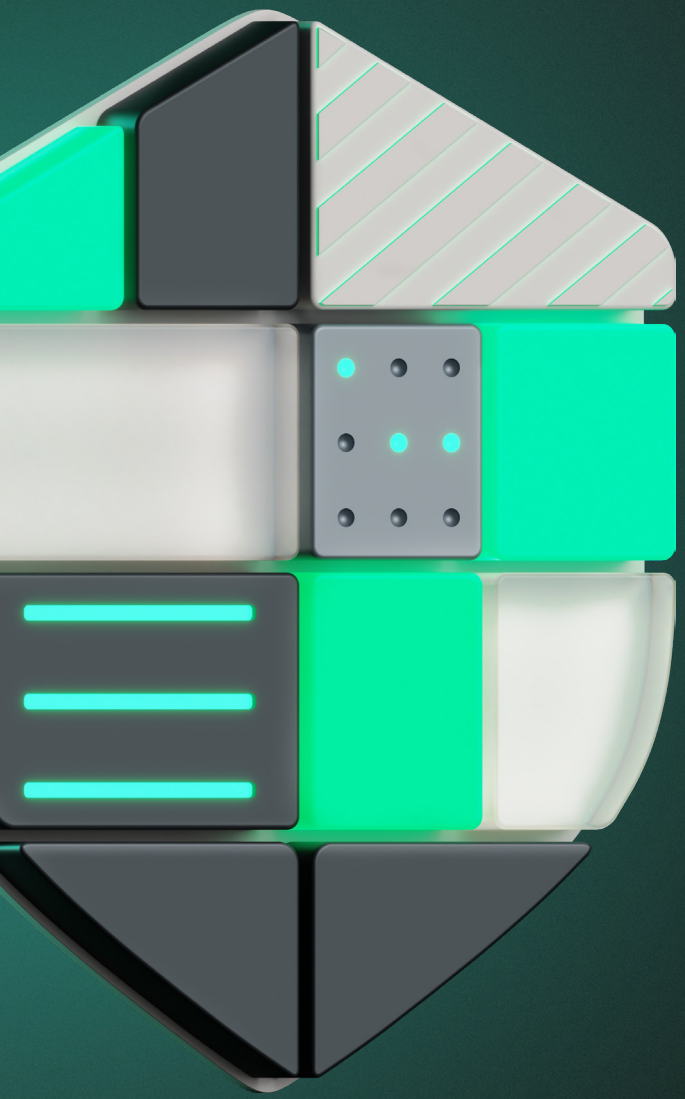


Решения «Лаборатории Касперского», предлагаемые в рамках приказа ФСТЭК России № 117

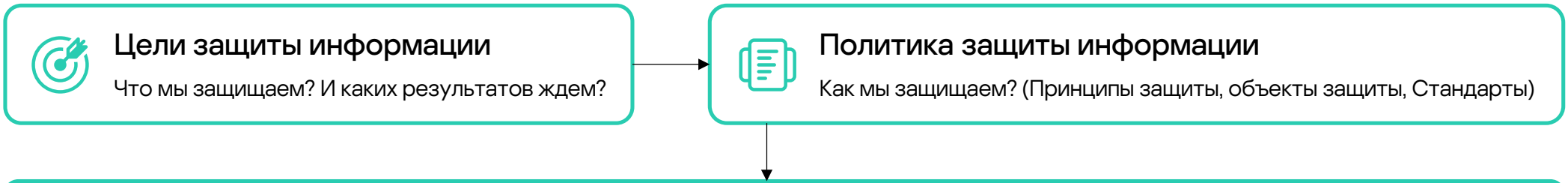
kaspersky активируй будущее

Приказ ФСТЭК России № 117 от 11.04.2025

«Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»

Защита информации в ГИС

Главная цель защиты информации — предотвращение негативных последствий для государства / организации.



Меры по защите информации

Организационные

- Стандарты
- Регламенты
- Инструкции

Технические

Запрещается применение средств защиты согласно ограничениям, введенным Указом Президента РФ № 250 от 01.05.2022

Ответственность

Руководители организации / ИБ

Состав средств защиты информации

Предложение под базовый набор мер по защите информации

Базовый набор мер

- Управление доступом
- Регистрация событий безопасности
- Защита виртуализации и облачных вычислений
- Защита веб-технологий
- Защита точек беспроводного доступа
- Антивирусная защита
- Обнаружение и предотвращение вторжений на сетевом уровне
- Сегментация и межсетевое экранирование
- Защита каналов передачи данных и сетевого взаимодействия
- Защита технологий контейнерных сред и их оркестрации
- Защита сервисов электронной почты
- Защита программных интерфейсов взаимодействия приложений
- Защита конечных устройств
- Защита мобильных устройств
- Защита технологий интернета вещей
- Защита от компьютерных атак, направленных на отказ в обслуживании
- Идентификация и аутентификация

Предлагаемые продукты

- Kaspersky NGFW
- Kaspersky Security для бизнеса
- Kaspersky Security для интернет-шлюзов
- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Detection and Response Expert
- Kaspersky Security для почтовых серверов
- Kaspersky Container Security
- Kaspersky SD-WAN

Предложение под базовый набор мер по защите информации

Базовый набор мер

Управление доступом

Регистрация событий безопасности

Защита виртуализации и облачных вычислений

Защита точек беспроводного доступа

Защита веб-технологий

Антивирусная защита

Защита каналов передачи данных и сетевого взаимодействия

Сегментация и межсетевое экранирование

Обнаружение и предотвращение вторжений на сетевом уровне

Kaspersky NGFW

Высокотехнологичный Stateful Firewall

Продвинутая SSL/TLS инспекция

Высокоточный веб-категоризатор

Гибкий IDPS с большим количеством сигнатур

Безопасный DNS

AI-Powered антивирус

Проверка репутации URL-адресов

Высокоскоростной потоковый антивирус

Гибкая настройка пользовательских политик доступа

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 49

Мероприятия по обеспечению мониторинга информационной безопасности должны предусматривать сбор данных о событиях безопасности, их обработке и анализе, а также выявлении признаков реализации угроз безопасности.

Мероприятия по осуществлению мониторинга должны проводиться в отношении всех информационных систем, за исключением локальных и изолированных систем.

В ходе проведения мониторинга ИБ для анализа зафиксированных событий безопасности и выявления в них признаков реализации актуальных угроз допускается использование доверенных технологий искусственного интеллекта.

Kaspersky Unified Monitoring and Analysis Platform

- Обеспечение мониторинга ИБ
- Сбор данных о событиях безопасности
- Выявление признаков реализации угроз безопасности
- Использование в составе доверенных технологий ИИ
- Учет ИТ-активов и контроль конфигураций ИС
- Выявление несанкционированных подключений устройств к информационным системам

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 37 Контроль конфигураций должен осуществляться на основе анализа результатов учета ИТ активов и сведений управляющих ИТ активами.

п. 39 Мероприятия по управлению обновлениями должны включать проведение проверки подлинности и целостности обновлений программных средств.

п. 41 Мероприятия по обеспечению защиты информации при применении конечных устройств информационных систем должны исключать возможность несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью "Интернет" и (или) доступные из сети "Интернет".

Kaspersky Endpoint Detection and Response Expert

Kaspersky Security для бизнеса

- Автоматический анализ подозрительных событий на конечных рабочих станциях
- Контроль используемого ПО / запуска ПО на рабочих станциях / серверах
- Реагирование на инциденты ИБ
- Оценка критичности уязвимостей
- Выявление и приоритизация уязвимостей компонентов информационной системы
- Определение методов и приоритетов устранения уязвимостей
- Проверка подлинности и целостности обновлений программных средств
- Возможность контроля воздействия на конечные устройства через интерфейсы и порты, взаимодействующие с сетью «Интернет»

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 38

Мероприятия по управлению уязвимостями должны включать выявление уязвимостей информационных систем, оценку их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

Kaspersky Container Security

- Выявление уязвимостей
- Автоматический анализ подозрительных событий в контейнерной инфраструктуре
- Контроль конфигураций компонентов контейнерной инфраструктуры
- Контроль процесса устранения уязвимостей компонентов контейнерной инфраструктуры
- Возможность проведения проверок безопасности узлов на платформе оркестрации
- Отслеживание и отображение истории изменений состояния компонентов контейнерной инфраструктуры
- Мониторинг и реагирование на события информационной безопасности контейнерной инфраструктуры

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 42

Посредством проведения мероприятий по обеспечению защиты информации при применении мобильных устройств должна быть исключена возможность несанкционированного доступа к информационным системам и содержащейся в них информации.

Осуществлять доступ пользователей с применением строгой аутентификации.

Kaspersky Secure Mobility Management

- Возможность контроля доступа к информационным системам с мобильного устройства
- Возможность реализации строгой аутентификации
- Защита от вредоносного ПО
- Контроль соответствия мобильных устройств требованиям по защите информации

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 56

Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации должны включать:

А) Доведение до пользователей информационных материалов, в том числе форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;

Б) Проведение лекций, семинаров, обучающих игр по вопросам защиты информации;

В) Проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;

Г) Проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

Kaspersky Automated Security Awareness Platform

- Реализация возможности проведения лекций по вопросам защиты информации
- Наличие информационных материалов по актуальным вопросам защиты информации
- Наличие возможности проведения имитационных рассылок электронных писем на служебные адреса
- Наличие возможности проведения тренировок с пользователями по практической отработке мероприятий по защите информации

Сопоставление требований и реализации

23 пункт

Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечивать выполнение возложенных на них обязанностей (функций) по защите информации.

п. 59

По средствам проведения мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании.

Kaspersky DDoS Protection

- Решение, которое позволяет защитить ресурсы информационной системы от компьютерных атак направленных на отказ в обслуживании
- Наличие сертификатов соответствия требованиям по защите информации

Сопоставление требований и реализации

66 пункт

Контроль уровня защищенности информации, содержащейся в информационных системах, должен обеспечивать включение проведения оценки возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями.

Kaspersky Security Assessment

- Оценка возможностей нарушения безопасности информации
- Оценка возможностей нарушения функционирования информационных систем внешним и внутренним нарушителем
- Выявление уязвимостей информационных систем с последующей оценкой возможности их использования нарушителем
- Тестирование ИС путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа

Остались вопросы?

Задайте их нашим специалистам, и мы обязательно вам ответим: regulhub@kaspersky.com.
За более подробной информацией можно обратиться к нам на сайт

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее