

???????????? ???? 239

???????????? ???? ??

???? KICS

В данном разделе мы рассмотрим меры 239 приказа ФСТЭК и как наши продукты помогут вам их закрыть

- [Введение](#)
- [Меры идентификации и аутентификации](#)
- [Меры управления доступом](#)
- [Меры ограничения программной среды](#)
- [Меры защиты машинных носителей информации](#)
- [Меры аудита информационной безопасности АСУ ТП](#)
- [Меры антивирусной защиты](#)
- [Меры предотвращения вторжений \(компьютерных атак\)](#)
- [Меры обеспечения целостности](#)
- [Меры обеспечения доступности](#)
- [Меры защиты технических средств и систем](#)
- [Меры управления конфигурацией АСУ ТП](#)
- [Меры реагирования на компьютерные инциденты](#)
- [Меры управления конфигурацией АСУ ТП](#)
- [Меры управления обновлениями программного обеспечения](#)
- [Меры планирования мероприятий по обеспечению безопасности](#)
- [Меры обеспечения действий в нештатных ситуациях](#)
- [Меры информирования и обучения персонала](#)

????????

Приказ ФСТЭК России № 239 является ключевым нормативным документом, который регулирует вопросы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ) Российской Федерации.

Приказ № 239 направлен на достижение ряда важных целей в области обеспечения информационной безопасности:

- Обеспечение национальной безопасности и устойчивости объектов КИИ

Объекты КИИ представляют собой информационные системы, сети и автоматизированные системы управления критически важных предприятий, поэтому нарушение работы данных систем может нанести ущерб здоровью граждан, экономике, общественному порядку и безопасности государства. Приказ устанавливает требования, которые направлены на защиту перечисленных систем от компьютерных атак.

- Выполнение требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказ разработан в соответствии с требованиями Федерального закона № 187-ФЗ и является обязательным для всех субъектов КИИ, чьи объекты признаны значимыми.

- Внедрение Системы безопасности

В приказе предусмотрены 17 организационных и технических мер безопасности, которые помогают выстроить комплексную систему безопасности в организации, пример мер представлен ниже:

- Идентификацию и аутентификацию (ИАФ).
- Управление доступом (УПД).
- Аудит безопасности (АУД).
- Антивирусную защиту (АВЗ).
- Предотвращение вторжений (СОВ).
- Обеспечение целостности и доступности (ОЦЛ, ОДТ).
- Реагирование на инциденты (ИНЦ) и другие.

Нужно учитывать, что те или иные меры применяются в зависимости от категории значимости объекта КИИ, что позволяет гибко выстраивать

комплексную систему безопасности.

- Повышение осведомленности и подготовки персонала

Приказ № 239 обязывает субъектов КИИ формировать процесс обучения и информирования сотрудников по вопросам безопасности, что способствует повышению киберграмотности и снижению рисков, связанных с человеческим фактором.

- Взаимодействие с государственными системами

Приказ № 239 обязывает осуществлять интеграцию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

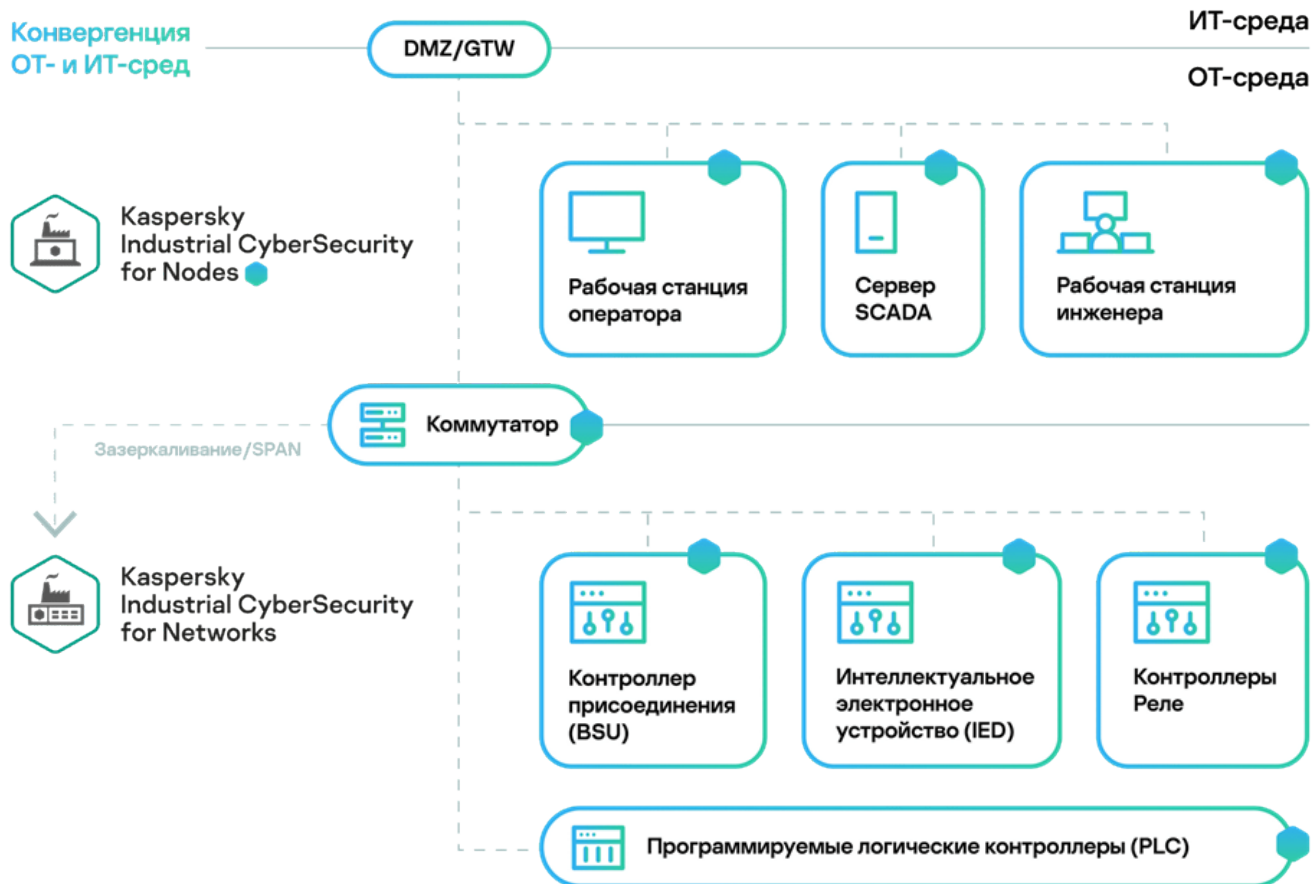
- Снижение рисков и минимизация последствий инцидентов.

Платформа Kaspersky Industrial CyberSecurity (далее - KICS) и решение класса SIEM - Kaspersky KUMA образуют мощный симбиоз для выполнения комплексных требований Приказа ФСТЭК России № 239.

KICS — это специализированная промышленная XDR-платформа, разработанная для комплексной защиты основных компонентов систем автоматизации и управления производством на всех уровнях, которая состоит из двух решений:

KICS for Nodes/ KICS for Linux Nodes со встроенной функциональностью EDR – решение, предназначенное для защиты рабочих мест, например, АРМ оператора, АРМ-инженера и т.д, также решение может осуществлять контроль целостности программ, исполняемых на ПЛК для управления технологическим процессом;

KICS for Networks – решение для защиты промышленных сетей, которое принимает копию трафика в одной или нескольких точках сети, а также телеметрию от узлов. На основании полученной телеметрии KICS for Networks изучает "нормальное" состояние сети, чтобы затем выявлять отклонения и аномалии. Помимо этого, KICS for Networks включает систему обнаружения вторжений (IDS), позволяет обнаруживать уязвимости устройств, небезопасную архитектуру сети, риски ИБ АСУ ТП, выполняет группировку и корреляцию своих событий и событий от KICS for Nodes. KICS for Networks предоставляет возможность активного опроса сети позволяет быстро и точно собирать данные о топологии сетей и настройках. Функция аудита рабочих мест помогает гарантировать соблюдение политик безопасности, включая безопасность текущих настроек, и организацию процесса выявления и митигации уязвимостей.



Kaspersky Security Center позволяет централизованно управлять программами KICS for Nodes и Kaspersky Endpoint Agent через политики и задачи, а также предоставляет интерфейс для анализа и реагирования на события безопасности от всех программ.

SIEM-система KUMA помогает усилить комплексную систему безопасности и собирает события от технологической, и от офисной сетей. Интегрируется с платформой KICS и позволяет централизованно управлять инцидентами.

???? ????????????? ?
????????????????

ИАФ.0 Разработка политики идентификации и аутентификации

Мера ИАФ.0 закрывается разработкой внутренних нормативных документов (это могут быть правила, процедуры и политики), в которых описывается процесс идентификации и аутентификации субъектов доступа и объектов доступа.

ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов

KICS for Nodes и KICS for Linux Nodes

Мера ИАФ.1 реализуется в задаче «Контроль запуска программ» в части идентификации пользователей при запуске программ. В параметрах задачи можно указать пользователей или группу пользователей, которым разрешается или запрещается запуск программ.

KICS for Networks

Мера реализуется в части идентификации устройств по MAC- и IP-адресам в обрабатываемой копии сетевого трафика и данных телеметрии от КЕА. При этом ведется составление и обновление таблицы устройств с информацией о них.

ИАФ.2 Идентификация и аутентификация устройств

KICS for Nodes и KICS for Linux Nodes

Мера реализуется в части идентификации устройств по IP-адресам путем выполнения задачи «Защита от сетевых угроз» и «Управление сетевым экраном».

KICS for Networks

Мера реализуется в части идентификации устройств по MAC- и IP-адресам в обрабатываемой копии сетевого трафика и данных телеметрии от КЕА. При этом ведется составление и обновление таблицы устройств с информацией о них.

Для усиления требований Приказа №239 нужно использовать встроенные механизмы защиты информации в части идентификации и аутентификации пользователей, которые являются сотрудниками субъектов КИИ, чтобы

обеспечить безопасность следующих систем: операционных систем, прикладного программного обеспечения, программируемых логических контроллеров, активного сетевого оборудования и т.п. Данные требования позволяет реализовать операционная система Astra Linux Special Edition, которая также совместима с решениями платформы KICS.

ИАФ.3 Управление идентификаторами

Для реализации данной меры используются встроенные механизмы защиты информации, системы защиты информации от несанкционированного доступа (далее – СЗИ от НСД), межсетевые экраны (МЭ, FW), системы управления учётными данными и доступом (далее – IAM-системы).

ИАФ.4 Управление средствами аутентификации

Для реализации данной меры используются встроенные механизмы защиты информации, а также службы каталогов, СЗИ от НСД, системы управления жизненным циклом сертификатов открытого ключа.

ИАФ.5 Идентификация и аутентификация внешних пользователей

Для реализации данной меры используются встроенные механизмы защиты информации, а также IAM-системы, системы контроля действий привилегированных пользователей.

ИАФ.6 Двусторонняя аутентификация

Для реализации данной меры используются встроенные механизмы защиты информации, а также IAM-системы.

ИАФ.7 Защита аутентификационной информации при передаче

Для реализации данной меры используются встроенные механизмы защиты информации, а также IAM-системы.

???? ?????????? ??????????

УПД.0 Разработка политики управления доступом

Мера УПД.0 закрывается разработкой внутренних нормативных документов (это могут быть правила, процедуры и политики), в которых описывается процесс управления доступом.

УПД.1 Управление учетными записями пользователей

Для реализации данной меры используются встроенные механизмы защиты информации, а также системы контроля действий привилегированных пользователей, СЗИ от НСД.

УПД.2 Реализация модели управления доступом

KICS for Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей и групп пользователей к заданным файлам и папкам с помощью задачи «Мониторинг файловых операций»;
- отслеживания и ограничения доступа пользователей и групп пользователей к запуску программ с помощью задачи «Контроль запуска программ»;
- отслеживания и блокирования действий пользователей и групп пользователей к указанным ветвям и разделам реестра с помощью задачи «Мониторинг доступа к реестру»;
- отслеживает и блокирование попыток подключения внешних устройств к защищаемому устройству с помощью задачи «Контроль устройств».

KICS for Linux Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей к заданным файлам и папкам с помощью задачи «Контроль целостности системы»;
Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл;
- отслеживания и ограничения доступа пользователей к запуску программ с помощью задачи «Контроль приложений»;

- отслеживает и блокирование попыток подключения внешних устройств к защищаемому устройству с помощью задачи «Контроль устройств».

УПД.3 Доверенная загрузка

Для реализации данной меры используются средства доверенной загрузки (далее - СДЗ), предназначенные для автоматизированных рабочих мест/серверов сотрудников субъектов КИИ и специализированным средствами для доверенной загрузки компонентов среды виртуализации.

УПД.4 Разделение полномочий (ролей) пользователей

Для реализации данной меры используются встроенные механизмы защиты информации, а также системы контроля действий привилегированных пользователей и СЗИ от НСД.

УПД.5 Назначение минимально необходимых прав и привилегий

Для реализации данной меры нужно разработать матрицу доступа, желательно в составе проектной документации на АСУ ТП.

УПД.6 Ограничение неуспешных попыток доступа в автоматизированную систему

KICS for Nodes

Мера реализуется для рабочих мест на базе ОС Windows в части обнаружения попыток подбора пароля путем анализа журналов событий Windows с помощью задачи «Анализ журналов».

УПД.7 Предупреждение пользователя при его доступе к информационным ресурсам

Для реализации данной меры используются встроенные механизмы защиты информации.

УПД.8 Оповещение пользователя при успешном входе о предыдущем доступе к автоматизированной системе

Kaspersky KUMA

Мера реализуется в части:

- Настройки аудита с помощью групповой политики на устройстве Windows путем отслеживания «Аудита входа в систему» и «Аудита событий входа в систему».

- Настройка политики аудита на устройстве Windows путем отслеживания «Аудита входа в систему» и «Аудита событий входа в систему».

УПД.9 Ограничение числа параллельных сеансов доступа

Для реализации данной меры используются встроенные механизмы защиты информации, а также данную меру можно реализовать с помощью служб каталогов LDAP или Microsoft AD.

УПД.10 Блокирование сеанса доступа пользователя при неактивности

Для реализации данной меры используются встроенные механизмы защиты информации, а также СЗИ от НСД, системы контроля действий привилегированных пользователей.

УПД.11 Управление действиями пользователей до идентификации и аутентификации

Для реализации данной меры используются механизмы встроенной защиты информации и СЗИ от НСД.

УПД.12 Управление атрибутами безопасности

Для реализации данной меры используются встроенные механизмы защиты информации, а также данную меру можно реализовать с помощью служб каталогов LDAP или Microsoft AD.

УПД.13 Реализация защищенного удаленного доступа

Для реализации данной меры используются средства защиты информации для организации удалённого доступа.

УПД.14 Контроль доступа из внешних информационных (автоматизированных) систем

KICS for Nodes

Мера реализуется в части:

- проверки входящего сетевого трафика на наличие действий, характерных для сетевых атак, а также блокирования сетевой активности со стороны атакующих устройств с помощью задачи «Защита от сетевых угроз»;
- отслеживания статуса работы и контроля работы брандмауэра Windows с помощью задачи «Управление сетевым экраном».

KICS for Linux Nodes

Мера реализуется задачей «Управление сетевым экраном» в части осуществления контроля состояния встроенного межсетевого экрана ОС и предотвращения несанкционированного изменения его конфигураций.

KICS for Networks

Мера реализуется в части:

- мониторинг сетевых сессий, выявление неразрешенных сетевых сессий, в том числе с доступом из внешних информационных (автоматизированных) систем;
- обнаружения вторжений в сессиях, в том числе с доступом из внешних информационных (автоматизированных) систем.

???? ???????????

????????????????

ОПС.0 Разработка политики ограничения программной среды

Для реализации данной меры используются встроенные механизмы защиты информации.

ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения

KICS for Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей и групп пользователей к запуску программ с помощью задачи «Контроль запуска программ»;
- возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Формирование правил контроля запуска программ» и сохранения данного перечня в XML-файл.

KICS for Linux Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей к запуску программ с помощью задачи «Контроль приложений»; возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Инвентаризация».

ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения

KICS for Nodes

Мера реализуется в части отслеживания и ограничения возможности пользователей и групп пользователей по установке программ с помощью задачи «Контроль запуска программ».

KICS for Linux Nodes

Мера реализуется в части отслеживания и ограничения возможности пользователей по установке программ с помощью задачи «Контроль приложений».

KICS for Networks

Мера реализуется в части выполнения контроля конфигураций установленных компонентов программного обеспечения путем сравнения их перечня с перечнем разрешенных процессов (эталонная конфигурация) и выявления отклонения от разрешенных значений.

Kaspersky Security Center

Мера реализуется в части:

- автоматизации установки и централизованного управления программными продуктами АО «Лаборатория Касперского»;
- возможности удаленной установки программ на защищаемые устройства с установленным агентом администрирования;
- возможности централизованного просмотра реестра программ на узлах с установленным агентом администрирования.

ОПС.3 Управление временными файлами

Для реализации данной меры используются встроенные механизмы защиты информации.

???? ?????? ??????????
????????????? ??????????????

ЗНИ.0 Разработка политики защиты машинных носителей информации

Для реализации данной меры выполняется разработка нормативных внутренних документов, регламентирующих правила пользования машинными носителями для сотрудников субъекта КИИ.

ЗНИ.1 Учет машинных носителей информации

Данное требование реализуется при помощи организационных мер, реализуемых путем выполнения положений внутренних руководящих документов Субъекта КИИ.

KICS for Nodes

Мера реализуется в части контроля использования внешних USB-устройств и подключаемых по USB CD/DVD-дисководов, а также формированию перечня "Доверенных устройств" с помощью задачи «Контроль устройств»

Kaspersky Security Center

Kaspersky Security Center предоставляет базовые возможности для учёта программного обеспечения и оборудования:

- Позволяет просматривать информацию о подключенных жестких дисках, носителях через отчеты и инвентаризацию;
- Позволяет настроить мониторинг подключенных носителей и генерации соответствующих событий;
- Позволяет настроить мониторинг подключения съемных носителей и генерации соответствующих событий;
- Позволяет настроить политики в KSC для ограничения использования съёмных носителей, если это необходимо.

Для реализации меры ЗНИ.1 KSC необходимо комбинировать с специализированными СЗИ (такими как Secret Net Studio или Dallas Lock) для полноценного учёта и контроля машинных носителей.

ЗНИ.2 Управление физическим доступом к машинным носителям информации

Данное требование реализуется при помощи организационных мер, реализуемых путем выполнения положений внутренних руководящих документов Субъекта КИИ.

ЗНИ.3 Контроль перемещения машинных носителей информации за пределы контролируемой зоны

Данное требование реализуется при помощи организационных мер, реализуемых путем выполнения положений внутренних руководящих документов Субъекта КИИ.

ЗНИ.4 Исключение возможности несанкционированного чтения информации на машинных носителях информации

Для реализации данной меры используются средства контроля съемных носителей информации, а также физическое ограничение доступа к портам ввода-вывода.

ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации

KICS for Nodes

Мера реализуется в части:

- регистрации и контроля использования внешних USB-устройств и подключаемых по USB CD/DVD-дисководов с помощью задачи «Контроль устройств»;
- формирования списка разрешающих правил для подключения флеш-накопителей и других внешних устройств на основе данных операционной системы обо всех внешних устройствах, которые ранее подключались к защищаемому устройству, с помощью задачи «Формирование правил контроля устройств».

KICS for Linux Nodes

Мера реализуется в части управления доступом пользователей к устройствам, которые установлены на клиентском устройстве или подключены к нему (например, жестким дискам, камерам или модулям Wi-Fi) с помощью задачи «Контроль устройств».

ЗНИ.6 Контроль ввода (вывода) информации на машинные носители

Для реализации данной меры используются средства контроля съемных носителей информации, а также физическое ограничение доступа к портам ввода-вывода.

ЗНИ.7 Контроль подключения машинных носителей информации

KICS for Nodes

Мера реализуется в части:

- регистрации и контроля использования съемных машинных носителей информации с помощью задачи «Контроль устройств»;
- формирования списка разрешающих правил для подключения съемных машинных носителей информации на основе данных операционной системы обо всех внешних устройствах, которые ранее подключались к защищаемому устройству, с помощью задачи «Формирование правил контроля устройств».

KICS for Linux Nodes

Мера реализуется в части управления доступом пользователей к съемным машинным носителям информации с помощью задачи «Контроль устройств».

ЗНИ.8 Уничтожение (стирание) информации на машинных носителях информации

??? ?????????? ?????? ??? ? ????????????????? ?????????? ?????????? ?????????????
????????????, ????????????????????? ?????????? ?????????????? (?????????) ?????????? ?? ??????????
????????????, ? ?????? ??? ?? ??? ? ?????????? ?????????????? ??????????????

???? ?????? ??????????????????
????????????????? ??? ??

АУД.0 Разработка политики аудита безопасности

Для реализации данной меры разрабатываются внутренние нормативные документы.

АУД.1 Инвентаризация информационных ресурсов

KICS for Nodes

Мера реализуется в части:

- возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Формирование правил контроля запуска программ» и сохранения данного перечня в XML-файл;
- возможности автоматизированного формирования перечня подключенных устройств с помощью задачи «Формирование правил контроля устройств» и сохранения данного перечня в XML-файл.

Kaspersky Endpoint Agent

Мера реализуется в части передачи в KICS for Networks данных телеметрии, включающих сведения об узле, на котором установлено Kaspersky Endpoint Agent.

KICS for Linux Nodes

Мера реализуется в части возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Инвентаризация».

KICS for Networks

Мера реализуется в части инвентаризации активов в АСУ ТП следующими способами:

- контроль активов с формированием таблицы устройств по сведениям об устройствах из трафика, поступающего через точки мониторинга, а также по сведениям от узлов с установленным Kaspersky Endpoint Agent;
- импорта в KICS for Networks результатов сканирования портативным сканером KICS for Nodes Portable;
- контроль оборудования на промышленных устройствах;

- контроль оборудования на Windows- и Linux-устройствах;
- контроль пользователей на устройствах;
- контроль приложений и патчей на устройствах;
- контроль рисков по данным из трафика (в том числе обнаружение уязвимостей устройств по сведениям об устройствах);
- проведение активных опросов устройств для получения наиболее точной и полной информации об устройствах и их конфигурациях с помощью методов активных опросов устройств как по протоколам прикладного уровня, так и по протоколам общего применения;
- карта сетевых взаимодействий по данным из трафика, поступающего через точки мониторинга, с возможностью просматривать сведения о взаимодействиях устройств в различные периоды времени;
- топологическая карта, на которой представлены устройства из таблицы устройств и соединения, добавленные по результатам активных опросов коммутаторов или вручную;
- мониторинг сетевых сеансов с формированием таблицы сетевых сеансов.

Kaspersky Security Center

Мера реализуется в части:

- обнаружения активных узлов в сети;
- регистрации сведений об устройствах, включая реестр программ и оборудования;
- регистрации сведений о программах и патчах, установленных на устройствах.

АУД.2 Анализ уязвимостей и их устранение

KICS for Nodes

Мера реализуется в части защиты памяти процессов от эксплуатации уязвимостей с помощью задачи «Защита от эксплойтов».

KICS for Nodes Portable

Мера реализуется в части поиска уязвимостей на узле с помощью задачи аудита безопасности с использованием встроенной Базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, базы OVAL-описаний из Банка данных уязвимостей ФСТЭК России или пользовательских баз OVAL-правил.

Kaspersky Endpoint Agent

Мера реализуется в части в части поиска уязвимостей на узле с помощью задачи аудита безопасности с использованием Базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, базы OVAL-описаний из Банка данных уязвимостей ФСТЭК

России или пользовательских баз OVAL-правил.

KICS for Networks

Мера реализуется в части:

- поиска уязвимостей на узле с помощью задачи аудита безопасности с использованием Базы данных уязвимостей Kaspersky ICS CERT для АСУ ТП, базы OVAL-описаний из Банка данных уязвимостей ФСТЭК России или пользовательских баз OVAL-правил;
- определения уязвимостей промышленных устройств в рамках функциональности «Контроль рисков» с учетом известных сведений об устройствах: производитель аппаратной части, модель аппаратной части, версия аппаратной части, производитель ПО, название ПО, версия ПО.

Kaspersky Security Center

Мера реализуется в части:

- централизованного сбора информации об уязвимостях на контролируемых узлах с помощью задачи «Поиск уязвимостей и требуемых обновлений»;
- централизованного закрытия уязвимостей в программах на управляемых устройствах с операционными системами Windows с помощью задачи «Закрытие уязвимостей».

АУД.3 Генерирование временных меток и (или) синхронизация системного времени

Для реализации данного требования нужно использовать сервера NTP, а также приемников ГЛОНАС/GPS.

АУД.4 Регистрация событий безопасности

KICS for Nodes

Мера реализуется в части регистрации событий в журналах в консоли KICS for Nodes:

- журнал выполнения задачи содержит информацию о текущем состоянии задачи и событиях, возникших за время ее выполнения;
- журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Industrial CyberSecurity for Nodes;
- журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве.

KICS for Linux Nodes

Мера реализуется в части:

- регистрации событий и отчетов в графическом пользовательском интерфейсе;
- регистрации событий безопасности в журнале событий приложения /var/opt/kaspersky/kics/private/storage/events.db;
- регистрации событий безопасности в журнале операционной системы (syslog).

KICS for Networks

Мера реализуется в части:

- регистрации событий и инцидентов, выявленных в сетевом трафике, а также полученных от KICS for Linux Nodes и KICS for Nodes (через Kaspersky Endpoint Agent);
- формирования отчетов о событиях безопасности (отчет о безопасности системы);
- регистрации сообщений программы;
- регистрации действий пользователей в журнале системного аудита.

Kaspersky Security Center

Мера реализуется в части регистрации событий безопасности, полученных от KICS for Nodes, KICS for Linux Nodes, KICS for Networks. KSC позволяет гибко настраивать параметры регистрации событий, включая выбор типов событий, уровней важности и сроков хранения.

KUMA

Мера реализуется в части сбора событий из различных источников. Обеспечивает сквозной цикл регистрации событий безопасности: от сбора и нормализации до анализа и интеграции с регуляторами. Ключевые преимущества — высокая производительность, поддержка отечественных стандартов (ФСТЭК, ГосСОПКА) и глубокие возможности аналитики через ИИ.

АУД.5 Контроль и анализ сетевого трафика

KICS for Nodes

Мера реализуется в части:

- проверки входящего сетевого трафика на предмет действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз»;

- отслеживает попытки подключения защищаемого устройства к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям Wi-Fi с помощью задачи «Контроль Wi-Fi».

АУД.6 ?????? ?????????? ? ????????? ??????????????

KICS for Nodes

Мера реализуется в части защиты доступа к функциям KICS for Nodes с помощью [пароля](#).

KICS for Linux Nodes

Мера реализуется в части реализации [ролевой модели управления доступом](#) к KICS for Linux Nodes.

KICS for Networks

Мера реализуется в части реализации ролевой [модели управления доступом](#) к веб-интерфейсу KICS for Networks.

Kaspersky Security Center

Мера реализуется в части реализации ролевой [модели управления доступом](#) к веб-консоли Kaspersky Security Center.

АУД.7 Мониторинг безопасности

KICS for Networks

Мера реализуется в части:

- [мониторинга безопасности](#) в онлайн-режиме в разделе «[Мониторинг](#)» через веб-интерфейс KICS for Networks;
- [мониторинга событий безопасности](#) и инцидентов в разделе «[События](#)» через веб-интерфейс KICS for Networks

KICS for Nodes

Мера реализуется в части:

- мониторинга статуса защиты узла и событий безопасности, выявленных по различным технологиям, через локальную консоль KICS for Nodes в журналах соответствующих компонентов (постоянная защита, контроль запуска программ и др.);
- мониторинга [статуса защиты узла](#) и [статистики событий безопасности](#) через диагностическое окно KICS for Nodes;
- обнаружения признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках кибератак, путем анализа журналов Windows с помощью задачи «[Анализ журналов](#)».

Kaspersky Security Center

Мера реализуется в части отображения веб-виджетов о состоянии безопасности на [панели мониторинга](#) и [формирования отчетов](#) о состоянии безопасности.

АУД.8 ??????????? ?? ???? ??? ??????????? ??????? ?????????????

KICS for Nodes

Мера реализуется в части регистрации событий в журналах KICS for Nodes. [Журнал событий](#) содержит информацию о событиях, которые нужны для диагностики сбоев в работе KICS for Nodes.

KICS for Linux Nodes

Мера реализуется в части регистрации событий приложения KICS for Linux Nodes в [журнале событий](#) приложения и журнале операционной системы (syslog).

АУД.9 Анализ действий пользователей

KICS for Nodes

Мера реализуется в части возможности сортировки событий в [журнале событий безопасности](#) и [журнале системного аудита](#) по имени пользователя в локальной консоли KICS for Nodes.

KICS for Linux Nodes

Мера реализуется в части возможности фильтрации событий при отображении в [командной строке](#) с помощью [логических выражений](#).

Kaspersky Security Center

Мера реализуется в части возможности фильтрации событий на узле при отображении в интерфейсе web-консоли Kaspersky Security Center.

АУД.10 ?????????? ?????????? ????????

KICS for Nodes Portable

Мера реализуется в части поиска уязвимостей на узле с помощью [задачи аудита](#) безопасности с использованием встроенных баз для оценки настроек операционных систем или пользовательских баз OVAL-правил.

KICS for Networks

Мера реализуется в части централизованного и автоматизированного аудита устройств на предмет соответствия встроенным или пользовательским базам OVAL-описаний с помощью функции «[Аудит безопасности](#)».

Kaspersky Security Center

Мера реализуется в части централизованного и автоматизированного аудита контролируемых узлов на предмет соответствия заданной базе OVAL-описаний с помощью задачи «[Аудит безопасности](#)».

АУД.11 ?????????? ?????????? ????????

Привлечение подрядных организаций для проведения аудита на соответствие требованиям.

???? ????????????????? ???? ?

AB3.0 Разработка политики антивирусной защиты

Для реализации данной меры разрабатываются внутренние нормативные документы.

AB3.1 Реализация антивирусной защиты

KICS for Nodes

Мера реализуется в части проверки устройств на базе ОС Windows с помощью задач «[Постоянная защита файлов](#)» и «[Проверка по требованию](#)» на предмет наличия вирусов и других программ, представляющих угрозу.

Под действие компонента «[Постоянная защита файлов](#)» попадают все объекты файловой системы и есть возможность настраивать уровни безопасности, а также предоставляется возможность исключить некоторые объекты из области действия.

Также, есть возможность обнаруживать и блокировать выполнение опасных и ли предположительно опасных скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например, скриптов VBScript или JScript, с помощью задачи [«AMSI-защита»](#).

Используются следующие способы обнаружения:

- Сигнатурный анализ вредоносных программ. База сигнатур – это список образцов кода известных вредоносных файлов. Если файл не соответствует ни одной записи в базе, то он не признается вредоносным по этой технологии. Полноценная база, где у каждого известного вредоносного или зараженного файла есть отдельная запись, требует слишком много места, поэтому база сигнатур – это оптимизированный список, уменьшенный до размера, который можно загрузить на компьютер. Каждая запись идентифицирует семейство похожих угроз.
- Эвристический анализ (эмуляция выполнения). Помогает обнаруживать полиморфные вредоносные файлы, которые меняют свой код во время выполнения и которые из-за этого сложно обнаружить по сигнатурам. Постоянная защита файлов запускает исполняемые файлы в специальной изолированной среде и ждет, не изменится ли код в памяти так, что начнет соответствовать сигнатуре.
- Проверка по базе данных Kaspersky Security Network. Постоянная защита файлов посылает в KSN контрольную сумму файла и получает ответ, есть ли такой файл в базе KSN и какая у него репутация. База KSN – это база контрольных сумм всех известных АО «Лаборатория Касперского» файлов. В этом списке есть файлы с репутацией «недоверенные» и «доверенные». Эта репутация файлов используется для принятия решения о файле.

KICS for Nodes Portable

Мера реализуется в части проверки устройств на базе ОС Windows на предмет наличия вирусов и других программ, представляющих угрозу. Результаты (отчет, подозрительные файлы в архиве с паролем) проверки сохраняются на том же USB-носителе.

Kaspersky Endpoint Agent

Мера реализуется в части сканирование YARA с помощью пользовательских YARA-файлов для поиска сигнатур вредоносной активности на устройствах. Сканирование выполняется рекурсивно на локальных дисках. Сканирование сетевых, подключаемых и облачных ресурсов не поддерживается.

KICS for Linux Nodes

Мера реализуется в части проверки устройств на базе ОС Linux с помощью компонентов «[Защита от файловых угроз](#)», «[Анализ поведения](#)», задачи «[Поиск вредоносного ПО](#)», «[Проверка важных областей](#)», «[Проверка съемных дисков](#)», «[Проверка контейнеров](#)» на предмет наличия вирусов и других программ, представляющих угрозу.

Используются следующие способы обнаружения:

- Сигнатурный анализ вредоносных программ. База сигнатур – это список образцов кода известных вредоносных файлов. Если файл не соответствует ни одной записи в базе, то он не признается вредоносным по этой технологии. Полноценная база, где у каждого известного вредоносного или зараженного файла есть отдельная запись, требует слишком много места, поэтому база сигнатур – это оптимизированный список, уменьшенный до размера, который можно загрузить на компьютер. Каждая запись идентифицирует семейство похожих угроз.
- Эвристический анализ (эмуляция выполнения). Помогает обнаруживать полиморфные вредоносные файлы, которые меняют свой код во время выполнения и которые из-за этого сложно обнаружить по сигнатурам. Постоянная защита файлов запускает исполняемые файлы в специальной изолированной среде и ждет, не изменится ли код в памяти так, что начнет соответствовать сигнатуре.
- Проверка по базе данных Kaspersky Security Network. Постоянная защита файлов посылает в KSN контрольную сумму файла и получает ответ, есть ли такой файл в базе KSN и какая у него репутация. База KSN – это база контрольных сумм всех известных АО «Лаборатория Касперского» файлов. В этом списке есть файлы с репутацией «недоверенные» и «доверенные». Эта репутация файлов используется для принятия решения о файле.

KICS for Linux Nodes Portable

Мера реализуется в части проверки устройств на базе ОС Linux на предмет наличия вирусов и других программ, представляющих угрозу. Результаты (отчет, подозрительные файлы в архиве с паролем) проверки сохраняются на том же USB-носителе

АВЗ.2 Антивирусная защита электронной почты и иных сервисов

Для реализации данной меры нужно использовать средства защиты для электронных почтовых систем, средства защиты веб-шлюзов.

АВЗ.3 Контроль использования архивных, исполняемых и зашифрованных файлов

KICS for Nodes

Мера реализуется в части проверки устройств на базе ОС Windows с помощью задач «[Постоянная защита файлов](#)» и «[Проверка по требованию](#)» на предмет наличия вирусов и других программ, представляющих угрозу. В задаче «[Проверка по требованию](#)» осуществляется проверка архивов ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и других архивов. Приложение проверяет архивы не только по расширению, но и по формату. При проверке архивов приложение выполняет рекурсивную распаковку. Это позволяет обнаруживать угрозы внутри многоуровневых архивов (архив внутри архива).

[Контроль запуска программ](#) позволяет контролировать запуск исполняемых файлов.

KICS for Linux Nodes

Мера реализуется в части антивирусной проверки архивных и исполняемых файлов с помощью компонентов «[Защита от файловых угроз](#)», «[Анализ поведения](#)», задачи «[Поиск вредоносного ПО](#)», «[Проверка важных областей](#)», «[Проверка съемных дисков](#)», «[Проверка контейнеров](#)» на предмет наличия вирусов и других программ, представляющих угрозу.

АВЗ.4 Обновление базы данных признаков вредоносных компьютерных программ

KICS for Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Linux Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

АВЗ.5 Использование средств антивирусной защиты различных производителей

KICS for Nodes

Мера реализуется в соответствии с описанием АВЗ.1 при установке совместно с антивирусным программным обеспечением стороннего производителя.

KICS for Linux Nodes

Мера реализуется в соответствии с описанием АВЗ.1 при установке совместно с антивирусным программным обеспечением стороннего производителя.

???? ??????????????
????????? (????????????
?????)

СОВ.0 Разработка политики предотвращения вторжений (компьютерных атак)

Для реализации данной меры разрабатываются внутренние нормативные документы.

СОВ.1 Обнаружение и предотвращение компьютерных атак

KICS for Nodes

Мера реализуется в части проверки входящего сетевого трафика на узле на предмет действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз».

KICS for Linux Nodes

Мера реализуется в части проверки входящего сетевого трафика на узле на предмет действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз».

Мера реализуется в части проверки входящего сетевого трафика, передаваемого по протоколам HTTP, HTTPS и FTP, веб-сайтов и IP-адресов с целью предотвращения загрузки вредоносных файлов из Интернета, а также блокирования доступа к фишинговым, рекламным и прочим опасным веб-сайтам с помощью компонента «Защита от веб-угроз».

KICS for Networks

Мера реализуется в части обнаружения вторжений с использованием встроенных и пользовательских [правил обнаружения вторжений](#).

Также применяются следующие [дополнительные методы](#) для обнаружения вторжений:

- обнаружения признаков подмены адресов в ARP-пакетах (ARP-спуфинг);
- обнаружения аномалий в протоколе TCP;
- обнаружения аномалий в протоколе IP;
- Обнаружение атак подбора и сканирования.

СОВ.2 Обновление базы разрешающих правил

KICS for Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Linux Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Networks

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

Kaspersky Security Center

Мера реализуется в части:

- централизованного автоматизированного обновления баз и модулей программного обеспечения АО «Лаборатория Касперского»;
- централизованного автоматизированного поиска обновлений программ сторонних производителей; при этом любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий АО «Лаборатория Касперского». Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение

???? ??????????
???????????

ОЦЛ.0 Разработка политики обеспечения целостности

Для реализации данной меры разрабатываются внутренние нормативные документы.

ОЦЛ.1 Контроль целостности программного обеспечения

Требование реализуется встроенными механизмами обеспечения защиты информации операционных систем, прикладного программного обеспечения, программируемых логических контроллеров, активного сетевого оборудования и т.п. совместно с средствами защиты информации.

KICS for Nodes

Мера реализуется в части:

- отслеживания и при необходимости блокирования действий, выполненных с заданной областью, где располагаются файлы или папки, и с указанными ветвями и разделами реестра с помощью задачи «[Контроль целостности системы](#)»;
- получения данных и проверки целостности проектов программируемых логических контроллеров с помощью задачи «[Защита промышленной сети](#)».

KICS for Linux Nodes

Мера реализуется в части контроля целостности операционной системы защищаемого устройства в режиме реального времени и по требованию с помощью компонента «[Контроль целостности системы](#)» и задачи «Проверка целостности системы».

ОЦЛ.2 Контроль целостности информации

KICS for Nodes

Мера реализуется в части отслеживания и при необходимости блокирования действий, выполненных с заданными файлами или папками с помощью задачи «[Контроль целостности системы](#)».

KICS for Linux Nodes

Мера реализуется в части контроля целостности операционной системы защищаемого устройства в режиме реального времени и по требованию с помощью компонента «[Контроль целостности системы](#)» и задачи «Проверка целостности системы».

ОЦЛ.3 Ограничения по вводу информации в автоматизированную систему

Требование реализуется встроенными механизмами обеспечения защиты информации операционных систем, прикладного программного обеспечения, программируемых логических контроллеров, активного сетевого оборудования и т.п совместно с средствами защиты информации, такими как межсетевые экраны.

ОЦЛ.4 Контроль данных, вводимых в автоматизированную систему

KICS for Networks

Мера реализуется в части:

- [контроля параметров технологического процесса](#) (осуществляется контроль отслеживания технологического процесса, отслеживание параметров технологического процесса и системных команд, передаваемых в трафике промышленной сети);
- [выявления системных команд](#) в сетевом трафике.

ОЦЛ.5 Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях

KICS for Networks

Мера реализуется в части:

- [контроля параметров технологического процесса](#) (осуществляется контроль отслеживания технологического процесса, отслеживание параметров технологического процесса и системных команд, передаваемых в трафике промышленной сети);
- [выявления системных команд](#) в сетевом трафике.

ОЦЛ.6 Обезличивание и (или) деидентификация информации

Требование реализуется встроенными механизмами обеспечения защиты информации операционных систем, прикладного программного обеспечения, программируемых логических контроллеров, активного сетевого оборудования и т.п

???? ??????????
?????????

ОДТ.0 ?????????? ?????????? ?????????????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ОДТ.1 ?????????????? ?????????????????? ?????????????? ??????????

Для реализации данной меры разрабатываются внутренние нормативные документы, где проектируется отказоустойчивая архитектура. Настраивается резервирование каналов связи, внедряется резервирование технических средств и создаются отказоустойчивые конфигурации.

ОДТ.2 ?????????????????? ????????? ? ???????

Для реализации данной меры разрабатываются внутренние нормативные документы, где проектируется отказоустойчивая архитектура. Настраивается резервирование каналов связи, внедряется резервирование технических средств и создаются отказоустойчивые конфигурации.

ОДТ.3 ?????????? ?????????????????? ?????????????????? ????????? ? ???????

KICS for Nodes

Мера реализуется в части защиты от вредоносных действий с помощью задач «[Постоянная защита файлов](#)» и «[Проверка по требованию](#)».

KICS for Linux Nodes

Мера реализуется в части защиты от вредоносных действий с помощью задач «[Защита от файловых угроз](#)», «[Поиск вредоносного ПО](#)», «[Проверка важных областей](#)», «[Проверка съемных дисков](#)», «[Проверка контейнеров](#)».

KICS for Networks

Мера реализуется в части непрерывного пассивного мониторинга состояния и конфигураций сетевых и промышленных устройств. Обнаруживает в трафике [системные команды](#), переданные или полученные устройствами, которые участвуют в автоматизации технологического процесса. Оповещает об обнаруженных неразрешенных системных

командах и ситуациях, которые могут быть признаками нарушения безопасности промышленной сети.

Kaspersky Security Center

Мера реализуется с помощью утилиты «Удаленная диагностика клиентских устройств», позволяющей выполнять следующие функции:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки системной информации и параметров программы;
- загрузки журналов событий;
- создание файла дампа для программы;
- запуска диагностики и загрузки результатов диагностики;
- запуска и остановки программ.

ОДТ.4 ?????????? ??????????? ???????????

Мера реализуется разработкой организационных мер, описанных в положениях руководящих документов, а также использованием средств резервного копирования.

ОДТ.5 ??????????? ??????????? ????????????????? ???????????

Мера реализуется разработкой организационных мер, описанных в положениях руководящих документов, а также использованием средств резервного копирования.

ОДТ.6 ??????????? ??????????? ????????????????? ????????????? ????????????? ??? ?????????? ???????????

Мера реализуется утверждёнными организационно-распорядительными документами, которые предписывают регулярное резервное копирование файлов конфигурации программного обеспечения, хранение их копий и выполнение восстановительных работ при возникновении нештатных ситуаций.

???7 ????????????????? ????????????????????? ?????????

Мера реализуется на базе специализированной платформы виртуализации, кластерных ОС или отказоустойчивое оборудование.

???8 ????????????????? ?????????????????????

Для реализации требования организуется непрерывный мониторинг систем дежурным персоналом с применением системы мониторинга, а также заключаются соглашения об уровне обслуживания и договоры на предоставление каналов передачи данных.

KICS for Networks

Мера реализуется в части:

- [мониторинга безопасности](#) в онлайн-режиме в разделе «[Мониторинг](#)» через веб-интерфейс KICS for Networks;
- [мониторинга событий безопасности](#) и инцидентов в разделе «[События](#)» через веб-интерфейс KICS for Networks.

???? ?????? ??????????
???????? ? ???????

ЗТС.0 Разработка политики защиты технических средств и систем

Для реализации данной меры разрабатываются внутренние нормативные документы.

ЗТС.1 Защита информации от утечки по техническим каналам

Для реализации данной меры организационные и технические меры защиты информации, такими как технические средства защиты от утечки по техническим каналам.

ЗТС.2 Организации контролируемой зоны

Для реализации данной меры используются физический меры защиты, такие как организация пропускного и внутриобъектового режима (системы контроля и управления доступом).

ЗТС.3 Управление физическим доступом

Для реализации данной меры используются физический меры защиты, такие как организация пропускного и внутриобъектового режима (системы контроля и управления доступом).

ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Для реализации данной меры используются организационные меры, описанные в положениях внутренних руководящих документах.

ЗТС.5 Защита от внешних воздействий

Для реализации данной меры используются инженерно-технические средства охраны и системы бесперебойного питания.

ЗТС.6 Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации

Для реализации данной меры используются организационные меры.

???? ??????????

???????????????? ???? ??

УКФ.0 Разработка политики управления конфигурацией

Для реализации данной меры разрабатываются внутренние нормативные документы.

УКФ.1 Идентификация объектов управления конфигурацией

KICS for Nodes

Мера реализуется в части возможности создания и поддержки строгого реестра программного обеспечения, что и является фундаментом для конфигурационного управления при помощи задачи «[Контроль запуска программ](#)».

KICS for Linux Nodes

Мера реализуется в части возможности создания и поддержки строгого реестра программного обеспечения, что и является фундаментом для конфигурационного управления при помощи задачи «[Контроль приложений](#)».

KICS for Networks

Мера реализуется в части контроля установки неразрешенных приложений (не входящих в эталонную конфигурацию) в ходе выполнения [задачи контроля конфигурации устройств](#) периодически и по запросу пользователя.

Kaspersky Security Center

Мера реализуется в части

Мера реализуется в части возможности просмотра [реестра приложений](#), установленных на устройстве, а также просмотр состояние и статус устройств.

УКФ.2 Управление изменениями конфигурации

KICS for Nodes

Мера реализуется в части:

- возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «[Формирование правил контроля запуска программ](#)» и сохранения данного перечня в XML-файл для дальнейшего анализа изменений;
- возможности автоматизированного формирования перечня подключенных устройств с помощью задачи «[Формирование правил контроля устройств](#)» и сохранения данного перечня в XML-файл для дальнейшего анализа изменений.

KICS for Linux Nodes

Мера реализуется в части возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «[Инвентаризация](#)».

УКФ.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения

KICS for Nodes

Мера реализуется в части запрета запуска исполняемых установочных файлов и скриптов с помощью задачи «[Контроль запуска программ](#)».

KICS for Linux Nodes

Мера реализуется в части запрета запуска исполняемых установочных файлов и скриптов с помощью задачи «[Контроль приложений](#)».

KICS for Networks

Мера реализуется в части обнаружения установки неразрешенных приложений (не входящих в эталонную конфигурацию) в ходе выполнения [задачи контроля конфигурации устройств](#) периодически и по запросу пользователя.

Kaspersky Security Center

Мера реализуется в части:

- возможности просмотра [реестра приложений](#), установленных на устройстве;
- возможности удаленной деинсталляции неразрешенного приложения с помощью задачи «[Удаленная деинсталляция приложения](#)».

УКФ.4 Контроль действий по внесению изменений в конфигурацию АСУ ТП

KICS for Nodes

Мера реализуется в части контроля целостности проектов ПЛК с помощью задачи «[Защита промышленной сети](#)».

KICS for Networks

Мера реализуется в части:

- обнаружения и контроля изменений сведений об устройствах - KICS for Networks обновляет сведения об известных устройствах на основе полученных данных из трафика или от KEA и KICS for Linux Nodes; при выявлении изменений в сведениях об устройствах формируются события безопасности;
- [Контроль чтения и записи проектов ПЛК](#) в сетевом трафике и сравнения этой информации с ранее полученной информацией о проектах ПЛК;
- возможности выполнения задачи [контроля конфигурации устройств](#) периодически и по запросу пользователя и дальнейшего сравнения конфигурации устройства с эталонной; при выявлении отклонений конфигурации устройств от эталонной формируются события безопасности.

???? ?????????????? ??
????????????????? ???????????

ИНЦ.1 Разработка политики реагирования на компьютерные инциденты

Для реализации данной меры разрабатываются внутренние нормативные документы.

ИНЦ.1 Выявление компьютерных инцидентов

KICS for Nodes

Мера реализуется в части:

- обнаружения вредоносного кода с помощью задач «[Постоянная защита файлов](#)» и «[Проверка по требованию](#)».
- обнаружения действий, характерных для сетевых атак, с помощью задачи «[Защита от сетевых угроз](#)»;
- обнаружения попыток подключения защищаемого устройства к Wi-Fi и обнаружения попыток подключения неразрешенных устройств с помощью задачи «[Контроль устройств](#)»;
- обнаружения вредоносного шифрования сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств с помощью технологии «[Защита от шифрования](#)»;
- обнаружения попыток запуска неразрешенных программ с помощью задачи «[Контроль запуска программ](#)»;
- обнаружения соединений, неразрешенных в брандмауэре Windows с помощью задачи «[Сетевой экран](#)»;
- обнаружения попыток запуска вредоносных скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript, с помощью задачи «[AMSI-защита](#)»;
- обнаружения неразрешенных действий с заданными ветвями и разделами реестра Windows и обнаружения нарушения целостности заданных файлов и папок с помощью задачи «[Контроль целостности системы](#)»;
- обнаружения признаков нетипичного поведения в системе на основе анализа журналов ОС Windows с помощью задачи «[Анализ журналов](#)»;
- обнаружения попыток использования эксплойтов с помощью задачи «[Защита от эксплойтов](#)»;

- обнаружения нарушений целостности проектов ПЛК с помощью задачи «[Защита промышленной сети](#)».

KICS for Nodes Portable

Мера реализуется в части обнаружения вредоносного кода с помощью проверки на вирусы и другие программы, представляющие угрозу.

KICS for Linux Nodes

Мера реализуется в части:

- обнаружения вредоносного кода с помощью задач «[Защита от файловых угроз](#)», «[Поиск вредоносного ПО](#)», «[Проверка важных областей](#)», «[Проверка съемных дисков](#)», «[Проверка контейнеров](#)» и «[Анализ поведения](#)»;
- обнаружения действий, характерных для сетевых атак, с помощью задачи «[Защита от сетевых угроз](#)»;
- обнаружения вредоносного шифрования сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств с помощью технологии «[Защита от удаленного вредоносного шифрования](#)»;
- обнаружения попыток запуска неразрешенных программ с помощью задачи «[Контроль приложений](#)»;
- обнаружения попыток подключения неразрешенных устройств с помощью задачи «[Контроль устройств](#)»;
- обнаружения соединений, неразрешенных в брандмауэре Windows с помощью задачи «[Управление сетевым экраном](#)»;
- обнаружения нарушения целостности заданных файлов и директорий с помощью задачи «[Контроль целостности системы](#)»;
- обнаружения попыток доступа к фишинговым, рекламным и прочим опасным веб-сайтам и попыток загрузки вредоносных файлов с помощью задачи «[Защита от веб угроз](#)»;
- обнаружения попыток доступа к неразрешенным веб-ресурсам с помощью «[Веб-контроль](#)».

KICS for Linux Nodes Portable

Мера реализуется в части обнаружения вредоносного кода с помощью проверки на вирусы и другие программы, представляющие угрозу.

KICS for Networks

Мера реализуется в части обнаружения и регистрации событий по следующим [технологиям](#):

- *Контроль технологического процесса (DPI).*

По этой технологии регистрируются события, связанные с нарушениями технологического процесса (например, событие при превышении заданного значения температуры).

- *Контроль целостности сети (NIC).*

По этой технологии регистрируются события, связанные с целостностью промышленной сети или с безопасностью взаимодействий (например, событие при обнаружении взаимодействия устройств в промышленной сети по новому для этих устройств протоколу).

- *Обнаружение вторжений (IDS).*

По этой технологии регистрируются события, связанные с обнаружением в трафике аномалий, которые являются признаками атак (например, событие при обнаружении признаков ARP-спуфинга).

- *Контроль системных команд (CC).*

По этой технологии регистрируются события, связанные с обнаружением в трафике системных команд для устройств (например, событие при обнаружении неразрешенной системной команды).

- *Внешние системы (EXT).*

К этой технологии относятся инциденты, а также события, которые поступают в KICS for Networks от сторонних систем с использованием методов KICS for Networks API.

- *Контроль активов (AM).*

По этой технологии регистрируются события, связанные с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие при обнаружении нового IP-адреса у устройства).

- *Защита конечных устройств (EPP).*

По этой технологии регистрируются события об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

ИНЦ.2 Информирование о компьютерных инцидентах

KICS for Nodes

Мера реализуется в части регистрации событий безопасности, выявленных различными модулями KICS for Nodes, в [журнале безопасности](#) в локальной консоли.

KICS for Linux Nodes

Мера реализуется в части возможности просмотра информации о событиях, возникающих в работе приложения, в следующие журналы:

- Журнал событий приложения. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kics/private/storage/events.db. Вы можете [настраивать параметры журнала событий приложения](#) в командной строке.
- Журнал операционной системы (syslog). По умолчанию журнал операционной системы не используется. Вы можете [включить запись событий в этот журнал](#).

Информацию о событиях приложения можно получать следующими способами:

- [В Консоли администрирования и в Web Console](#).
- [В командной строке](#).
- Если вы используете [графический пользовательский интерфейс](#) KICS for Linux Nodes – во всплывающих окнах приложения.

KICS for Nodes Portable

Мера реализуется в части возможности просмотра общего отчета о проверке узла.

KICS for Linux Nodes Portable

Мера реализуется в части возможности просмотра общего отчета о проверке узла.

KICS for Networks

Мера реализуется в части регистрации событий безопасности, выявленных различными модулями KICS for Networks, в разделе «[События](#)» в веб-интерфейсе, а также отправка уведомлений о событиях безопасности по электронной почте, SIEM и API.

Kaspersky Security Center

Мера реализуется в части отправки информации о событиях безопасности по электронной почте и SMS, а также SIEM.

ИНЦ.3 Анализ компьютерных инцидентов

KICS for Nodes

Мера реализуется в части предоставления детальной информации о событиях безопасности в [журнале безопасности](#) в локальной консоли.

KICS for Linux Nodes

Мера реализуется в части предоставления детальной информации о событиях безопасности в журнале безопасности.

KICS for Networks

Мера реализуется в части:

- возможности выгрузки рсар-файла с записью трафика по событию;
- предоставления информации о событии безопасности в разделе «[События](#)»;
- предоставление [графа событий](#) по EDR-инциденту.

Kaspersky Security Center

Мера реализуется в части предоставления информации о событиях безопасности на защищаемом устройстве, а также предоставления информации [по выборке событий](#), полученных от заданного приложения с заданного набора устройств за установленный интервал времени.

ИНЦ.4 Устранение последствий компьютерных инцидентов

KICS for Nodes

Мера реализуется в части:

- лечения (способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных) или удаления зараженных файлов с помощью задач «[Постоянная защита файлов](#)» и «[Проверка по требованию](#)»;
- [помещения на карантин](#) возможно зараженных файлов;
- блокирования запуска зараженных и возможно зараженных файлов с помощью задачи «[Постоянная защита файлов](#)»;
- запрета запуска неразрешенных программ и исполняемых файлов с помощью задачи «[Контроль запуска программ](#)»;
- запрет подключения неразрешенных устройств с помощью задачи «[Контроль устройств](#)»
- запрета неразрешенных сетевых соединений с помощью задачи «[Управление сетевым экраном](#)»;
- запрета неразрешенных файловых операций с заданными файлами и папками с помощью задачи и запрета неразрешенных операций с ветвями и разделами реестра с помощью задачи «[Контроль целостности системы](#)»;
- блокирования выполнения скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript с помощью задачи «[AMSI-защита](#)»;
- защиты памяти процессов от использования эксплойтов с помощью задачи «[Защита от эксплойтов](#)»;

- блокирования подключений к неразрешенным Wi-Fi сетям с помощью задачи «[Контроль устройств](#)»;
- блокирования сетевых соединений при обнаружении сетевых атак с помощью задачи «[Защита от сетевых угроз](#)»;
- блокирования удаленных узлов при обнаружении от них попыток шифрования файлов на общих сетевых ресурсах с помощью задачи «[Защита от шифрования](#)».

KICS for Linux Nodes

- Мера реализуется в части:
 - лечения (способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных) или удаления зараженных файлов с помощью задач «[Защита от файловых угроз](#)», «[Поиск вредоносного ПО](#)», «[Проверка важных областей](#)», «[Проверка съемных дисков](#)», «[Проверка контейнеров](#)»;
- блокирования запуска зараженных и возможно зараженных файлов с помощью задачи «[Защита от файловых угроз](#)»;
- блокирования вредоносных приложений с помощью задачи «[Анализ поведения](#)»;
- запрета запуска неразрешенных программ и исполняемых файлов с помощью задачи
- «[Контроль приложений](#)»;
- запрет подключения неразрешенных устройств с помощью задачи «[Контроль устройств](#)»;
- запрета неразрешенных сетевых соединений с помощью задачи «[Управление сетевым экраном](#)»;
- запрета неразрешенных файловых операций с заданными файлами и папками с помощью задачи «[Контроль целостности системы](#)»;
- блокирования сетевых соединений при обнаружении сетевых атак с помощью задачи «[Защита от сетевых угроз](#)».

KICS for Nodes Portable

Мера реализуется в части возможности лечения и удаления зараженных и возможно зараженных файлов, выявленных в области сканирования.

KICS for Linux Nodes Portable

Мера реализуется в части возможности лечения и удаления зараженных и возможно зараженных файлов, выявленных в области сканирования.

KICS for Networks

Мера реализуется в части выполнения следующих действий по реагированию из интерфейса KICS for Networks:

- запрета запуска файлов;
- помещения файлов на карантин;
- сетевой изоляции устройства.

Kaspersky Security Center

Мера реализуется в части предоставления информации о событиях безопасности на защищаемом устройстве, а также предоставления информации [по выборке событий](#), полученных от заданного приложения с заданного набора устройств за установленный интервал времени. Также создания политик и формирования задач, например, запуск задач в [KICS for Nodes](#).

ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов

Организационные меры, реализуемые путем выполнения положений внутренних руководящих документов.

ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

KICS for Nodes

Мера реализуется в части предоставления возможности очистки журналов выполнения задач, системного аудита и безопасности только пользователям, имеющим права на управление KICS for Nodes.

KICS for Linux Nodes

Мера реализуется в части отсутствия функционала очистки журнала событий приложения KICS for Linux Nodes. Удаление и установка KICS for Linux Nodes производится пользователем с привилегиями администратора.

KICS for Networks

Мера реализуется в части отсутствия функционала очистки событий безопасности приложения KICS for Networks. Удаление и установка KICS for Networks, сброс до настроек по умолчанию производится пользователем с привилегиями администратора.

Kaspersky Security Center

Мера реализуется в части хранения событий безопасности, полученных от управляемых узлов, на сервере администрирования Kaspersky Security Center (или связанном с ним сервером СУБД). При этом права на удаление событий безопасности есть только у пользователей с ролями «Главный администратор» и «Администратор сервера

администрирования».

???? ???????????

???????????????? ???? ??

УКФ.0 ?????????? ?????????? ?????????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

УКФ.1 ?????????????? ?????????? ?????????? ??????????????

KICS for Nodes

Мера реализуется в части задачи «[Контроль устройств](#)» и идентифицирует подключенные USB-устройства и сетевые интерфейсы

KICS for Linux Nodes

Мера реализуется в части задачи «[Контроль устройств](#)» путем добавления устройства в список доверенных устройств по его идентификатору.

KICS for Networks

Мера реализуется в части Мера реализуется в части отслеживания конфигураций устройств в ходе выполнения задачи [контроля конфигурации](#) устройств периодически и по запросу пользователя.

Kaspersky Security Center

Мера реализуется в части:

- уникальной [идентификации](#) всех подключенных устройств по имени;
- запрета **изменения локальных настроек защиты** на конечных устройствах через политики, а также управления защитой устройств через политики.

УКФ.2 ?????????? ?????????? ??????????

KICS for Nodes

Мера реализуется в части:

- возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «[Формирование правил контроля запуска](#)

[программ](#)» и сохранения данного перечня в XML-файл для дальнейшего анализа изменений;

- возможности автоматизированного формирования перечня подключенных устройств с помощью задачи «[Формирование правил контроля устройств](#)» и сохранения данного перечня в XML-файл для дальнейшего анализа изменений.

KICS for Linux Nodes

Мера реализуется в части возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «[Инвентаризация](#)».

KICS for Networks

Мера реализуется в части сбора сведений о конфигурации устройств в АСУ ТП и формировании событий об их изменении следующими способами:

- [контроль активов](#) с формированием [таблицы устройств](#) по сведениям об устройствах из трафика, поступающего через точки мониторинга, а также по сведениям от узлов с установленным Kaspersky Endpoint Agent;
- импорта в KICS for Networks результатов сканирования портативным сканером KICS for Nodes Portable;
- [контроль оборудования на промышленных устройствах](#);
- [контроль оборудования на Windows- и Linux-устройствах](#);
- [контроль пользователей на устройствах](#);
- [контроль приложений и патчей на устройствах](#);
- проведение [активных опросов устройств](#) для получения наиболее точной и полной информации об устройствах и их конфигурациях с помощью методов активных опросов устройств как по протоколам прикладного уровня, так и по протоколам общего применения;
- [карта сетевых взаимодействий](#) по данным из трафика, поступающего через точки мониторинга, с возможностью просматривать сведения о взаимодействиях устройств в различные периоды времени;
- [топологическая карта](#), на которой представлены устройства из таблицы устройств и соединения, добавленные по результатам активных опросов коммутаторов или вручную;
- [мониторинг сетевых сеансов](#) с формированием таблицы сетевых сеансов.

Kaspersky Security Center

Мера реализуется в части:

- Примененная к устройству политика **блокирует** возможность изменения соответствующих локальных настроек на конечной точке;

- [обнаружения активных узлов в сети](#);
- регистрации [сведений об устройствах](#), включая реестр программ и оборудования;
- регистрации сведений о программах и [патчах](#), установленных на устройствах.

УКФ.3 ????????? (????????????) ?????? ?????????????? ? ???????????????
 ?????????????? ??????????????

KICS for Nodes

Мера реализуется в части запрета запуска исполняемых установочных файлов и скриптов с помощью задачи «[Контроль запуска программ](#)». Проверяет попытки пользователей запускать различные приложения и разрешает или запрещает запуск этих приложений.

KICS for Linux Nodes

Мера реализуется в части запрета запуска исполняемых установочных файлов и скриптов с помощью задачи «[Контроль приложений](#)».

KICS for Networks

Мера реализуется в части Мера реализуется в части обнаружения установки неразрешенных приложений (не входящих в эталонную конфигурацию) в ходе выполнения задачи [контроля конфигурации](#) устройств периодически и по запросу пользователя.

Kaspersky Security Center

Мера реализуется в части:

- возможности просмотра [реестра приложений](#), установленных на устройстве;
- возможности удаленного удаления неразрешенного приложения с помощью задачи «[Удаленная деинсталляция приложения](#)»;
- экспорта с управляемого устройства параметров Контроля приложений, настроенных правил и созданных категорий приложений и импорта на управляемое устройство параметров Контроля приложений, настроенных правил и созданных категорий приложений.

УКФ.4 Контроль действий по внесению изменений

KICS for Nodes

Мера реализуется в части контроля целостности проектов ПЛК с помощью задачи «[Защита промышленной сети](#)».

KICS for Networks

Мера реализуется в части:

- [обнаружения попыток чтения и записи проектов ПЛК](#) в сетевом трафике и сравнения этой информации с ранее полученной информацией о проектах ПЛК;
- возможности выполнения задачи [контроля конфигурации](#) устройств периодически и по запросу пользователя и дальнейшего сравнения конфигурации устройства с эталонной; при выявлении отклонений конфигурации устройств от эталонной формируются события безопасности.

Kaspersky Security Center

Мера реализуется в части запрета **изменения локальных настроек защиты** на конечных устройствах через политики.

???? ??????????

???????????????? ??????????????

?????????????

ОПО.0 ?????????? ?????????? ?????????? ?????????????? ?????????????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ОПО.1 ?????, ?????????? ?????????? ?????????????? ?????????????? ?????????????? ?? ??????????????
?????????????

KICS for Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Nodes Portable

Мера реализуется в части обновления собственных [антивирусных баз](#).

KICS for Linux Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Linux Nodes Portable

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Networks

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

Kaspersky Security Center

Мера реализуется в части централизованного автоматизированного [обновления баз и модулей программного обеспечения](#) АО «Лаборатория Касперского».

ОПО.2 ????????? ????????????? ????????????? ?????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ОПО.3 ????????????? ????????????? ????????????? ?????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ОПО.4 ????????????? ????????????? ????????????? ?????????????

KICS for Nodes

Мера реализуется в части [обновления собственных баз и программных модулей](#) KICS for Nodes.

KICS for Linux Nodes

Мера реализуется в части [обновления собственных баз и программных модулей](#) KICS for Linux Nodes.

KICS for Networks

Мера реализуется в части [обновления собственных баз и программных модулей](#).

Kaspersky Security Center

Мера реализуется в части централизованного автоматизированного [обновления баз и модулей программного обеспечения](#) АО «Лаборатория Касперского».

???? ?????????????

?????????????? ?? ?????????????

??????????????

ПЛН.0 ?????????? ?????????? ?????????????? ?????????????? ?? ?????????????? ??????
?????????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ПЛН.1 ??????????, ?????????????? ? ?????????????? ?????? ?????????????? ??
????????????? ?????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы. План должен содержать перечень конкретных мер защиты (ссылки на ЗИС, ИПО, ДНС и др.) с указанием:

- Конкретных действий (внедрить, настроить, обучить).
- Сроков выполнения (этапы, дата окончания).
- Ответственных исполнителей (должности/подразделения).
- Необходимых ресурсов (бюджет, оборудование).

ПЛН.2 ?????????? ?????????????? ?????????????? ?? ?????????????? ?????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы, а также:

- Рекомендуется выделить ответственную роль (отдел ИБ, ответственный за ИБ) для контроля обеспечения защиты информации.
- Рекомендуется вести «Журнал контроля выполнения Плана мероприятий по обеспечению защиты информации» с фиксацией статусов (не начато, в работе, выполнено, просрочено).
- Рекомендуется проводить анализ результатов контроля руководством. Отклонения должны вести к корректирующим действиям (перенос сроков, перераспределение ресурсов).

???? ?????????????? ?????????? ? ????????????? ??????????????

ДНС.0 ?????????? ?????????? ?????????????? ?????????? ? ?????????? ??????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ДНС.1 ?????????? ?????? ?????????? ? ?????????? ??????????

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов.

ДНС.2 ?????????? ? ?????????? ?????????? ?????????? ? ?????????? ??????????

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов.

ДНС.3 ?????????? ?????????????????? ???? ?????????? ? ?????????? ?????????????? ?? ??????? ????????????????? ?????????? ??????????

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов, а также использования систем хранения.

ДНС.4 ?????????????????? ?????????????? ??????????????, ?????????????? ?????????, ??????? ?????? ?? ??????? ?????????????????? ?????????? ??????????

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов, а также внедряются системы резервирования, кластеризация серверов, RAID-массивы.

ДНС.5 ?????????????? ?????????????? ?????????????????? ??? ?? ? ?????? ????????????????? ????????????? ??????????

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов, а также использования систем резервирования. Помимо прочего, рекомендуется:

- Разработать «План восстановления АСУ ТП».
- Определить приоритетность восстановления компонентов.
- Создать и регулярно обновлять «золотые образы» рабочих станций и серверов, конфигурации ПЛК.

**ДНС.6 ?????? ?????????? ?????????? ?????????? ? ?????????? ??? ?? ?????????????? ??
????????????? ??????????????????**

Для реализации данной меры используются организационные меры и разрабатываются положения внутренних нормативных документов, а также рекомендуется:

- Ввести обязательное составление «Акта расследования нештатной ситуации».
- В Акте фиксировать: причины, ущерб, принятые меры, корректирующие действия.
- Назначить ответственных за выполнение корректирующих действий и сроки.
- Регулярно проводить анализ эффективности всех мер ДНС.

???? ?????????????? ?
????????? ??????????

ИПО.0 ?????????? ?????????? ?????????????????? ? ?????????? ??????????

Для реализации данной меры разрабатываются внутренние нормативные документы.

ИПО.1 ?????????????????? ?????????? ? ? ?????????? ?????????????????? ?????????? ? ?
????????? ?????????????? ???????

Для реализации данной меры разрабатываются внутренние нормативные документы, а также используются платформы для повышения осведомленности персонала, например, [Kaspersky Automated Security Awareness Platform](#).

ИПО.2 ?????????? ?????????? ?????????? ?????????? ???????

Для реализации данной меры рекомендуется:

- Разработать программы обучения для разных категорий персонала, либо использовать решения по повышению осведомленности персонала, например, [Kaspersky Automated Security Awareness Platform](#).
- Создать «Руководство по безопасной работе» с практическими инструкциями.
- Организовать обучение: силами внутренних специалистов или привлекая подрядную организацию (аккредитованную в области ИБ), либо использовать [Kaspersky Automated Security Awareness Platform](#).

ИПО.3 ?????????? ?????????????????? ?????????? ? ?????????????? ? ? ?????????? ??????????????
???????

Для реализации данной меры рекомендуется:

- Проводить тренинги по реагированию на инциденты (обнаружение фишингового письма, действия при утечке).
- Организовывать учения с разбором различных сценариев кибератак.
- Привлекать подрядные организации для проведения тестовые тренировки для закрепления полученных навыков.

ИПО.4 ?????????? ?????????????????? ?????????? ? ? ?????????? ?????????????????? ??????????????
? ? ?????????? ?????????????? ???????

Для реализации данной меры рекомендуется:

- Проводить регулярное тестирование знаний (анкетирование, опросы, тесты).
- Анализировать статистику инцидентов ИБ, связанных с человеческим фактором.
- Привлекать подрядные организации для проведения независимого аудита осведомлённости (например, через тестовые фишинговые рассылки).