Практическое выполнение требований приказа ФСТЭК №117 на основе продуктов ИнфоТеКС

Андрей Петров

руководитель центра мониторинга и реагирования
на инциденты информационной безопасности – начальник
отдела аттестаций и разработки документов ООО «Инфолайн»

инфотекс ТЕХНОФЕСТ

Белый поток

Компания ИНФОЛАЙН

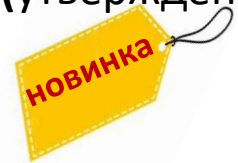
Практическое выполнение требований приказа ФСТЭК № 117 на основе продуктов ИнфоТеКС

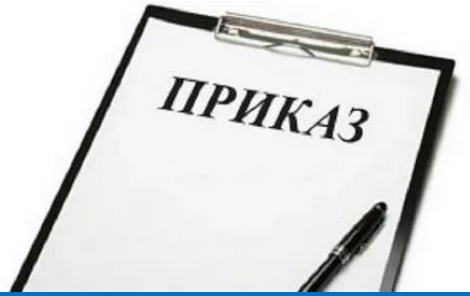
Петров Андрей
руководитель центра мониторинга и реагирования
на инциденты информационной безопасности – начальник
отдела аттестаций и разработки документов ООО «Инфолайн»

Новые и измененные правила

Приказ ФСТЭК России от 11.04.2025 **№ 117**
«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

Методический документ
«Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах**»**
(утвержден ФСТЭК России 12.04.2026**)**





Набор мероприятий в Приказе ФСТЭК № 117

Выявление и оценка угроз БИ	Контроль конфигураций ИС	Управление уязвимостями	Управление обновлениями	Защита при обработке информации
Защита конечных устройств	Защита мобильных устройств	Защита удаленного доступа	Защита беспроводного доступа	Защита привилегированного доступа
Мониторинг ИБ	Разработка безопасного ПО	Физическая защита ИС	Непрерывное функционирование ИС	Повышение уровня знаний
Защита при взаимодействии с подрядными организациями	Защита от КА на отказ в обслуживании	Защита искусственного интеллекта	Реализация мер по защите информации	контроль уровня защищенности
		Взаимодействие с ГосСОПКА		

Набор мероприятий в Приказе ФСТЭК № 117

Выявление и оценка угроз БИ	Контроль конфигураций ИС	Управление уязвимостями	Управление обновлениями	Защита при обработке информации
Защита конечных устройств	Защита мобильных устройств	Защита удаленного доступа	Защита беспроводного доступа	Защита привилегированного доступа
Мониторинг ИБ	Разработка безопасного ПО	Физическая защита ИС	Непрерывное функционирование ИС	Повышение уровня знаний
Защита при взаимодействии с подрядными организациями	Защита от КА на отказ в обслуживании	Защита искусственного интеллекта	Реализация мер по защите информации	контроль уровня защищенности
		Взаимодействие с ГосСОПКА		

21 мероприятие

Набор мероприятий в Приказе ФСТЭК № 117

Выявление и оценка угроз БИ	Контроль конфигураций ИС	Управление уязвимостями	Управление обновлениями	Защита при обработке информации
Защита конечных устройств	Защита мобильных устройств	Защита удаленного доступа	Защита беспроводного доступа	Защита привилегированного доступа
Мониторинг ИБ	Разработка безопасного ПО	Физическая защита ИС	Непрерывное функционирование ИС	Повышение уровня знаний
Защита при взаимодействии с подрядными организациями	Защита от КА на отказ в обслуживании	Защита искусственного интеллекта	Реализация мер по защите информации	контроль уровня защищенности
		Взаимодействие с ГосСОПКА		

18 мероприятий

Выявление и оценка УБИ

- Выявление и оценка УБИ ИС для ИТКС;
- Поиск данных и признаков, идентифицирующих актуальные УБИ;
- Использование в качестве исходных данных БДУ ФСТЭК;
- Оповещение о выявленных УБИ;
- Выявление УБИ с обогащением данными из СОВ, АВЗ, МЭ;
- Привлечение лицензиатов ФСТЭК для выявления актуальных УБИ;
- Применение средств анализа угроз, TI-платформ.

- Создание ИТКС на основе продуктов ViPNet;
- IoC и IoA от ЦМ Перспективный мониторинг;
- Хостовые и сетевые СОВ линейки ViPNet IDS HS, EPP, NS;
- Межсетевые экраны: ПАК ViPNet Coordinator, HW, IG, xFirewall, хостовые ViPNet Client, EPP;
- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн;
- AM TIP - TI-платформа от Перспективного мониторинга.

Контроль конфигураций ИС

- Определение объектов инвентаризации;
- Сбор, учет и хранение данных об объектах инвентаризации;
- Контроль состава объектов инвентаризации;
- Определение конфигураций объектов инвентаризации;
- Сбор, анализ и регистрацию фактов несанкционированного изменения состава объектов инвентаризации и их конфигураций, реагирование.

- Система управления продуктами ViPNet Prime;
- ViPNet TDR IDS MC;
- ViPNet SafeBoot.

Управление уязвимостями

- Мониторинг уязвимостей и оценка их применимости;
- Определение методов и приоритетов устранения уязвимостей;
- Устранение уязвимостей;
- Контроль устранения уязвимостей;
- Применение средств анализа угроз, в том числе TI-платформы;
- Использование результатов мониторинга ИБ.

- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн;
- AM TIP - TI-платформа от Перспективного мониторинга.

Защита при обработке информации

- Обеспечение доступа к информации;
- Контроль передачи, распространения информации в ИС;
- Контроль и регистрация всех фактов доступа пользователей к информации.

- СЗИ НСД: ViPNet SafePoint, SafeBoot, EPP;
- Межсетевые экраны: ПАК ViPNet Coordinator, HW, IG, xFirewall, хостовые ViPNet Client, EPP;

Защита конечных устройств

- Реализация мер ЗИ от НСД;
- Осуществление на устройствах мониторинга и анализа процессов и событий для выявления актуальных УБИ;
- Предупреждение пользователя о произошедших на конечных устройствах событиях ИБ;
- Контроль доступа в сеть Интернет.

- СЗИ НСД: ViPNet SafePoint, SafeBoot, EPP, IDS HS;
- Межсетевые экраны: ПАК ViPNet Coordinator, HW, IG, xFirewall, хостовые ViPNet Client, EPP;
- Хранение информации в зашифрованном виде: ViPNet CryptoFile;
- ViPNet CSS Connect.

Защита мобильных устройств

- Предоставление доступа к ИС с использованием мобильных устройств только пользователям;
- Реализация в мобильных устройствах мер по защите информации от НСД;
- Защита каналов передачи данных при доступе к ИС с использованием мобильных устройств с использованием СКЗИ;
- Идентификация и аутентификация мобильных устройств.

- СКЗИ ViPNet Client 4U, ViPNet PKI Client;
- Хранение информации в зашифрованном виде: ViPNet CryptoFile;
- ViPNet CSS Connect.

Защита удаленного доступа

- Идентификации и аутентификации удаленно подключаемых пользователей;
- Разграничение и контроль доступа удаленных пользователей к объектам доступа ИС;
- Регистрация событий безопасности;
- Защита web-технологий;
- Защита данных, передаваемых по сети «Интернет», с использованием СКЗИ;
- Контроль сетевых доступов к сегментам ИС;
- Обнаружение и предотвращение вторжений на сетевом уровне при осуществлении удаленного доступа.

- Хостовые и сетевые СОВ линейки ViPNet IDS HS, EPP, NS;
- Межсетевые экраны: ПАК ViPNet Coordinator, HW, IG, xFirewall, хостовые ViPNet Client, EPP;
- СКЗИ: ViPNet Client 4U, ViPNet PKI Client;
- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн.

Защита беспроводного доступа

- Обеспечение защиты беспроводных каналов передачи данных;
- Защиту точек беспроводного доступа;
- Идентификации и аутентификации точек беспроводного доступа.

- СКЗИ: ViPNet Client 4U, ViPNet PKI Client;
- ViPNet CSS Connect;
- ViPNet Coordinator IG.

Защита привилегированного доступа

- Применение для привилегированных учетных записей строгой аутентификации или усиленной многофакторной аутентификации;
- Аутентификационная информация привилегированных учетных записей, заданная разработчиком, производителем программных, программно-аппаратных средств по умолчанию, подлежит изменению при первоначальной настройке программных, программно-аппаратных средств.

- Система управления продуктами ViPNet Prime;
- ViPNet Coordinator HW, IG;

.

Мониторинг событий ИБ

- Сбор данных о событиях безопасности и иных данных мониторинга ИБ, предусмотренных ГОСТ Р 59547-2021 «ЗИ. Мониторинг ИБ. Общие положения»;
- Обработка и анализ событий ИБ;
- Контроль, учет и анализ действий пользователей ИС;
- Своевременное информирование о выявленных нарушениях функционирования ИС;
- Привлечение организаций-лицензиатов ФСТЭК.

- Хостовые сенсоры ViPNet HS, EPP;
- Сетевые сенсоры ViPNet IDS NS, xFirewall;
- Системы анализа событий ИБ и поиска инцидентов ViPNet TIAS ПАК, VA;
- ViPNet TDR ViPNet IDS MC;
- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн.

.

Разработка безопасного ПО

- Обучение разработчиков безопасного ПО;
- Формирование и предъявление требований по безопасности к ПО;
- Управление конфигурацией ПО;
- разработка, уточнение и анализ архитектуры ПО, снижение потенциальных уязвимостей;
- Моделирование актуальных УБИ;
- Формирование и поддержание правил безопасного кодирования;
- Экспертиза исходного кода ПО, проведение статического, динамического анализа кода;
- Использование безопасной системы сборки ПО;
- Обеспечение безопасности сборочной среды ПО;
- Управление доступом и контроль целостности кода в ходе разработки ПО;
- Проверку на внедрение вредоносного ПО;
- **Обеспечение безопасности при выпуске готовой к эксплуатации версии ПО;**
- **Безопасная доставка ПО;**
- **Поддержка ПО при эксплуатации;**
- **Поиск и устранение выявленных уязвимостей в ПО.**

- Порядок проведения сертификации. Утвержден приказом ФСТЭК России от 1 декабря 2023 г. № 240;
- Компания Инфотекс имеет сертификат № 4 ФСТЭК России от 08.04.2025 соответствии процессов безопасной разработки программного обеспечения требованиям ГОСТ Р 56939-2016.


СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

Непрерывное функционирование ИС

- Применение программных, программно-аппаратных средств, обеспечивающих выполнение значимых функций, в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций ИС;
- Применение систем мониторинга производительности и доступности средств вычислительной техники;
- Использование средств синхронной настройки параметров безопасности.

- Кластеризация ViPNet Coordinator HW, IG, KB, ViPNet IDS NS, ViPNet xFirewall;
- Сегментирование ViPNet TDR: TIAS, NS, HS, MC;
- Определение временных характеристик работы ПАК СКЗИ;
- ViPNet Prime.

.

Повышение уровня знаний и информированности пользователей по ИБ

- Доведение до пользователей НПА по ЗИ;
- Проведение лекций, семинаров, обучающих игр по вопросам ЗИ;
- Проведение тренировок с пользователями по практической отработке мероприятий по ЗИ;
- Разработка специализированных курсов для повышения уровня знаний;
- Использование АС (платформ),, для обучения и прохождения тестирования уровня знаний и компетенций работников по вопросам ЗИ.

- Курсы сертификации и повышения квалификации в Учебном центре Инфотекс;
- Учебно-тренировочная платформа Ampire;
- Проведение киберучений.

.

Защита при взаимодействии с подрядными организациями

- отдельные учетные записи для подрядчиков с правами доступа, минимально необходимыми для выполнения условий договора;
- Мониторинг и регистрация действий учетных записей подрядчиков. При обнаружении попыток нарушения правил доступа незамедлительная блокировка;
- Меры по ЗИ в ИС подрядчиков;
- Удаленный доступ подрядчиков с использованием СКЗИ.

- **Удаленный доступ:**

СКЗИ: ViPNet Coordinator KB, HW, IG, VA, ViPNet Client, ViPNet TLS., SIES;

МЭ: ViPNet xFirewall, ViPNet EPP;

- **Мониторинг ИБ**: ViPNet TDR (TIAS, NS, HS, MC), ViPNet EPP, услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн;
- **СЗИ НСД:** ViPNet SafePoint, ViPNet SafeBoot; ViPNet EPP.

.

Защита от КА отказ в обслуживании

- Ограничение доступа к интерфейсам и сервисам ИС, доступных из «Интернет», публичных сетевых адресов и доменных имен, не используемых функционирования ИС;
- Определение сетевых адресов, с которыми должно быть взаимодействие ИС, формирование списка разрешенных сетевых адресов в условиях реализации КА, направленных на отказ в обслуживании;
- Использование ПАК, обеспечивающих анализ и фильтрацию входящего трафика с возможностью его блокирования;
- Обеспечение хранения информации о фактах реализации КА, направленных на отказ в обслуживании;
- Взаимодействие с ГосСОПКА.

- МЭ/СКЗИ: ViPNet Coordinator KB, HW, IG, VA, ViPNet Client;
- МЭ: ViPNet xFirewall, ViPNet EPP;

- Хостовые сенсоры ViPNet HS, EPP ;
- Сетевые сенсоры ViPNet IDS NS, xFirewall;
- Системы анализа событий ИБ и поиска инцидентов ViPNet TIAS ПАК, VA;
- ViPNet TDR ViPNet IDS MC;
- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн.

Проведение периодического контроля уровня защищенности информации в ИС

- Тестирование ИС путем моделирования реализации актуальных угроз с целью оценки возможностей проникновения в них;
- Проведение тренировок по отработке работниками оператора (обладателя информации) действий по обеспечению требуемого уровня защищенности информации в ИС, в условиях реализации актуальных угроз.

+

- Показатель Кзи «показатель состояния ТЗИ». Методика ФСТЭК от 11.11.2025. Раз в полгода !

- Услуги ЦМ Перспективный мониторинг и ЦМ Инфолайн;
- Хостовые сенсоры ViPNet HS, EPP ;
- Сетевые сенсоры ViPNet IDS NS, xFirewall;
- Системы анализа событий ИБ и поиска инцидентов ViPNet TIAS ПАК, VA;
- ViPNet TDR ViPNet IDS MC;
- МЭ/СКЗИ: ViPNet Coordinator KB, HW, IG, VA, ViPNet Client;
- МЭ: ViPNet xFirewall, ViPNet EPP;

Выполнение мероприятий и мер по ЗИ

- 60+ продуктов компании ИнфоТеКС;
- Различные сценарии применения продуктов;
- Возможность выполнять разные меры из разных групп мер.

Спасибо за внимание!

Контактные данные представителей ООО «Инфолайн» в г. Санкт-Петербург:

Антон Тектониди
тел.: +7 963 324 86 46
e-mail: spb@infoline-rk.ru

Руслан Магомедов
тел.: +7 921 411 04 11
e-mail: spb.magomedov@infoline-rk.ru

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети