

????????????? ?????????????? KSC ??? Kaspersky Industrial CyberSecurity for Nodes (Windows)

Давайте начнем с определения, что такое Политика.

Политика — это набор параметров приложений «Лаборатории Касперского», которые применяются к группе администрирования и её подгруппам. Для каждого приложения в группе администрирования KSC хранит по одной политике. Мы будем рассматривать политику для KICS for nodes.

У политики есть статусы:

- **Активна** - Текущая политика, применяется к устройству. Для KICS for nodes в группе администрирования может быть активна только одна политика.
- **Неактивна** - Политика существует в папке «Политики», но не применяется. Её можно активировать в любой момент.

Важно:

- для KICS for nodes можно держать несколько политик с разными значениями, но активна — только одна;
- политика может иметь дочерние политики.

1. Для того, чтобы создать политику, нужно перейти в раздел "**Активы**" - > "**Политики и профили политик**". (проверьте, что установлен и синхронизирован **плагин управления** — без него KICS for Nodes не появится в окне «Выберите приложение» на шаге 4 мастера создания политики.)

[image.png](#)

2. Далее выберите группу администрирования, для которой нужна политика:

- для корневой группы — переходите сразу к следующему шагу;
- для подгруппы — нажмите на ссылку текущего пути вверху окна и выберите нужную подгруппу в открывшейся панели.

3. Нажмите **Добавить**. Откроется окно **Выберите приложение**.

4. Выберите **Kaspersky Industrial CyberSecurity for Nodes** из списка управляемых программ (программа должна быть представлена в консоли — то есть соответствующий плагин управления должен быть установлен и синхронизирован с сервером).

[image.png](#)

5. Нажмите **Далее**. Откроется окно параметров новой политики на вкладке **Общие**.

6. При необходимости измените имя политики, статус (активна / неактивна / для автономных пользователей) и параметры наследования.

7. Перейдите на вкладку **Параметры приложения** — либо нажмите **Сохранить**, чтобы выйти и вернуться к настройке позже (политика уже появится в списке).

8. В левой области вкладки «Параметры приложения» выбирайте разделы и настраивайте параметры — их набор специфичен для KICS for Nodes и в справке KSC не описан (см. раздел 5 ниже с пометкой источника).

9. Нажмите **Сохранить**.

Настроить политику можно как во время ее создания, так и после. Настройка политики осуществляется в разделе: **Активы (Устройства) → Политики и профили политик →** выбрать политику → **Параметры приложения**, где открывается список разделов, специфичных для продукта.

[image.png](#)

Для примера возьмем раздел **Постоянная защита файлов** и перейдем к разделу **Постоянная защита файлов** и нажимаем кнопку **Настройка** и переходим в раздел **Общие**.

[image.png](#)

Обратите внимание, что есть несколько режимов работы объекта. **Интеллектуальный режим** — программа сама решает, какие объекты проверять (обычно на основе анализа операций с файлом), в режиме «При открытии» осуществляется проверка на чтение, а «При открытии и изменении» осуществляется проверка на чтение, выполнение и изменение или «При выполнении» (проверка только при запуске на исполнение).

Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл). Мы можем

выбирать уровень работы данного функционала.

[image.png](#)

Также во многих компонентах есть дополнительные параметры, например, Запустить сканирование важных областей при обнаружении активного заражения, если этот параметр выключен, при обнаружении активного заражения программа не создаёт и не запускает дополнительную временную задачу проверки важных областей системы.

Обратите внимание на тумблер **Принудительно** - это означает, что данная политика применяется ко всем устройствам, на которых она распространяется. Локально на рабочем месте изменить его нельзя.

Далее перейдем в раздел область защиты и нажмем кнопку изменить. У нас появляются дополнительные параметры для настройки защищаемой области.

[image.png](#)

В этом разделе мы можем выбрать действия над обнаруженными объектами:

[image.png](#)

При первых использованиях рекомендуется выбирать режим **Только сообщать**. Далее как уже появится понимание, что настройки корректны и система работает штатно, то можно на узлах реального времени (HMI, серверы SCADA) выбирать уровень не выше «Рекомендуемого» и включать интеллектуальный режим — это снижает нагрузку на процессор по сравнению с проверкой «При открытии» для всех типов обращений.

В разделе **Управление задачей** мы можем настраивать запуск компонента.

Остальные компоненты настраиваются по аналогии.

Хочу обратить внимание на раздел **Контроль активности на компьютерах**. Обратим внимание на компоненты **Контроль запуска программ** и **Контроль устройств** и рассмотрим особенности настройки.

[image.png](#)

Переходим в раздел **Активы (Устройства) → Задачи** и нажимаем кнопку **Добавить**.

[image.png](#)

Далее необходимо настроить раздел Область применения разрешающих правил (исполняемые файлы, скрипты, пакеты MSI), также обратим внимания на чекбокс **Создавать разрешающие правила на основе запущенных программ**, при выборе которого правила сформируются на основе запущенных программ, в противном случае будет

сформирован список всего ПО, которое установлено на рабочем месте. Нажимаем далее и заполняем дополнительные настройки, на основании чего будут формироваться правила: сертификат, хеш SHA256, путь, аргументы командной строки; нужно минимум одно условие, иначе правило не будет добавлено. Далее настройте следующие параметры:

- **Добавлять разрешающие правила в список правил контроля запуска программ** — включите этот параметр, чтобы добавить созданные правила в список.
- **Принцип добавления** — выберите способ добавления правил.
- **Задайте полный путь к файлу с расширением .xml** — укажите путь для экспорта правил. После выполнения задачи «Формирование правил контроля запуска программ» Kaspersky Industrial CyberSecurity for Nodes сохранит разрешающие правила в XML-файл по указанному пути.
- **Добавлять информацию о защищаемом устройстве в имя файла** — включите этот параметр, чтобы добавить сведения об устройстве в имя файла.

Если требуется, на вкладке Исключения укажите объекты, которые хотите исключить из области действия задачи, например, разрешить запуск по пути `C:\Windows`, но исключить `Regedit.exe`.

При создании правил обязательно убедитесь, что они разрешают запуск приложений самой операционной системы — иначе можно случайно заблокировать системные процессы Windows.

Формирование правил контроля устройств формируется аналогичным образом.

Теперь вернемся к самой политике и активируем компонент Контроль запуска программ. Перед нами окно настройки, обратите внимание, что доступно два режима работы:

- **Только статистика** (значение по умолчанию) — правила не используются для запрета или разрешения запуска, программа только фиксирует события о срабатывании/несрабатывании условий правил. Запуск всех программ разрешён.
- **Активный** — правила реально регулируют запуск. Это блокирующая модель «запрещено всё, что явно не разрешено» — если программа не подпадает ни под одно правило, её запуск не разрешается.

Без предварительного формирования правил и прогона в режиме статистики переключение сразу в активный режим гарантированно остановит часть легитимного ПО.

[image.png](#)

На вкладке «Общие» параметров задачи задаётся, что именно контролируется:

- **Использовать правила для исполняемых файлов** — включает/выключает контроль запуска именно `.exe` и подобных исполняемых файлов. Если флажок снят, запуск исполняемых файлов не контролируется правилами вообще и разрешён безусловно, независимо от режима задачи.
- **Контролировать загрузку DLL-модулей** — отдельный флажок для контроля DLL.

- Контроль **скриптов и MSI-пакетов**: если выключен, их запуск/установка разрешены без проверки правилами.

В блоке использование KSN, обратите внимание, что этот компонент влияет и на Контроль запуска программ: репутационные данные могут использоваться при принятии решения о запуске. Критичный нюанс, который стоит держать в голове именно для этого компонента: **при включённой службе «Использование KSN», но отсутствии реального соединения с серверами KSN** (типично для изолированной промышленной сети без интернета), программа **игнорирует режим «Только статистика» и начинает блокировать запуск** — то есть поведение компонента незаметно меняется с безопасного наблюдения на блокирующее.

В разделе Правила загрузите созданные правила и выберете нужную для вас опцию:

[image.png](#)

Обратите внимание на раздел Контроль пакетов установки , который актуален для сценариев, где на узлах регулярно автоматически обновляется ПО. Это дополнительный список исключений: добавленный в него пакет установки становится доверенным, для него разрешена распаковка, а для программ, установленных или обновлённых из доверенного пакета, разрешается автоматический запуск.

KICS for nodes контролирует только полный цикл распространения — если при первом запуске пакета Контроль пакетов установки был выключен или не был установлен Контроль запуска программ, корректно обработать запуск изменённых файлов система не сможет.

Если на инженерных станциях используется автообновляемое специализированное ПО (например, самообновляющиеся инженерные пакеты от интегратора), включение Контроля пакетов установки избавит от необходимости пересоздавать правила после каждого обновления — вместо этого обновление просто проходит как доверенный пакет.

Revision #9

Created 30 September 2026 15:18:37 by Olga Sinotova

Updated 2 October 2026 11:04:27 by Olga Sinotova