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

АВ3.0 Разработка политики антивирусной защиты

Для реализации данной меры разрабатываются внутренние нормативные документы.

АВ3.1 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

АВ3.2 Антивирусная защита электронной почты и иных сервисов

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

АВ3.3 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 поверка 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.

АВ3.4 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.

АВ3.5 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.

Revision #4
Created 29 December 2025 15:28:41 by Olga Sinotova
Updated 14 January 2026 20:00:59 by Olga Sinotova