов и анализ инфраструктуры
- Выявление уязвимостей, ошибок конфигурации и устаревшего ПО
- Приоритизация рисков по критичности активов и актуальности угроз
- Централизованный мониторинг и аналитика уязвимостей
- Контроль процессов vulnerability management и политик безопасности
- Интеграция с SIEM, Service Desk и другими системами безопасности
- Автоматизация реагирования и повышение эффективности SOC и IT-команд
- Снижение риска киберинцидентов и повышение киберустойчивости

Средства обнаружения и реагирования на уровне узла

Меры защиты:

- ЗКУ.3 (1)
- ЗКУ.4

Max Patrol EDR

Комплексное решение для максимальной безопасности активов

Автономная работа

Агенты способны проводить анализ и выполнять реагирование без обращения к серверу управления или доступа в интернет

Поддержка отечественных ОС

Продукт совместим со всеми популярными ОС, включая отечественные (Astra Linux, «РЕД ОС», «Альт» и др.)

Ручное или автоматическое реагирование

Более 40 действий реагирования, которые можно полностью автоматизировать

Гибкая настройка

Позволяет гибко управлять функциональностью продукта, обеспечивая баланс между реальными задачами SOC и нагрузкой на устройство

Своевременное и непрерывное обнаружение

Поставляется с набором экспертных правил от PT ESC, обнаруживающих актуальные угрозы, включая тактики и техники атакующих из матрицы MITRE ATT&CK. Новые пакеты экспертизы поставляются непрерывно

Интеграционный потенциал

Передает события в сторонние системы

Сканирует узлы в режиме аудита

Предоставляет API для реагирования на агентах

Позволяет отправлять файлы на анализ в сторонние системы

Антивирусная защита

- Меры защиты:
  - АВЗ.1
  - ЗКУ.3
- Показатель защищенности Кзи:
  - 3.4
  - 3.5

Max Patrol EPP

Непрерывное обнаружение и устранение ВПО

Решение отслеживает и оперативно блокирует новые угрозы, обеспечивая постоянную защиту конечных устройств

Интеграция с другими средствами защиты

Интеграция с SIEM-системами и песочницами для глубокого анализа угроз при минимальном расходе ресурсов

Комбинация с MaxPatrol EDR для обнаружения инцидентов и реагирования на сложные атаки

Целевое реагирование

Блокировка запуска вредоносных файлов

Помещение образца файла в карантин

Удаление файлов и завершение процессов

Сетевая изоляция узла

Масштабируемость

Подходит как для небольших инсталляций, так и для крупных георасределенных инфраструктур

Сканирование по вашим правилам

Проверки по расписанию или по запросу

Оптимизация потребления ресурсов

Возможность внесения исключений

Гибкая настройка

Модульная структура позволяет настроить функциональность продукта с учетом поставленных задач и внутренних регламентов

КАК ВЛИЯЮТ ПРИМЕНЯЕМЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ВЫБОР СРЕДСТВ ЗАЩИТЫ?

Технология	Класс решений
Технология применения веб-технологий	Межсетевой экран уровня веб-сервера
Технология использования программных интерфейсов взаимодействия приложений API	Межсетевой экран уровня веб-сервера
Технология электронной почты	Средства защиты электронной почты
Технология контейнеризации	Сертифицированные средства контейнеризации
Технология виртуализации	Сертифицированные средства виртуализации
	Средства доверенной загрузки
Технология использования мобильных устройств	Системы управления мобильными устройствами
Технология "интернета вещей"	Физическая защита, защита канала связи
Технология ИИ	Сертифицированные ИИ
Технология беспроводного доступа	Средства идентификации и аутентификации в точках беспроводного доступа

WAF

Меры защиты:

- ЗВТ.3
- ЗВТ.4
- ЗПИ.1
- ЗПИ.3

PT AF

Высокопроизводительный межсетевой экран для непрерывной защиты веб-приложений

- Выявляет сложные многоступенчатые атаки
- Предотвращает загрузку ВПО
- Противодействует вредоносным ботам
- Поддерживает приложения с NLTM
- Блокирует атаки нулевого дня
- Обнаруживает аномальное поведение трафика и позволяет задавать правила обработки (L7)
- Предоставляет аналитику в режиме реального времени
- Защищает API веб-приложений
- Мультитенантность
- Поддержка full proxy HTTP/2
- Автосканирование ресурсов
- Выявление подозрительной активности пользователя
- Несколько типов развертывания

ОЦЕНКА ПОКАЗАТЕЛЯ, ХАРАКТЕРИЗУЮЩЕГО ТЕКУЩЕЕ СОСТОЯНИЕ ЗАЩИТЫ ИНФОРМАЦИИ (КЗИ) И ПРОДУКТЫ POSITIVE TECHNOLOGIES

Группа показателей	Номер показателя безопасности	Реализация
1. Организация и управление	1	Организационные меры
	2	Организационные меры
	3	Организационные меры
2. Защита пользователей	1	Организационные меры + средства реализации парольной политики + Max Patrol VM
	2	Средства многофакторной аутентификации + организационные меры
	3	Средства реализации парольной политики + Max Patrol VM
	4	Организационные меры
3. Защита информационных систем	1	Организационные меры + PT NGFW
	2	Организационные меры + Max Patrol VM
	3	Организационные меры + Max Patrol VM
	4	Организационные меры + Max Patrol EDR
	5	Организационные меры + Max Patrol EPP
	6	Организационные меры
4. Мониторинг информационной безопасности и реагирование	1	Организационные меры + Max Patrol SIEM или SOCRAT
	2	Организационные меры + Max Patrol SIEM или SOCRAT
	3	Организационные меры

SOCRAT
SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА КСБ-СОФТ

Режим работы 24x7

Корпоративный центр ГосСОПКА
(класс А)

- ✓ **Инвентаризация**
- ✓ **Анализ уязвимостей**
- ✓ **Тестирование на проникновение**

Пакетная система предоставления услуг
(выбор только необходимого)

Год создания: 2020

Средства анализа сетевого трафика на предмет наличия вторжений

PT NAD

Система поведенческого анализа сетевого трафика для обнаружения кибератак и расследования инцидентов

- Контроль соблюдения регламентов ИБ
- Обнаружение теневой инфраструктуры
- Выявление атак и аномалий в сети
- Расследование атак
- Обнаружение некорпоративных ОС и ПО
- Проверка сетевых узлов
- Обнаружение средств удаленного администрирования
- Проактивный поиск угроз

Замкнутая система (среда) предварительного выполнения программ («песочница»)

PT Sandbox

Статический анализ

- Правила PT ESC
- Анализ содержимого ссылок PT Crawler
- Категоризатор ссылок PT Categorizer
- Индикаторы компрометации PT IoC
- Анализ с помощью внешней экспертизы

Предфильтрация

Поведенческий анализ

- Анализ сетевого трафика и подключений
- Дампы памяти и процессы
- Технологии ML
- Правила PT ESC

Ретроспективный анализ | **Хранилище** | **Ручная перепроверка**

Источники


API-интеграция


Ручная загрузка объектов


Электронная почта


Объекты из сетевого трафика (ICAP)


Файловые хранилища

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»