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

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.

Revision #8
Created 21 September 2025 19:55:27 by Olga Sinotova
Updated 12 January 2026 15:27:57 by Olga Sinotova