Средство защиты информации

«Secure Pack Rus»

Версия 3.0

Руководство администратора безопасности

Политики управления приложениями

ЖТЯИ.00106-01 90 04

Листов 25

Компания «КРИПТО-ПРО»

2019

Компания «КРИПТО-ПРО», 2019. Все права защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании «КРИПТО-ПРО» этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании «КРИПТО-ПРО».

ООО «КРИПТО-ПРО»
Адрес 127018, г. Москва, ул. Сущевский Вал, дом 18
Телефон +7 (495) 995-4820
e-mail info@cryptopro.ru
Web www.cryptopro.ru

Оглавление

Список сокращений

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ЗПС	Замкнутая программная среда
ИС	Информационная система
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
СХКИ	Средство хранения конфиденциальной информации

1. Введение

Данное руководство предназначено для администраторов средства защиты информации «Secure Pack Rus» версия 3.0 (сокращенные названия изделия – Secure Pack Rus 3.0 или SPR 3.0). В руководстве содержатся сведения, необходимые администраторам для управления механизмами замкнутой программной среды.

2. Основные подсистемы

Функционирование СЗИ SPR 3.0 опирается на следующие подсистемы:

- Подсистема управления политиками;
- Подсистема доверенной аутентификации;
- Подсистема дискреционного разграничения доступа;
- Подсистема защиты критических ресурсов;
- Подсистема контроля доступа к устройствам;
- Подсистема мандатного шифрования;
- Подсистема замкнутой программной среды;
- Подсистема контроля запуска сценариев;
- Подсистема аудита безопасности.

Данное Руководство описывает порядок настройки следующих политик безопасности основных подсистем, реализуемых СЗИ SPR 3.0:

- Подсистема замкнутой программной среды.

Описание порядка настройки политик безопасности, не входящих в данное Руководство, содержится в соответствующих документах в составе документации (1), (2), (3) и (4).

3. Политика управления приложениями (AppLocker)

Политика управления приложениями позволяет администраторам ограничивать запуск пользователями нежелательных или ненадежных приложений на серверах и рабочих станциях, работающих как в сценарии домена, так и в рабочей группе.

Для применения политик управления приложениями (AppLocker) на АРМ необходимо наличие лицензии ОС уровня «Корпоративная» или «Максимальная». На АРМ с лицензией ОС уровня «Профессиональная» следует использовать политики ограниченного использования программ (SRP).

3.1. Настройка автоматического запуска службы

Для внедрения правил политики необходима работа службы удостоверения приложений (ApplicationIdentityService). По умолчанию служба удостоверений приложений не запускается автоматически.

3.1.1. Ручной запуск службы

Для настройки корректной работы службы удостоверений приложений на рабочей станции или сервере в режиме рабочей группы необходимо использовать диспетчер управления службами (ServiceControlManager), чтобы установить тип запуска для службы удостоверений приложений в автоматический режим, а затем запустить эту службу (Рисунок 1).

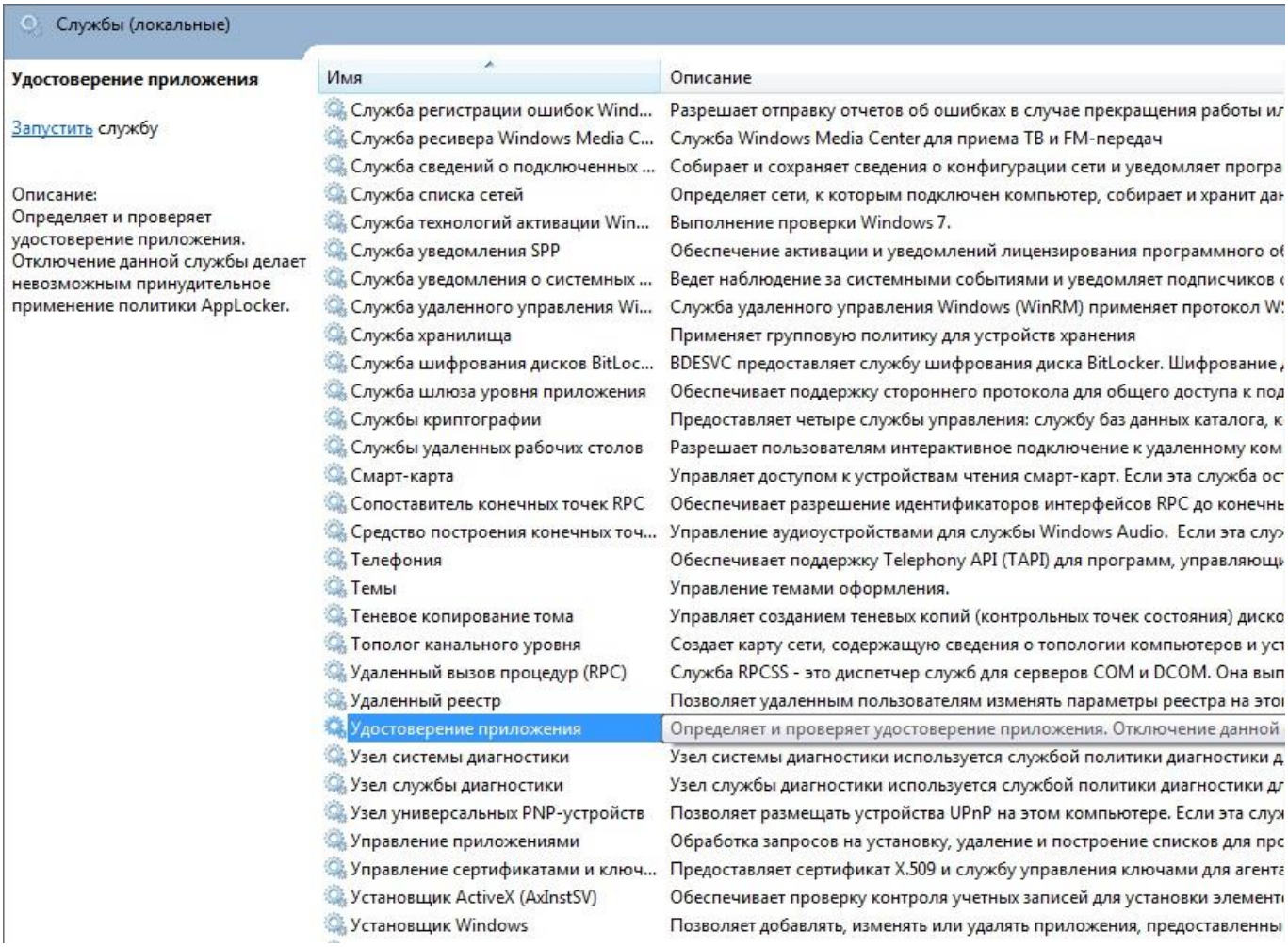

Рисунок 1 – Запуск службы идентификации приложений

При развертывании политики в домене предприятия для автоматизации запуска службы удобно использовать список системных служб на уровне групповой политики. Системные службы расположены по следующему пути: Конфигурация компьютера | Настройки Windows | Настройки безопасности | Системные службы в древе групповой политики.

3.1.2.Настройка групповой политики запуска службы

Управление политикой осуществляется через консоль редактора групповой\локальной политики безопасности: Конфигурация компьютера (ComputerConfiguration) | Настройки Windows (WindowsSettings) | Настройки безопасности (SecuritySettings) | Политики управления приложениями (ApplicationControlPolicies) | AppLocker (Рисунок 2).

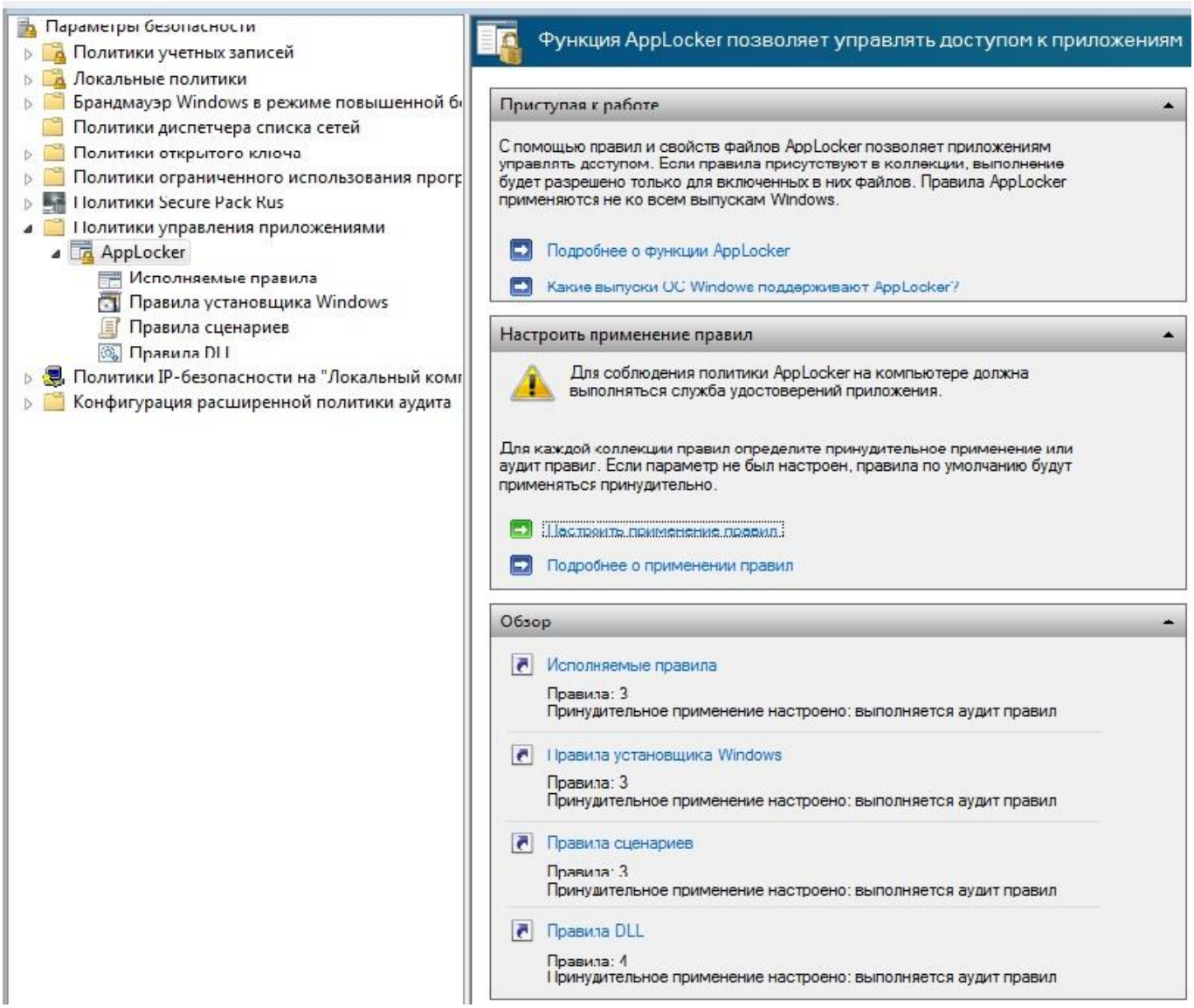

Рисунок 2 - Управление политикой

3.2. Инициализация коллекций правил

Для настройки политик необходимо выбрать пункт *“Настроить применение правил”*. Каждое правило может быть отнесено к одной из следующих коллекций (Рисунок **3**):

- правила исполняемых файлов;
- правила установщика Windows;
- правила сценариев;
- правила DLL.

Правила применяются объектам в соответствии с их маской:

- исполняемые файлы;
  «.exe», «.com»
- файлы установщика Windows;
  «.mst», «.msi», «.msp»
- сценарии;
  «.js», «.ps1», «.vbs», «.bat»
- DLL-файлы.
  «.dll»

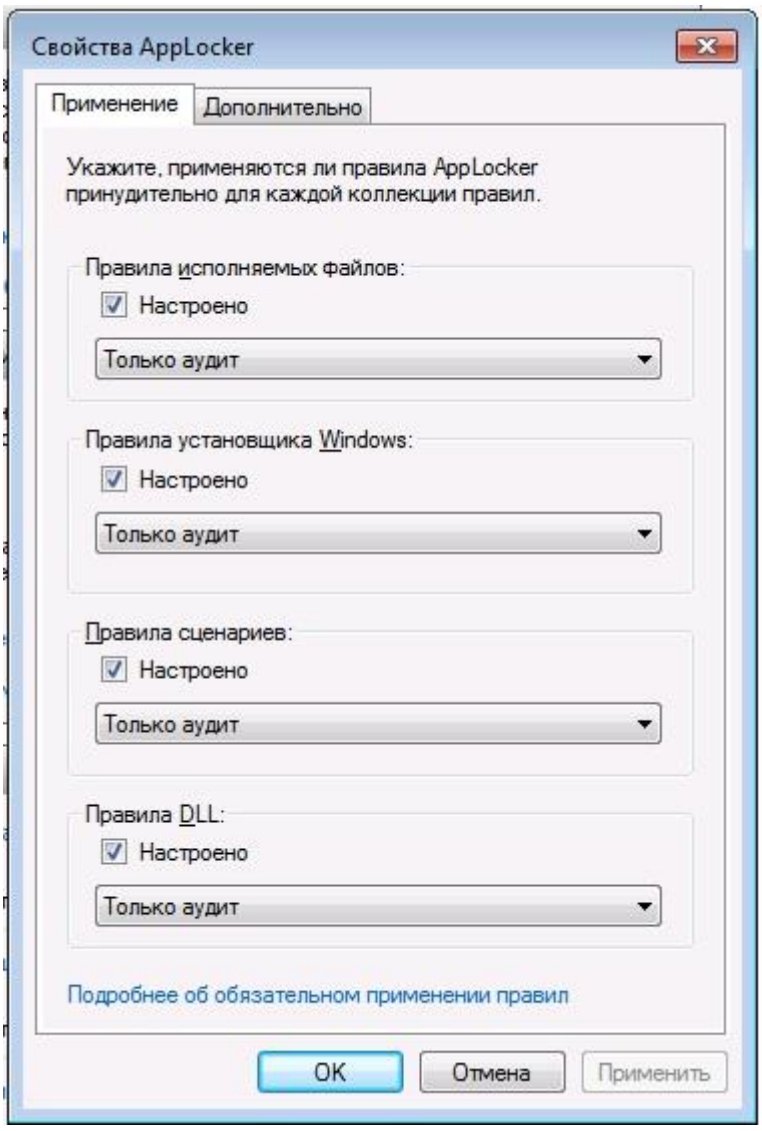

Рисунок 3 – Коллекции правил AppLocker

Правило коллекции DLL отключено по-умолчанию. Для включения отображения этой коллекции в общем списке необходимо открыть вкладку “*Дополнительно*” и отметить пункт “*Включить коллекцию правил DLL*” (Рисунок 4).

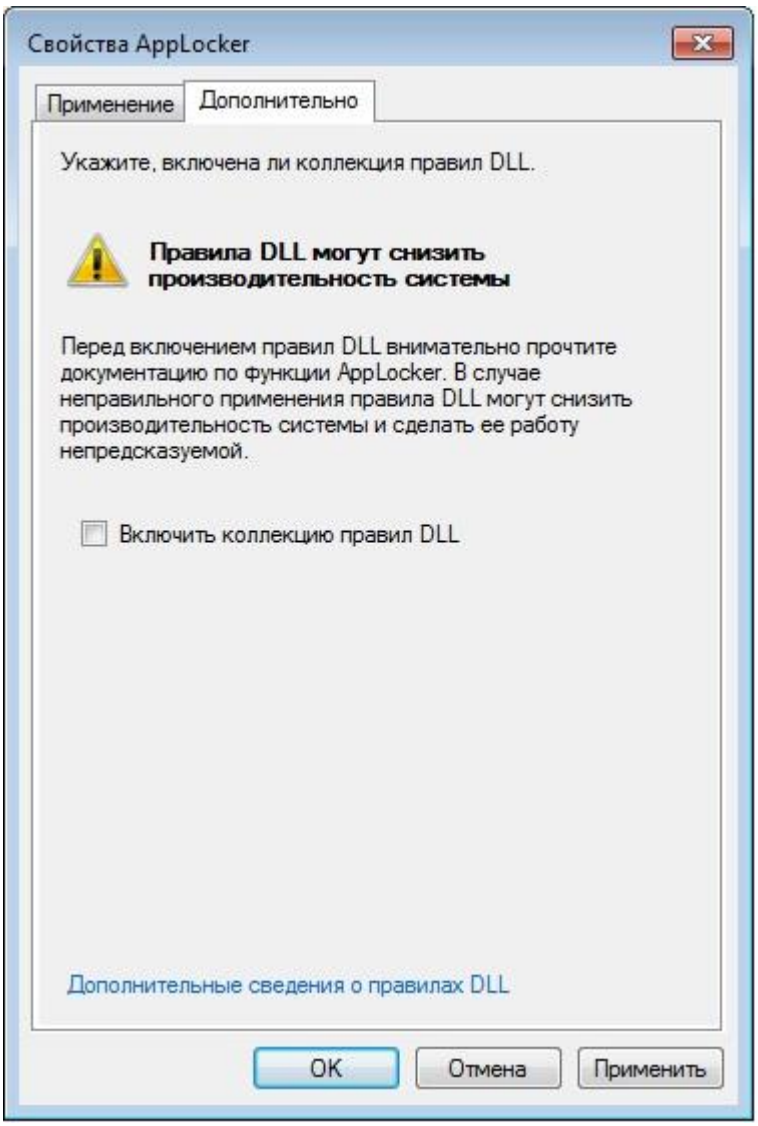

Рисунок 4 – Включение коллекции правил DLL

3.3. Перевод коллекций в режим аудита

Концепция использования политики управления приложениями заключается в применении политики запрещения запуска по умолчанию, что означает вероятность нарушения работы ОС и ее приложений в случае неверной настройки политики. Особенностью политики является ее безусловная работа при наличии хотя бы одного правила в списке правил коллекции, независимо от того, отмечен ли пункт “*Настроено*” для данной коллекции. Для минимизации рисков нарушения работы системы ввиду неверной настройки параметров политики необходимо первоначально явно включить все коллекции и задать правила работы по умолчанию, добавить правила разрешения запуска приложений, проверить журналы аудита на предмет корректности работы заданных правил, после чего включить штатный режим работы политики.

Для перевода политики в отладочный режим необходимо в окне списка коллекций отметить пункт “*Настроено*” и выбрать режим “*Только аудит*” для каждой коллекции из списка.

3.4. Создание правил политики в ручном режиме

По умолчанию список правил для каждой коллекции пуст и перед формированием разрешающих пользовательских правил необходимо сформировать правила политики по умолчанию: выполнить вход в каждую коллекцию правил и в меню “*Действия*” выбрать пункт *“Создать правила по умолчанию”.*

В каждой коллекции можно создать правила на основании трех критериев:

- правила для путей;
- правила для сертификата;
- хэш-правила.

Для создания правила в коллекции необходимо в меню “*Действия*” выбрать пункт *“Создать новое правило”.* Запуститься мастер создания правила. В разделе “*Разрешения*” указывается тип создаваемого правила (разрешить\запретить) и область его действия (пользователь\группа) (Рисунок 5). В разделе “*Условия*” задается критерий работы правила (путь\издатель\хэш-значение) (Рисунок 6). В случае использования в качестве критерия пути к файлу или подписи издателя возможно так же задать исключения, попадающие под общее описание правила, но не подлежащие его обработке (Рисунок 7). Механизм исключений позволяет расширить список разрешений через создание запрещающих правил с исключениями. Критерии для описания исключений совпадают с критериями для правил. В разделе “*Имя*” задается уникальное имя правила и его описание (Рисунок 8).

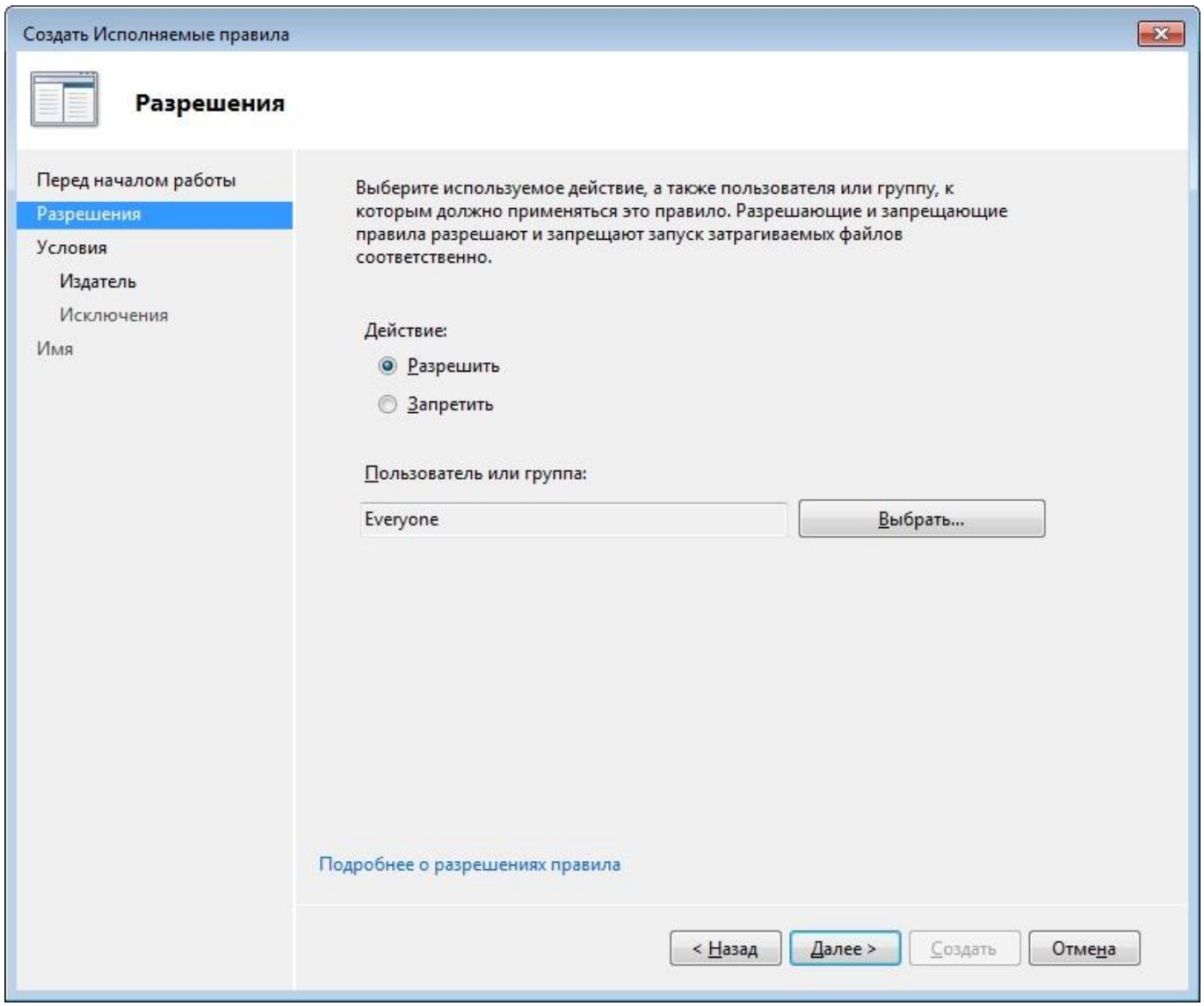

Рисунок 5 – Разрешения правила

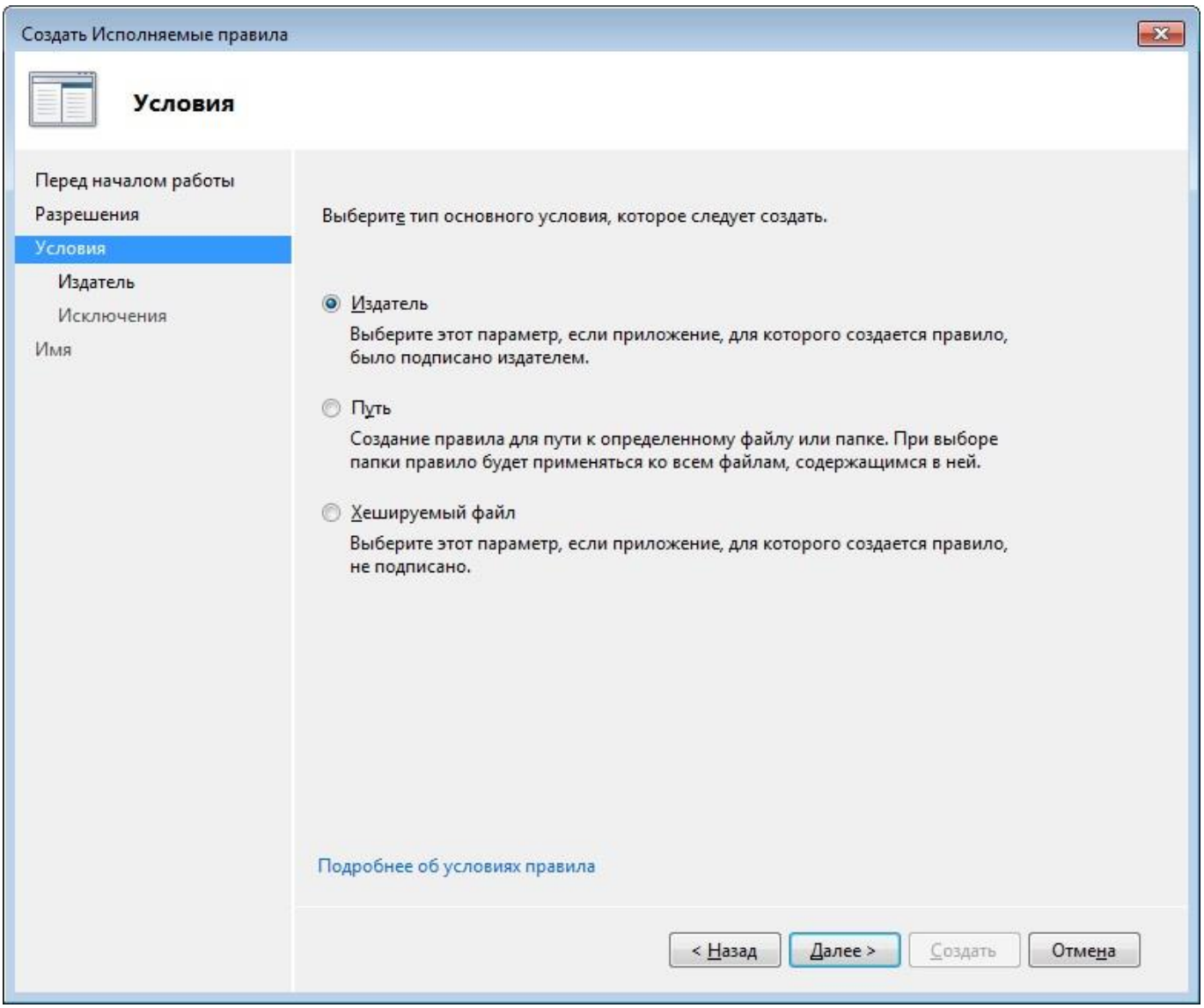

Рисунок 6 – Условия правила

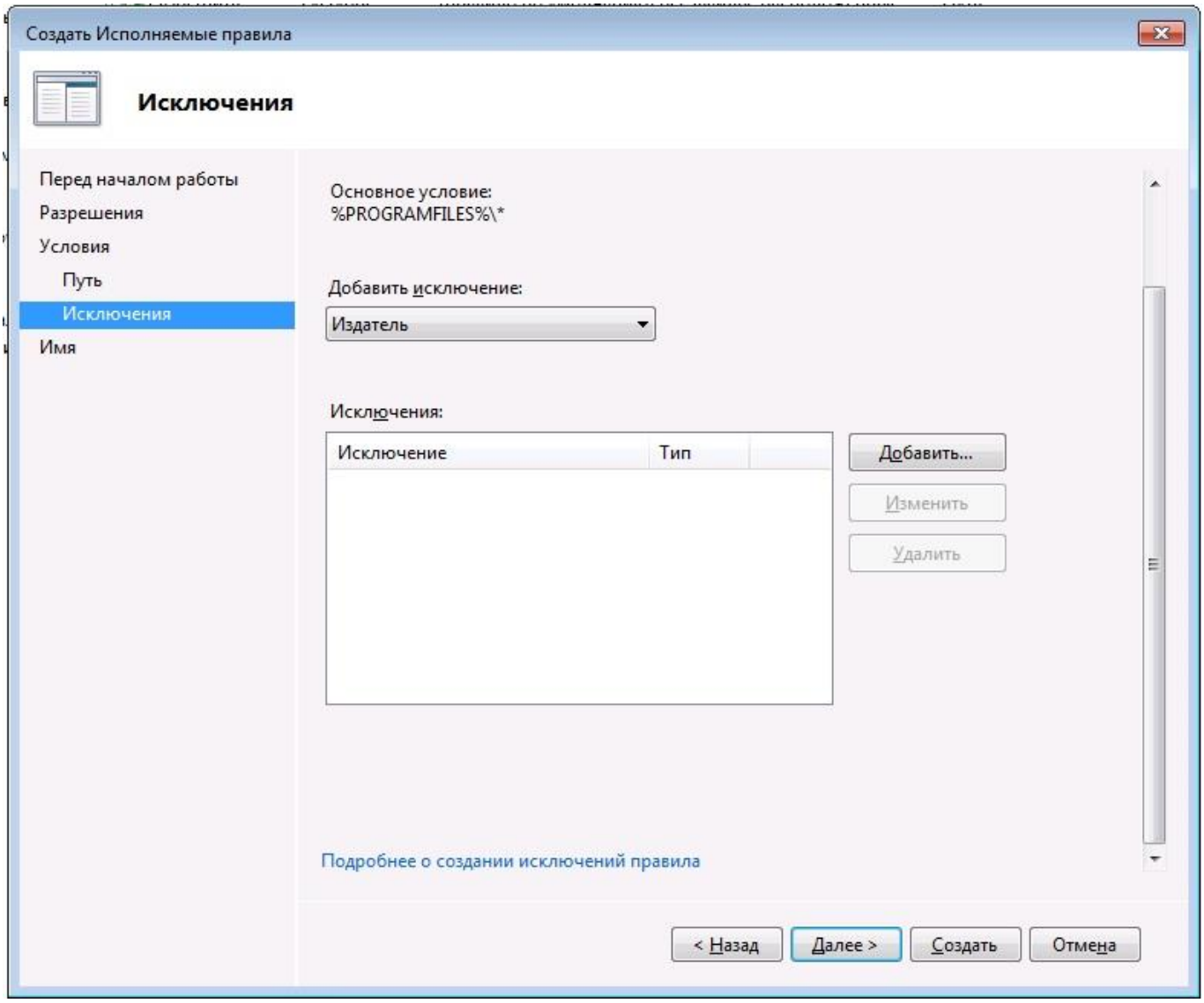

Рисунок 7 – Исключения правила

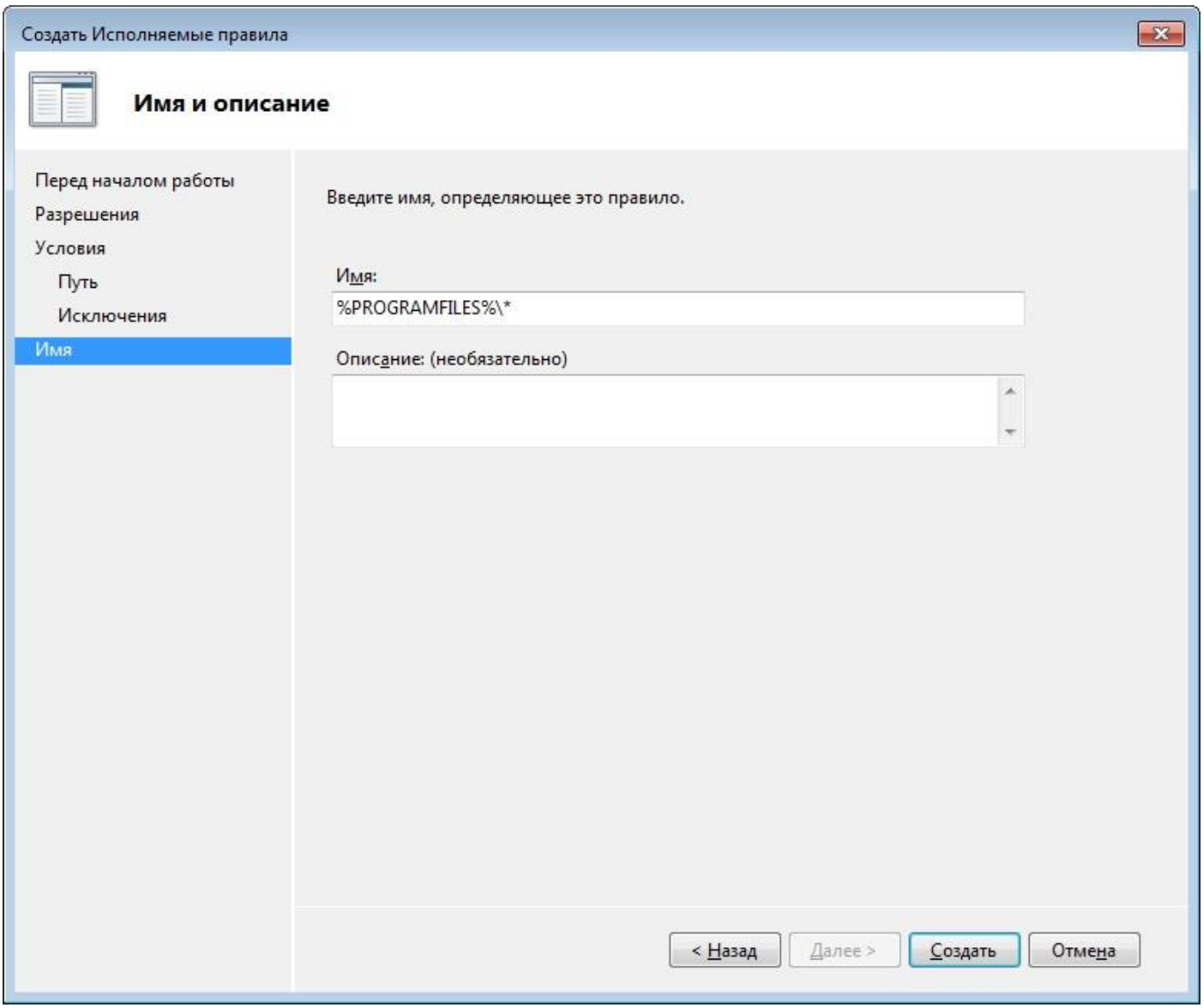

Рисунок 8 – Описание правила

3.5. Создание правил политики в автоматическом режиме

Для упрощения и автоматизации процесса создания правил политики управления приложениями возможно использование мастера автоматического создания правил. Для запуска мастера в коллекции необходимо в меню *“Действия”* выбрать пункт *“Создать правила автоматически”.* Мастер позволяет создавать правила для всех файлов в указанной папке на основании цифровой подписи, а в случае ее отсутствия, указывать в качестве параметра для файла путь к нему или его хэш-сумму. Кроме того, можно явно указать хэш-сумму файла в качестве параметра для создания правила (Рисунок 9). После завершения работы мастера будет выдана информация о количестве созданный правил и их типе (Рисунок 10).

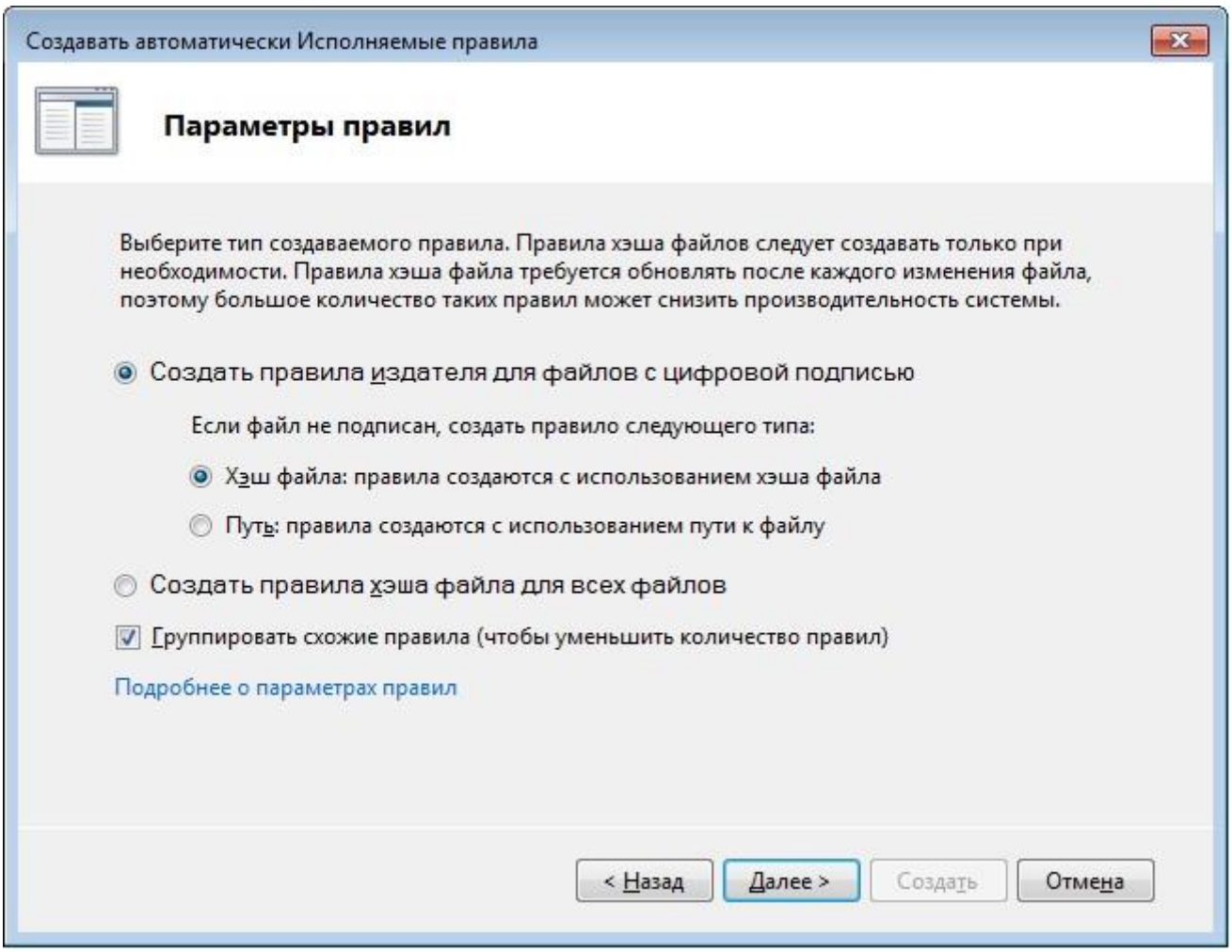

Рисунок 9 – Мастер автоматического создания правил

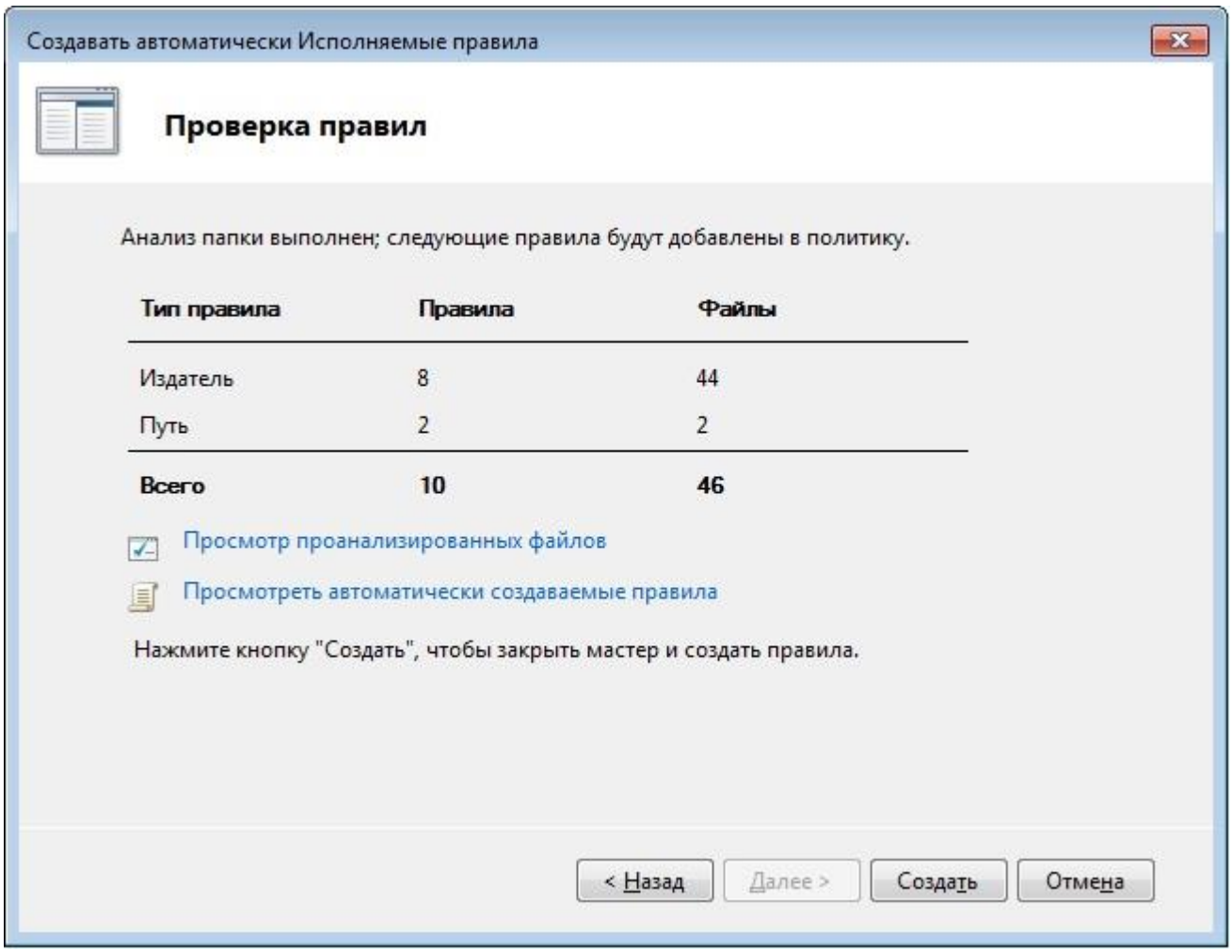

Рисунок 10 – Отчет о созданных правилах

3.6. Перевод коллекций в штатный режим работы

После создания правил политики и проверки корректности их работы в режиме аудита необходимо поменять режим работы политик на штатный: в окне списка для каждой коллекций выбрать режим “*Принудительное применение правил*” (Рисунок 3).

Более подробные сведения о настройке и описание функций политики управления приложениями см. (5).

3.7. Требования к базовым настройкам.

Базовые настройки политики управления приложениями должны включать следующие ограничения запуска:

- Исполняемые файлы
  1. Path - %PROGRAMFILES%* - everyone
  2. Path - %WINDIR%* - everyone
  3. Path - * - Administrators

- Установщики
  1. Publisher - Signed – everyone
  2. Path - %WINDIR%\Installer* - everyone
  3. Path - * - Administrators
- Запуск скриптов
  1. Path - %PROGRAMFILES%* - everyone
  2. Path - %WINDIR%* - everyone
  3. Path - * - Administrators

В дополнение к базовым настройкам, необходимо запретить для всех групп пользователей кроме Администраторов запуск следующих программ: %WINDIR%\system32\regsvr32.exe, %WINDIR%\system32\rundll32.exe, %WINDIR%\system32\subst.exe, %WINDIR%\system32\mklink.exe.

4. Политики ограниченного использования программ (SRP)

Политика ограниченного использования программ (SRP – SoftwareRestrictionPolicy) позволяет администраторам ограничивать запуск пользователями нежелательных или ненадежных приложений на серверах и рабочих станциях, работающих как в сценарии домена, так и в рабочей группе. Поставляется в составе операционной системы (ОС) начиная с Microsoft Windows 2000.

4.1. Настройка политик ограниченного использования программ

Управление политикой осуществляется через консоль редактора групповой\локальной политики безопасности: Конфигурация компьютера | Настройки Windows | Параметры безопасности | Политики ограниченного использования программ.

Для активации политики ограниченного использования программ необходимо вызвав меню выбрать пункт «Создать новые политики»(Рисунок 11).

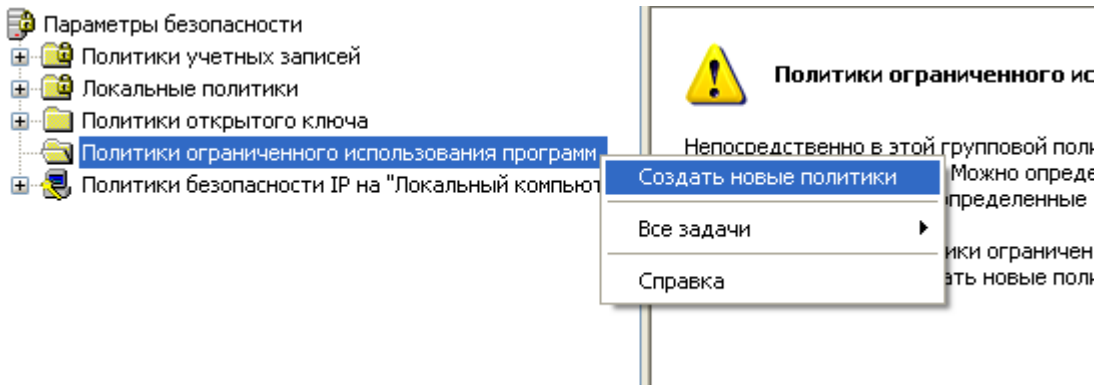

Рисунок 11 - Создание новой политики ограниченного использования программ

При создании политики она переходит в состояние «Неограниченный», то есть не запрещает ничего. Внутри консоли будет 5 объектов (Рисунок 12):

- **Уровни безопасности** – определяет основной уровень безопасности политики по умолчанию.
- **Дополнительные правила** – здесь задаются исключения для уровня по умолчанию.
- **Принудительный** – окно для выбора степени действия политики.
- **Назначенные типы файлов** – окно управления списком расширений файлов, которые проверяются правилом по умолчанию.
- **Доверенные издатели** – представляет настройки управления списками доверенных подписчиков для приложений и скриптов.

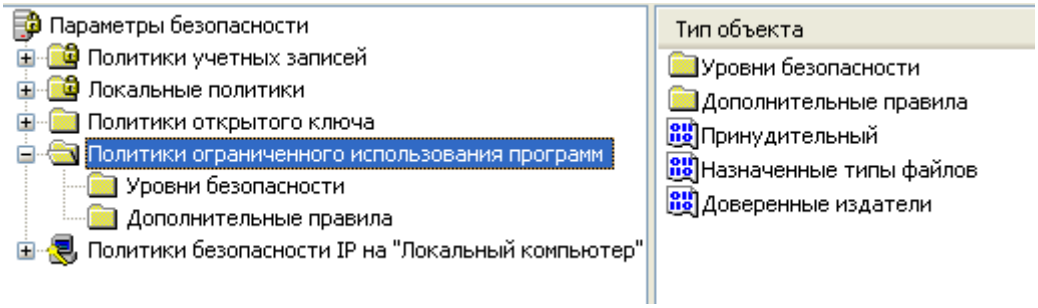

Рисунок 12 - Внешний вид консоли управления политикой

Сначала идет раздел «Уровни безопасности». Политики SRP имеют 2 уровня безопасности:

- **Не разрешено** – запрещено всё, кроме исключений в Дополнительных правилах.
- **Неограниченный** – разрешено всё, кроме исключений в Дополнительных правилах.

Далее идет раздел «Дополнительные правила». В этом разделе составляются все исключения для действия политики по умолчанию. Можно использовать следующие типы дополнительных правил с учётом порядка их применения (Рисунок 13):

- **Правило для сертификата** – правило для сертификатов. Данный тип правила используется только для подписанных приложений и скриптов. Можно разрешить или запретить запуск приложений, которые подписаны сертификатом определенного издателя, вне зависимости от их расположения.
- **Правило для хэша**– правило хэша. Для каждого приложения требуется создание отдельного правила. Можно разрешить или запретить запуск приложения по его хэшу. Данное правило полезно для защиты пользователей от запуска подмененных или инфицированных вирусом файлов, так как в обоих случаях хэш самого файла изменится и не подпадёт под правило хэша политики SRP и запуск его будет невозможен.
- **Правило для зоны Интернета** – правило зоны сети. В Windows реализовано несколько зон сети, как «Интернет», «Надежные узлы», «Ограниченные узлы» и «Местная интрасеть». Данный тип правил регулирует, какие установочные пакеты разрешены для скачивания исходя из условия их размещения.
- **Правило для пути** – правило пути. Правила данного типа позволяют указывать размещение приложений и файлов, которые будут разрешены или запрещены для запуска. По умолчанию уже созданы четыре разрешающих правила для системных папок. Благодаря этому приложения из данных папок будут разрешены для запуска, если не удалить правила вручную.

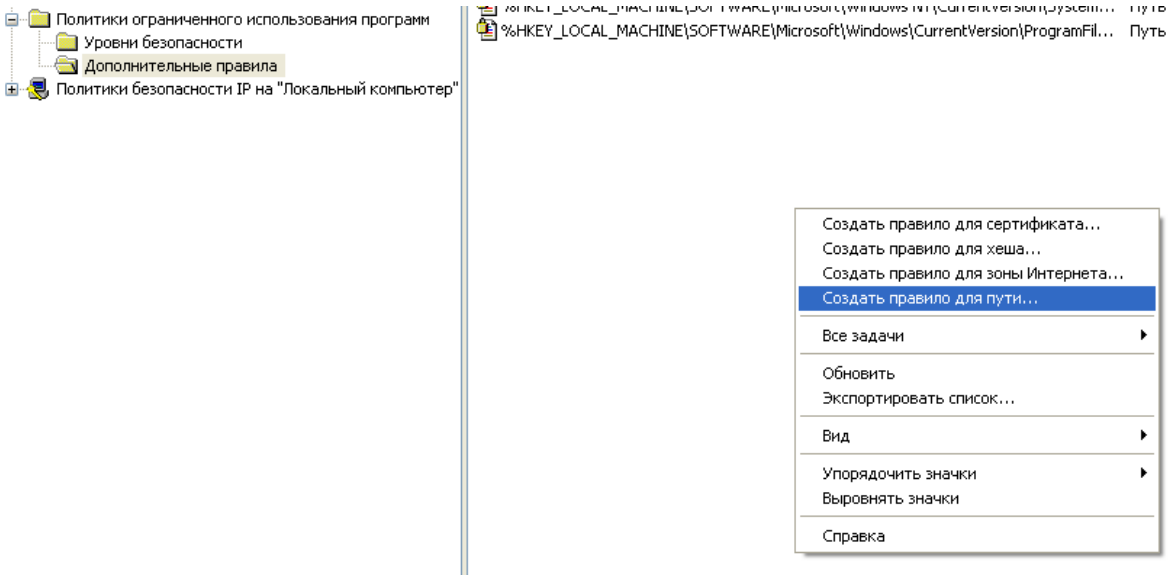

Рисунок 13 - Меню дополнительных правил

Далее идет объект «Принудительный» (Рисунок 14).

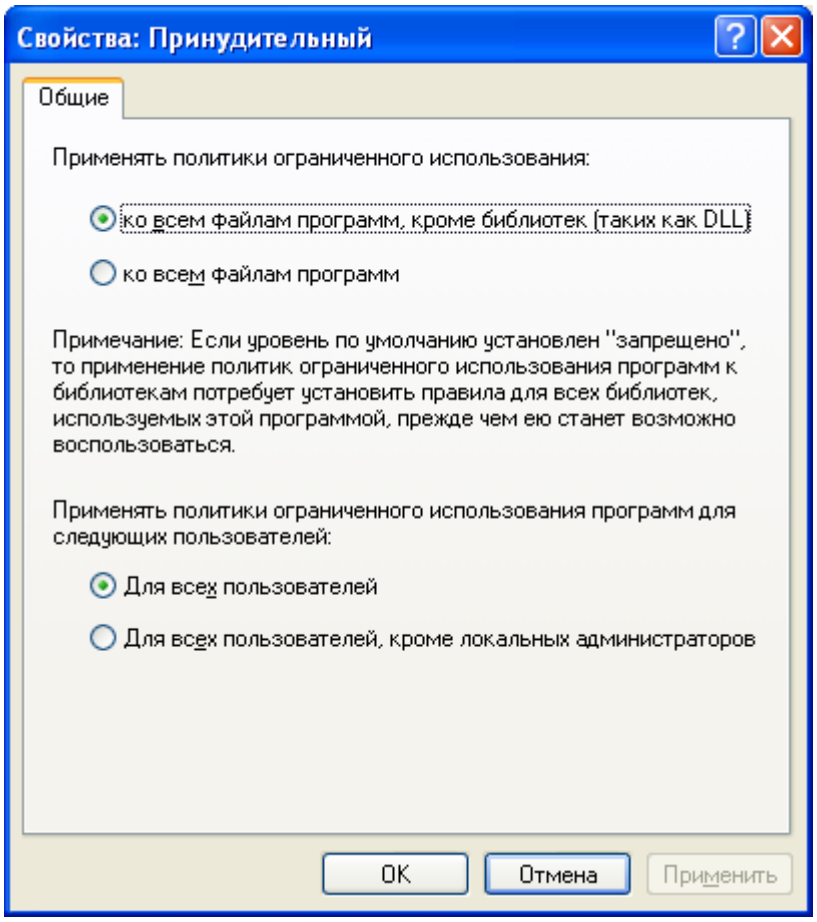

Рисунок 14 - Окно объекта "Принудительный"

В этом окне можно принудительно применить политики не только к исполняемым файлам, но и к связанным с ними библиотекам DLL, а также выбрать к какой группе («Все», «Все, кроме локальных администраторов») пользователей применять политики.

После идет объект «Назначенные типы файлов» (Рисунок 15).

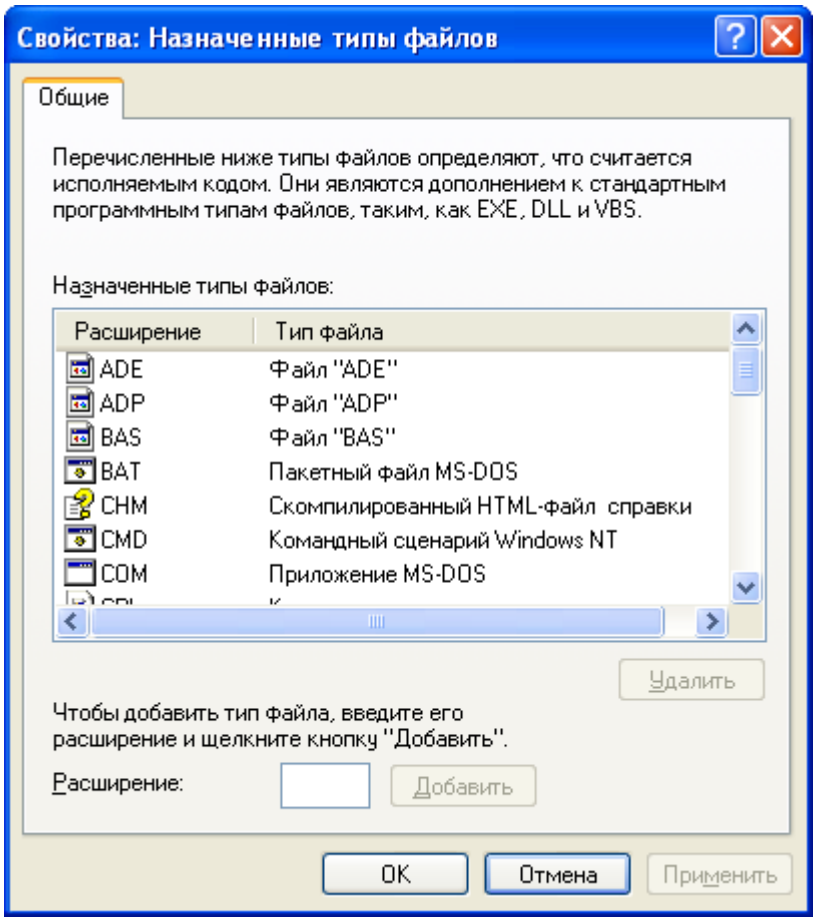

Рисунок 15 - Настройка типов файлов

В данном окне перечислен список расширений файлов, которые контролируются политиками ограниченного использования программ. Данный список можно редактировать под свои условия.

Последним пунктом идет объект «Доверенные издатели» (Рисунок 16).

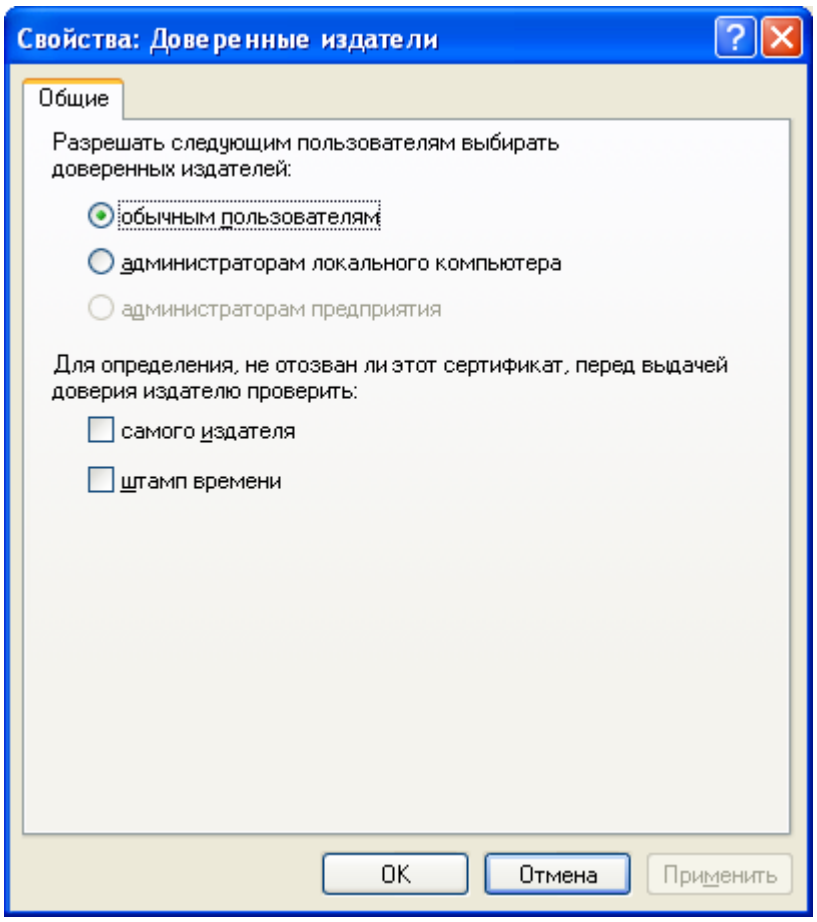

Рисунок 16 - Настройка доверенных издателей сертификатов

В этом окне регулируются настройки доверенных издателей сертификатов, которыми подписываются приложения. Данное окно актуально, только если используются правила для сертификатов.

Для примера создадим правило для пути запрещающее запуск приложения мгновенного обмена сообщениями Microsoft Messenger. Для этого необходимо вызвав меню в рабочей области раздела «Дополнительные правила» выбрать пункт меню «Создать правило для пути»(Рисунок 17).

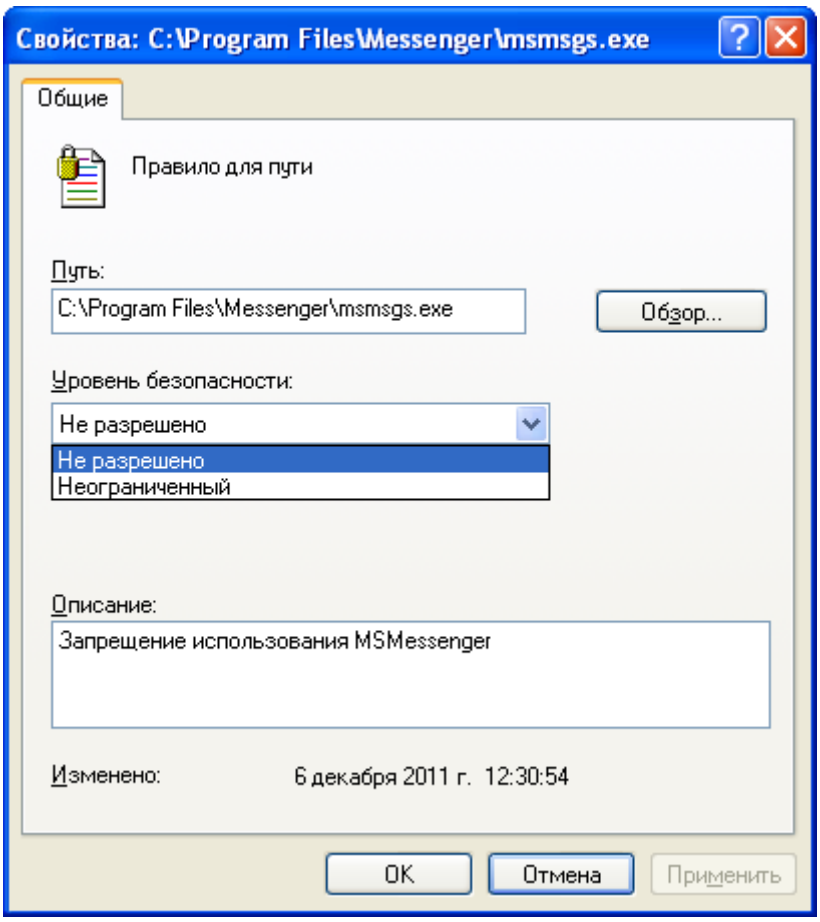

Рисунок 17 - Пример настройки правила пути

- в строке «Путь» указать полный путь до запускаемого файла. Выбрать в списке «уровень безопасности» пункт «Не разрешено» и нажать «Ок».

После этого созданное правило будет создано в рабочей области (Рисунок 18).

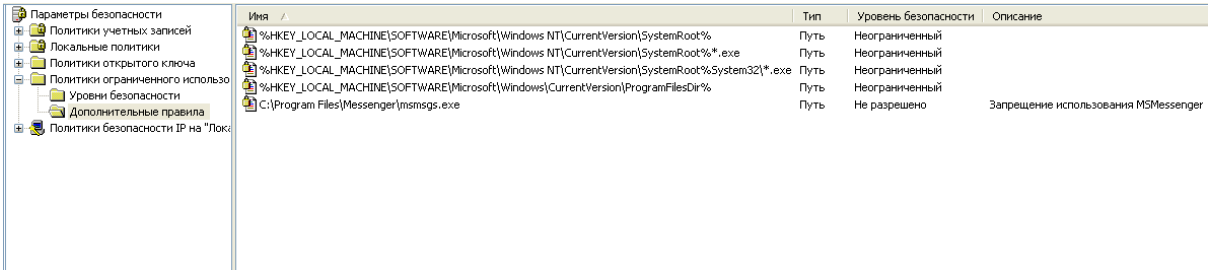

Рисунок 18 - Созданное правило, запрещающее запуск приложения

Для применения изменений необходимо либо перезагрузить компьютер, либо выполнить команду «gpupdate».

Список литературы

1. **Компания "КРИПТО-ПРО".** Руководство администратора безопасности. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 01.

2. —. Руководство администратора безопасности. Установка. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 02.

3. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 03.

4. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 05.

5. **Компания "Microsoft".** AppLocker. *Microsoft Docs.* [В Интернете] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd723678(v=ws.10).

6. **Компания "КРИПТО-ПРО".** Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 30 01.