

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

???0 ?????????? ???????? ?????? ??????????????

Для реализации данной меры разрабатываются внутренние нормативные документы, которые описывают какие события регистрируются, как долго хранятся журналы, кто имеет к ним доступ и как проводится анализ.

???1 ?????????????????? ?????????????????? ??????????

KICS for Nodes

Мера реализуется посредством обеспечения следующих возможностей:

- автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Формирование правил контроля запуска программ» и его сохранения в XML-файл;
- автоматизированного формирования перечня подключённых устройств с помощью задачи «Формирование правил контроля устройств» и его сохранения 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 посредством автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Инвентаризация». Для каждого обнаруженного приложения предоставляются сведения о пути к файлу, его хеш-сумме и типе, а также категории, если она задана.

KICS for Networks

Инвентаризация активов АСУ ТП в KICS for Networks обеспечивается следующими функциями:

- выявление и контроль активов с формированием таблицы устройств на основе данных об устройствах, полученных из трафика через точки мониторинга, а также от узлов с установленным Kaspersky Endpoint Agent;
- импорт результатов сканирования, выполненного с помощью портативного сканера KICS for Nodes Portable;

- сбор сведений об оборудовании промышленных устройств, а также устройств под управлением Windows и Linux;
- сбор сведений о пользователях, приложениях и установленных патчах;
- оценка рисков на основе данных сетевого трафика, включая выявление уязвимостей устройств по сведениям об их характеристиках;
- активный опрос устройств для получения наиболее полной и точной информации об устройствах и их конфигурациях с использованием протоколов прикладного уровня и протоколов общего назначения;
- построение карты сетевых взаимодействий на основе трафика, поступающего через точки мониторинга, с возможностью просматривать сведения о взаимодействиях устройств за разные периоды времени;
- построение топологической карты, включающей устройства из таблицы устройств и соединения, выявленные при активном опросе коммутаторов или добавленные вручную;
- мониторинг сетевых сеансов с формированием таблицы сетевых сеансов;
- KICS for Networks фиксирует появление новых устройств, исчезновение старых, изменение конфигурации — это критически важно для актуализации инвентаря.

Kaspersky Security Center

Мера реализуется посредством следующих функций:

- автоматического сбора на каждом узле сведений об установленном программном обеспечении, аппаратных компонентах и подключённых периферийных устройствах;
- регистрации сведений об устройствах, включая данные об установленном программном обеспечении и оборудовании;
- учёта программ и обновлений, установленных на устройствах.

АУД.2 Анализ уязвимостей и их устранение

Мера АУД.2 «Анализ уязвимостей и их устранение» предполагает, что организация не только выявляет уязвимости, но и обеспечивает последовательное выполнение полного цикла работ: выявление уязвимостей, оценка связанных с ними рисков, устранение уязвимостей или применение компенсирующих мер, а также проверка результатов. Платформа KICS лишь частично покрывает данную меру.

KICS for Nodes

Мера реализуется в части защиты памяти процессов от эксплуатации уязвимостей с помощью задачи «Защита от эксплойтов». Компонент предотвращает эксплуатацию определённых типов уязвимостей в процессах, выполняемых на защищаемых узлах. При этом блокирование попыток эксплуатации не устраняет саму уязвимость, а лишь снижает риск её использования.

Для полного выполнения меры необходимо дополнить защиту следующими процессами и средствами: анализом уязвимостей операционных систем и программного обеспечения, оценкой рисков и приоритизацией исправлений, управлением обновлениями, а также документированием результатов повторной проверки.

KICS for Linux Nodes

Мера реализуется в части защиты памяти процессов от эксплуатации уязвимостей с помощью задачи «Защита от эксплойтов». Компонент предотвращает эксплуатацию определённых типов уязвимостей в процессах, выполняемых на защищаемых узлах. При этом блокирование попыток эксплуатации не устраняет саму уязвимость, а лишь снижает риск её использования.

Для полного выполнения меры необходимо дополнить защиту следующими процессами и средствами: анализом уязвимостей операционных систем и программного обеспечения, оценкой рисков и приоритизацией исправлений, управлением обновлениями, а также документированием результатов повторной проверки.

KICS for Nodes Portable

Выявление уязвимостей на узле в рамках меры выполняется с помощью задачи аудита безопасности. Для анализа используются встроенная база данных уязвимостей Kaspersky ICS CERT для АСУ ТП, база OVAL-описаний из Банка данных угроз (уязвимостей) ФСТЭК России или пользовательские базы OVAL-правил.

Kaspersky Endpoint Agent

В рамках меры поиск уязвимостей на узле выполняется с помощью задачи аудита безопасности. Для этого используются база данных уязвимостей Kaspersky ICS CERT для АСУ ТП, база OVAL-описаний из Банка данных уязвимостей ФСТЭК России либо пользовательские базы 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».

3.3. Требования к централизованному сбору информации об уязвимостях

Мера требует, чтобы все события безопасности в информационной системе имели точные, однозначные и синхронизированные временные метки. Это критически важно для корреляции событий, расследования инцидентов и юридической значимости журналов. Для реализации данного требования нужно использовать сервера NTP, а также приемников ГЛОНАС/GPS.

3.4. Требования к централизованному закрытию уязвимостей

Информационная система должна не только обеспечивать штатную работу, но и регистрировать все значимые события, связанные с безопасностью, включая попытки доступа, изменения конфигурации, запуск программ, подключение устройств и выявленные сетевые аномалии.

KICS for Nodes

Мера реализуется в части детальной регистрации событий безопасности непосредственно в журналах локальной консоли KICS for Nodes, которые обеспечивают прозрачность всех процессов на защищаемом узле:

- **Журнал выполнения задачи:** Содержит информацию о текущем состоянии задач (например, работа компонента **Постоянная защита файлов и других компонент**, обновление баз) и о всех событиях, возникших за время их выполнения. Это гарантирует аудируемость операционной деятельности средств защиты.
- **События компонента «Контроль запуска программ»:** Формирует детализированные события как об успешном запуске, так и о блокировке исполняемых файлов. Каждое такое событие в обязательном порядке содержит критически важные для расследования атрибуты: **полный путь к файлу, его хэш-сумму и имя пользователя**, инициировавшего действие.
- **Журнал системного аудита:** Содержит информацию о событиях, связанных с администрированием и управлением самим продуктом (например, изменение политик, вход в консоль, обновление компонентов). Это исключает возможность незаметного изменения настроек защиты.
- **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 обеспечения многоуровневого и отказоустойчивого журналирования событий безопасности на узлах под управлением ОС семейства Linux, что достигается за счет следующих механизмов:

- 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 ??????????? ?? ???? ??? ??????????? ??????? ?????????????

Требование предполагает, что при сбое — например, переполнении диска, остановке службы или потере связи — информационная система должна не просто прекратить запись журналов, а зафиксировать причину сбоя и оперативно уведомить администраторов, чтобы они могли принять необходимые меры.

KICS for Nodes

Мера реализуется за счет повышения отказоустойчивости подсистемы аудита и детализации локального журналирования.

KICS for Nodes ведет собственные защищенные [журналы событий](#), в которых фиксируются не только события безопасности — например, блокировки и запуски, — но и диагностические события, связанные с работой агента. К ним относятся ошибки инициализации драйверов, нарушения связи с сервером администрирования, сбои записи на диск и нештатное завершение процессов.

Журналы событий содержат коды ошибок, имена модулей и временные метки. Эти данные помогают администратору оперативно установить причину сбоя при регистрации событий и отличить программную ошибку от возможного злонамеренного воздействия.

KICS for Linux Nodes

Мера реализуется за счет интеграции с подсистемой журналирования операционной системы, что повышает надежность регистрации событий и сбоев.

Дублирование записей. События приложения KICS for Linux Nodes фиксируются как в

собственном [журнале событий](#), так и в системном журнале операционной системы — `syslog` или `systemd-journald`.

Даже если собственный журнал приложения станет недоступен, например из-за повреждения файла, сведения о нештатном завершении службы или ошибке драйвера сохранятся в системном журнале операционной системы (`syslog` или `systemd-journald`). Таким образом обеспечивается резервный канал регистрации критически важных событий.

АУД.9 Анализ действий пользователей

Для реализации меры информационная система должна обеспечивать не только сбор журналов событий, но и привязку событий безопасности к конкретным учетным записям пользователей. Также должны быть доступны средства для последующего поиска, фильтрации и анализа этих событий.

KICS for Nodes

Мера реализуется в части:

- Сортировка событий по имени пользователя: В локальной консоли KICS for Nodes администратор может отсортировать события в [журнале событий безопасности](#) и [журнале системного аудита](#) по полю «Имя пользователя». Это позволяет оперативно выявить все действия, совершенные конкретной учетной записью, без необходимости обращения к центральной консоли KSC.
- **Детализация действий:** Для каждого события отображается полный контекст: время, тип действия (запуск приложения, подключение устройства, сетевое соединение), результат (разрешено/заблокировано), путь к файлу или устройству.
- **Экспорт и передача данных:** Отфильтрованные и отсортированные события могут быть экспортированы для последующего анализа или передачи в группу реагирования на инциденты.

KICS for Linux Nodes

Мера реализуется в части возможности фильтрации событий при отображении в [командной строке](#) с помощью [логических выражений](#). Администратор может использовать командную строку для фильтрации событий безопасности с применением логических выражений (например, `AND`, `OR`, `NOT`, сравнения по полям).

Kaspersky Security Center

Kaspersky Security Center позволяет фильтровать события безопасности и формировать по ним отчёты, связывая события с конкретными учётными записями пользователей во всей инфраструктуре.

???10 ?????????? ?????????? ????????

Мера реализуется организационными процедурами: разработаны и утверждены Положение о внутреннем аудите, ежегодный План проверок, Программы (чек-листы) аудита, а также формы Акта и Плана корректирующих мероприятий.

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 с использованием компонента «[Аудит безопасности](#)», входящего в состав Kaspersky Industrial CyberSecurity for Networks. Система централизованно и в автоматизированном режиме проверяет сетевые устройства, ПЛК и узлы АСУ ТП на соответствие их конфигураций и версий программного обеспечения встроенным или пользовательским наборам описаний на языке OVAL (Open Vulnerability and Assessment Language).

Такой подход позволяет автоматизировать проверку соблюдения внутренних регламентов информационной безопасности, выявлять отклонения от эталонных конфигураций и уязвимости без существенного воздействия на технологический процесс. По результатам аудита формируются подробные отчёты о соответствии, которые могут использоваться в качестве доказательной базы при проведении внутренних и внешних проверок.

Kaspersky Security Center

Мера реализуется с помощью задачи «[Аудит безопасности](#)», которая обеспечивает централизованную и автоматизированную проверку контролируемых узлов на соответствие заданной базе описаний OVAL.

Запустить задачу можно только при наличии активного лицензионного ключа Kaspersky Industrial CyberSecurity for Nodes, включающего лицензионный объект ICS Audit.

???11 ?????????? ??????? ????????

Привлечение подрядных организаций для проведения аудита соответствия установленным требованиям.