

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

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

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

Для реализации данной меры необходимо разработать и утвердить регламент управления программной средой. В нём следует определить, кто и на каких основаниях согласует установку и запуск программного обеспечения, устанавливает требования к его проверке и контролирует их соблюдение. Также необходимо закрепить порядок оформления исключений, сроки их действия, ответственных за согласование и периодический пересмотр выданных разрешений.

???1 ?????????? ?????????? (?????????????) ?????????????? ??????????????

Мера предусматривает применение в информационной системе механизма контроля запуска программного обеспечения. Механизм должен предотвращать выполнение неавторизованных объектов, включая вредоносные и неразрешённые программы, исполняемые файлы, скрипты и библиотеки.

Реализация с помощью KICS for Nodes

В рамках меры используются следующие задачи:

- **«Контроль запуска программ»** — для отслеживания и ограничения возможности запуска программ пользователями и группами пользователей. Правила контроля позволяют определять, каким пользователям и группам разрешён запуск программного обеспечения. Администратор формирует и поддерживает перечень разрешённых объектов, в который могут включаться исполняемые файлы, библиотеки DLL и скрипты. После настройки политики контроля попытки запуска объектов, отсутствующих в перечне разрешённых, блокируются.
- **«Формирование правил контроля запуска программ»** — для автоматизированного составления перечня программ и исполняемых файлов, обнаруженных в системе, и сохранения этого перечня в XML-файл.

Для эффективной работы механизма необходимо регулярно актуализировать перечень разрешённых объектов, проверять корректность применяемых правил и контролировать события блокировки. Добавление нового программного обеспечения в перечень следует выполнять после проверки и согласования в установленном организацией порядке. При необходимости временного исключения из правил следует определить основание, срок действия и ответственных за его согласование и пересмотр.

Реализация с помощью KICS for Linux Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей к запуску программ с помощью задачи «Контроль приложений». Администратор формирует и поддерживает перечень разрешённых объектов, в который могут включаться исполняемые файлы и скрипты. После настройки политики контроля попытки запуска объектов, отсутствующих в перечне разрешённых, блокируются.;
- возможности автоматизированного формирования перечня программ и исполняемых файлов с помощью задачи «Инвентаризация».

2022.2 2022.2.22 2022.2.22 (2022.2.22) 2022.2.22 2022.2.22
 2022.2.22

Приказ ФСТЭК № 239 требует, чтобы в информационной системе были реализованы механизмы, предотвращающие несанкционированную установку ПО, ограничивающие круг лиц, имеющих право на установку, и контролирующие источники установки.

Реализация с помощью KICS for Nodes

В рамках меры используются следующие задачи:

- **«Контроль запуска программ»** — для отслеживания и ограничения возможности запуска программ пользователями и группами пользователей. Правила контроля позволяют определять, каким пользователям и группам разрешён запуск программного обеспечения. Также в компоненте присутствует возможность осуществлять Контроль пакетов установки.

Модуль «Контроль пакетов установки» использует отдельный список исключений. Добавление пакета в этот список присваивает ему статус доверенного: его распаковка разрешается, а установленным или обновлённым из него программам разрешается запускаться автоматически. Извлечённые файлы также могут наследовать доверенный статус родительского пакета.

Основным пакетом установки считается пакет, внесённый в список исключений и получивший статус доверенного.

- **«Формирование правил контроля запуска программ»** — для автоматизированного составления перечня программ и исполняемых файлов, обнаруженных в системе, и сохранения этого перечня в XML-файл.

KICS for Linux Nodes

В среде Linux установка ПО — это, по сути, запуск исполняемого файла (скрипта `.sh`, `.run`, бинарного файла) или вызов пакетного менеджера (`rpm`, `dpkg`, `apt`, `yum`). KICS for Linux Nodes контролирует именно эти действия

- Мера реализуется в части отслеживания и ограничения возможности пользователей по установке программ с помощью задачи «Контроль приложений».
- Компонент контроль целостности файлов осуществляет мониторинг критических системных каталогов (/bin, /sbin, /usr/bin, /opt). Если каким-то образом файл

был изменен или добавлен без ведома системы, KICS фиксирует это как инцидент нарушения целостности.

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.

???.3 ?????????? ?????????? ????????

Для реализации данной меры следует использовать встроенные средства защиты операционной системы и приложений. Необходимо ограничить права доступа к временным каталогам, настроить регулярную очистку и определить политики хранения и удаления временных файлов. При необходимости очистку можно автоматизировать с помощью централизованных сценариев, а выполнение установленных требований — контролировать средствами управления конечными устройствами. При настройке сроков хранения следует учитывать, что временные файлы могут быть необходимы для работы активных приложений.