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

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.

Revision #2
Created 9 January 2026 19:52:38 by Olga Sinotova
Updated 9 January 2026 20:44:43 by Olga Sinotova