МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт–Петербургский государственный университет  
аэрокосмического приборостроения»

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ОТЧЕТ

ЗАЩИЩЕН С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| преподаватель |  |  |  | И. В. Козлов |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ  по дисциплине МДК 02.01. Администрирование сетевых операционных систем |
|  |
|  |
|  |
|  |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | С342 |  |  |  | Б. И. Глаголевский,  Е. Ю. Барабаш |
|  |  |  | подпись, дата |  | инициалы, фамилия |

# Практическая работа 1: Создание и управление GPO

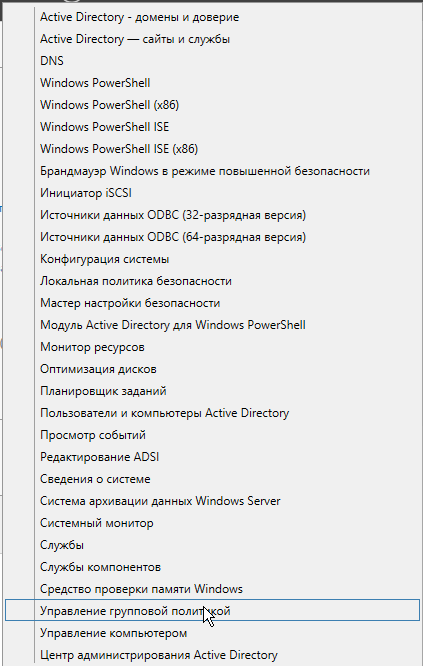


Рисунок 1

Для создания групповой политики (GPO) с использованием консоли управления групповыми политиками (GPMC) необходимо выполнить следующие действия. Первоначально требуется авторизоваться на контроллере домена DC1 с использованием учетных данных администратора. После входа в систему следует открыть Диспетчер серверов, где в разделе "Средства" будет доступна консоль "Управление групповой политикой". Данный инструмент позволяет централизованно настраивать и применять политики в доменной среде.

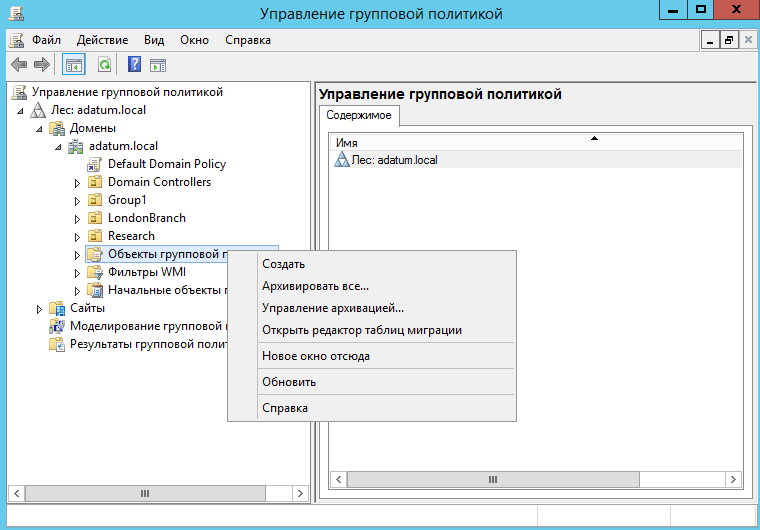


Рисунок 2

После запуска консоли управления групповыми политиками (GPMC) необходимо последовательно развернуть структуру каталогов, начиная с уровня леса Adatum.local. Далее требуется перейти в раздел доменов и выбрать целевой домен Adatum.local для продолжения работы с групповыми политиками. Данная последовательность действий обеспечивает корректный доступ к объектам групповых политик в рамках указанного домена.

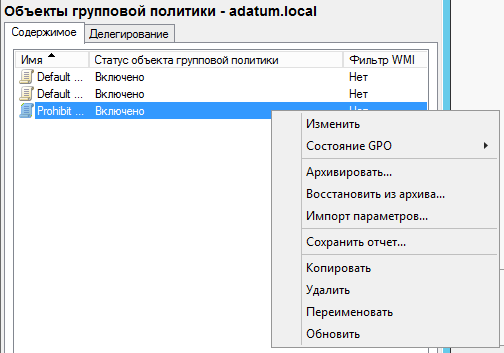


Рисунок 3

Для создания нового объекта групповой политики необходимо в консоли GPMC выбрать соответствующий пункт меню. В открывшемся диалоговом окне указывается имя политики - "Prohibit Windows Messenger", после чего подтверждается действие нажатием кнопки OK. Далее в списке объектов групповой политики требуется выделить только что созданный объект с именем "Prohibit" и выбрать функцию редактирования, что позволит перейти к настройке параметров данной политики.

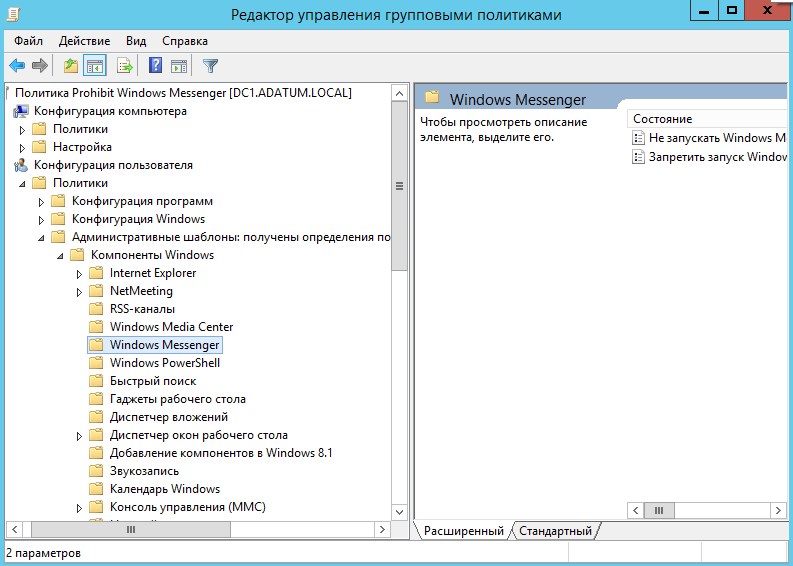


Рисунок 4

Для настройки созданного объекта групповой политики необходимо воспользоваться редактором управления групповыми политиками. В интерфейсе редактора следует последовательно раскрыть разделы: Конфигурация пользователя, Компоненты Windows и Windows Messenger. После перехода в указанный раздел требуется активировать политику "Не запускать Windows Messenger автоматически при входе в систему" путем двойного щелчка на соответствующем пункте. Это действие откроет диалоговое окно для установки требуемых параметров политики.

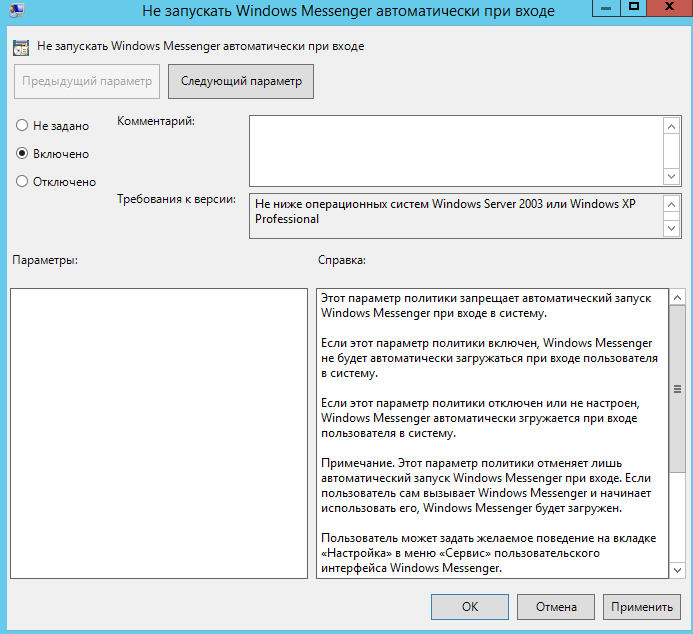


Рисунок 5

После открытия параметров политики необходимо активировать функцию, выбрав значение "Применить" в диалоговом окне настроек. Подтверждение изменений осуществляется нажатием кнопки "OK", после чего внесенные изменения автоматически сохраняются в объекте групповой политики. Завершив настройку, можно закрыть окно редактора групповых политик - все изменения вступят в силу после следующего цикла обновления групповых политик на клиентских рабочих станциях.

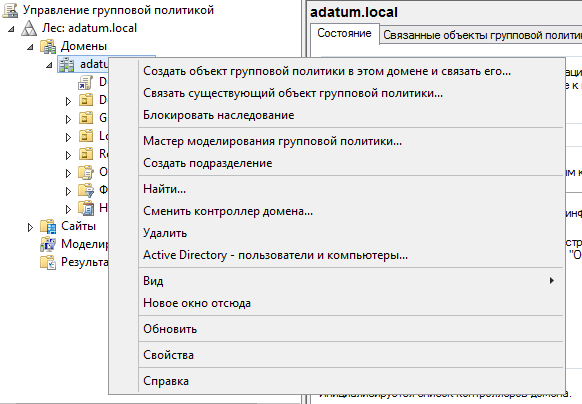


Рисунок 6

Для применения созданной групповой политики в доменной среде необходимо в консоли управления групповыми политиками (GPMC) выделить целевой домен Adatum.local. Далее следует выбрать функцию "Связать существующий объект групповой политики", что позволит ассоциировать ранее созданный GPO с выбранным доменом. Данная операция обеспечит распространение настроек политики на все компьютерные объекты и учетные записи пользователей в пределах указанного домена.

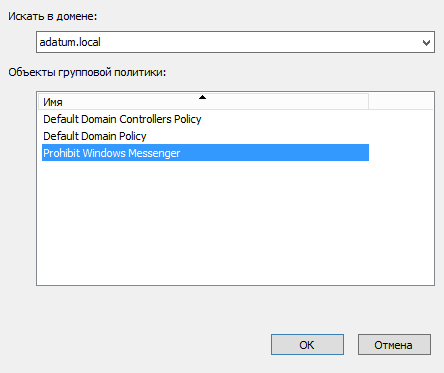


Рисунок 7

В диалоговом окне выбора объектов групповой политики необходимо выделить ранее созданный объект "Prohibit Windows Messenger" из списка доступных политик. После выбора требуемого объекта следует подтвердить действие нажатием кнопки OK, что инициирует процесс связывания данной групповой политики с выбранным доменом. Эта операция обеспечит применение указанных ограничений для клиентских рабочих станций в соответствии с установленным расписанием обновления групповых политик.

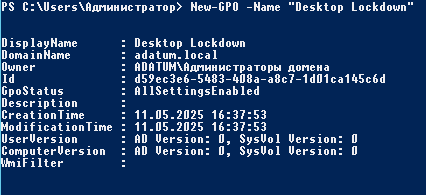


Рисунок 8

Для создания объекта групповой политики с именем "Desktop Lockdown" средствами Windows PowerShell следует выполнить следующую процедуру. Необходимо запустить сеанс Windows PowerShell с правами администратора и ввести соответствующую команду создания групповой политики, указав требуемое имя объекта.

Конкретная команда для создания GPO может выглядеть следующим образом:

New-GPO -Name "Desktop Lockdown"

Данный метод позволяет автоматизировать процесс создания объектов групповой политики и может быть интегрирован в сценарии управления групповыми политиками.

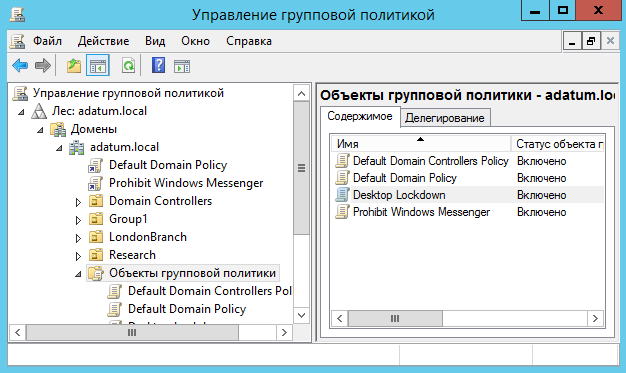


Рисунок 9

Для проверки успешного создания объекта групповой политики "Desktop Lockdown" необходимо выполнить следующую процедуру. В консоли управления групповыми политиками (GPMC) следует открыть раздел "Объекты групповой политики" и визуально убедиться в наличии нового объекта с указанным именем в общем списке доступных политик.

# Практическая работа 2: Использование инструментов диагностики Group Policy

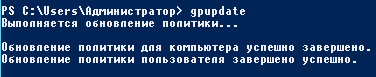


Рисунок 10

Для принудительного обновления групповых политик с использованием Windows PowerShell следует выполнить команду gpupdate с параметром /force. Данная команда инициирует немедленное применение всех актуальных групповых политик без ожидания стандартного цикла обновления. Система обработает как пользовательские, так и компьютерные политики, обеспечивая актуальность всех конфигурационных параметров.

При необходимости можно уточнить область применения, добавив параметр target с указанием computer для обработки только компьютерных политик или user для обновления исключительно пользовательских настроек. Для полного вступления в силу некоторых изменений может потребоваться перезагрузка системы или завершение пользовательского сеанса, что также можно указать соответствующими параметрами.



Рисунок 11

Данная команда создаст детализированный отчет в формате HTML, содержащий актуальную информацию о примененных групповых политиках для текущего пользователя и компьютера. Отчет включает сведения о всех активных политиках, их источниках, а также о фильтрах безопасности, которые повлияли на обработку политик.

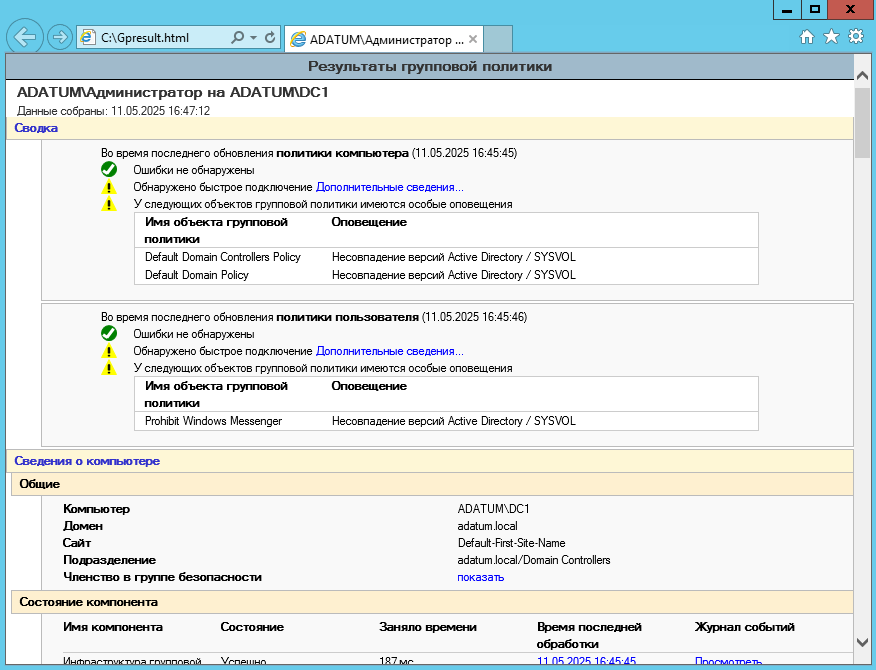


Рисунок 12

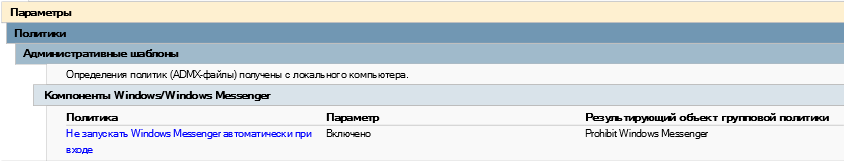


Рисунок 13

После генерации и сохранения HTML-отчета необходимо открыть полученный файл с помощью любого веб-браузера для анализа данных. В содержимом отчета следует найти раздел, посвященный настройкам компонентов Windows, а конкретно - подраздел, касающийся параметров Windows Messenger.

Для быстрой навигации по документу рекомендуется использовать стандартную функцию поиска по странице (обычно вызываемую сочетанием клавиш Ctrl+F), введя в строку поиска фразу "Компоненты Windows" или "Windows Messenger". Это позволит оперативно перейти к интересующему разделу без необходимости ручного просмотра всего содержимого отчета.

В указанном разделе будет представлена подробная информация о текущем состоянии политик, касающихся работы Windows Messenger, включая параметр автоматического запуска при входе в систему. Особое внимание следует обратить на статус применения политики и возможные конфликты с другими параметрами групповых политик.

При обнаружении расхождений между ожидаемыми и фактическими настройками рекомендуется провести дополнительную проверку в консоли управления групповыми политиками для выявления возможных проблем наследования или фильтрации политик. Также стоит убедиться в корректности связывания объектов групповых политик с соответствующими подразделениями домена.

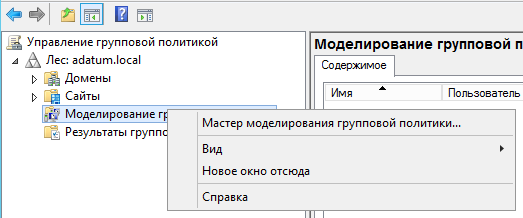


Рисунок 14

Для проверки корректности применения групповой политики необходимо выполнить следующие действия. В открытом HTML-отчете следует убедиться, что параметр "Не запускать Windows Messenger автоматически при входе" имеет статус "Включено", а в разделе "Результирующий объект групповой политики" указано значение "Prohibit Windows Messenger". Это подтверждает успешное применение требуемых ограничений.

После верификации настроек в отчете необходимо вернуться в консоль управления групповыми политиками (GPMC). В данном инструменте требуется выбрать функцию "Моделирование групповой политики", где следует запустить "Мастер моделирования групповой политики". Этот инструмент позволяет проанализировать потенциальные результаты применения политик для различных сценариев без фактического внесения изменений в рабочую среду.

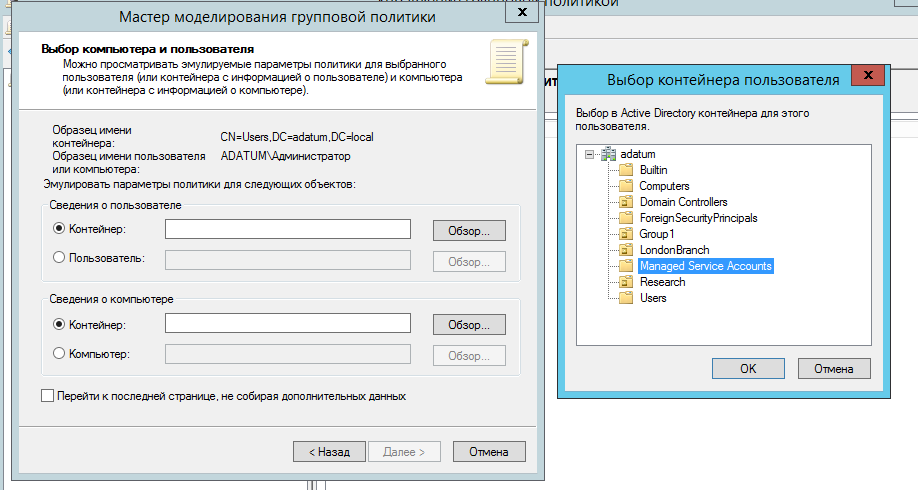


Рисунок 15

Для выполнения моделирования групповой политики с учетом управляемых сервисных учетных записей (Managed Service Accounts) необходимо в мастере моделирования указать соответствующий контейнер в разделе сведений о пользователе. В диалоговом окне выбора местоположения пользователя следует развернуть структуру каталогов домена и выбрать организационное подразделение, содержащее управляемые сервисные учетные записи.

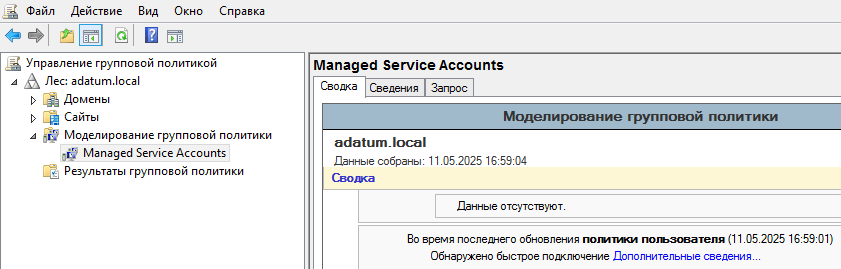


Рисунок 16

# Практическая работа 3: Создание правил AppLocker

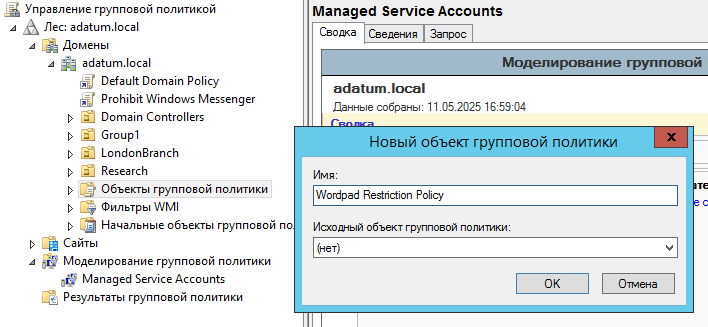


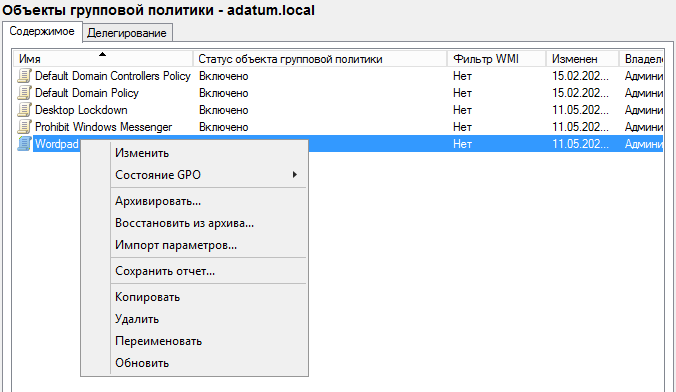
Рисунок 17

Для создания объекта групповой политики, обеспечивающего применение правил AppLocker, необходимо выполнить следующую последовательность действий.

Инициализация процесса осуществляется через Диспетчер серверов, где в разделе "Средства" требуется выбрать консоль "Управление групповой политикой". В открывшейся консоли GPMC необходимо создать новый объект групповой политики, используя соответствующую функцию в контекстном меню.

При создании объекта следует указать понятное имя, отражающее его назначение, например "AppLocker Policy Enforcement". После создания GPO требуется перейти к его редактированию для настройки конкретных параметров AppLocker.

В редакторе групповых политик необходимо последовательно открыть раздел:  
Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики ограниченного использования программ → AppLocker



В «Редакторе управления групповыми политиками» переходим в «Конфигурация компьютера → Политики → Конфигурация Windows → Политики управления приложениями → Applocker → Исполняемые правила.

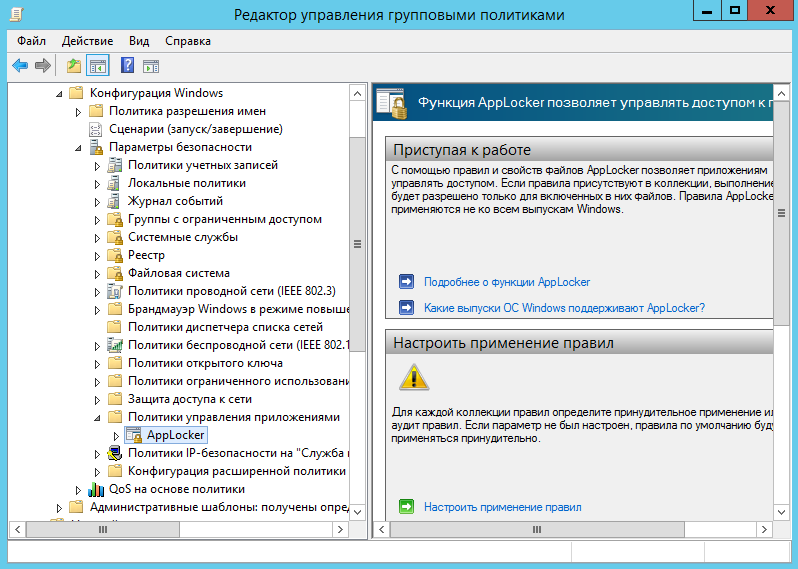


Рисунок 18

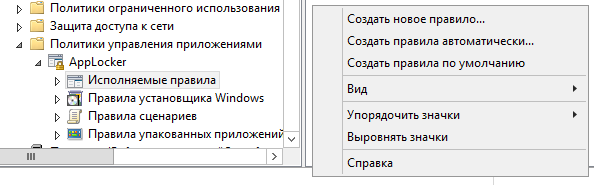


Рисунок 19

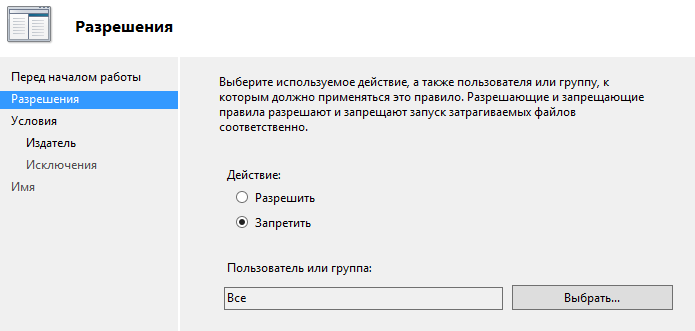


Рисунок 20

Для настройки запрещающего правила в политике AppLocker необходимо в мастере создания правил выбрать действие "Запретить" в разделе "Разрешения"

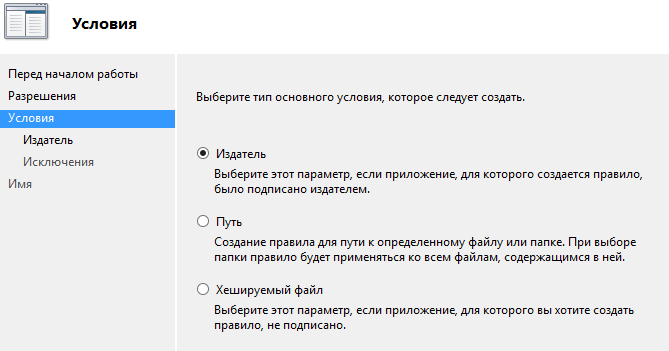


Рисунок 21

При выборе условия "Издатель" в процессе создания правила AppLocker необходимо выполнить следующие действия. В окне мастера создания правил после указания запрещающего действия следует выбрать параметр "Издатель" в разделе определения условий. Это позволит создать ограничение на основе цифровой подписи приложений.

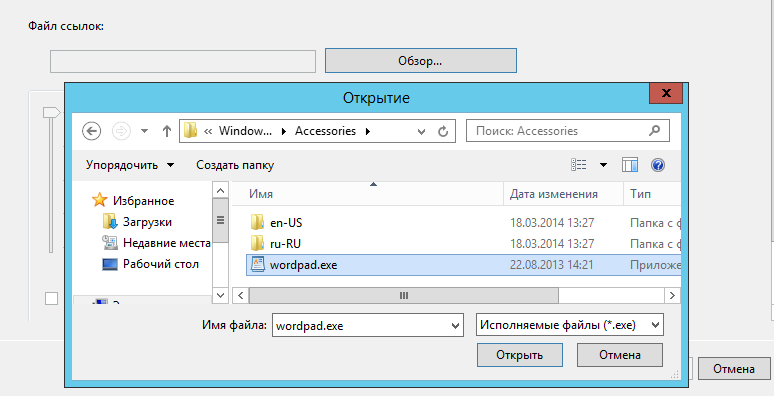


Рисунок 22

Для настройки правила на основе издателя необходимо в мастере создания правил AppLocker выбрать условие "Издатель", нажать кнопку "Обзор" и последовательно перейти в директорию C:\Program Files\Windows NT\Accessories, где следует выбрать исполняемый файл wordpad.exe. После подтверждения выбора система автоматически проанализирует цифровую подпись файла и заполнит соответствующие поля данными издателя.

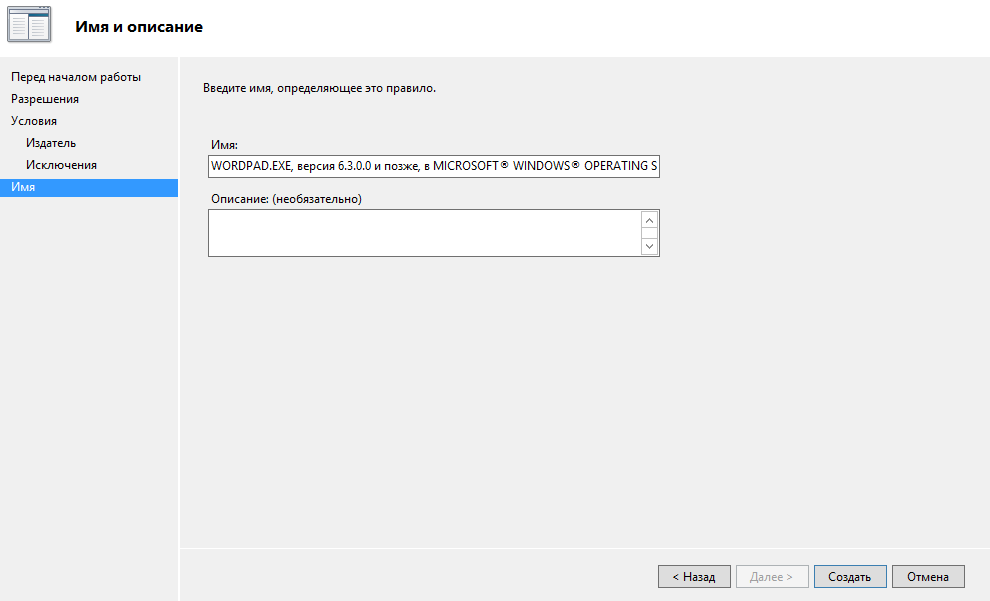


Рисунок 23

После выполнения всех необходимых настроек правила AppLocker, включая выбор условия "Издатель", указание пути к файлу wordpad.exe и настройку соответствующих параметров, следует завершить процесс создания правила. В окне мастера настройки политики необходимо нажать кнопку "Создать", что приведет к окончательному формированию и сохранению нового правила ограничения.

Данное действие добавляет созданное правило в общий набор ограничений политики "Wordpad Restriction Policy". После сохранения изменения будут автоматически применены ко всем объектам, связанным с данной групповой политикой, в соответствии с установленным циклом обновления групповых политик.

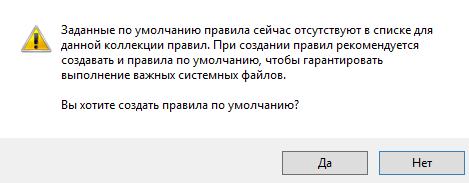


Рисунок 24

При появлении диалогового окна с запросом подтверждения создания стандартных правил в рамках политики AppLocker следует выбрать вариант "Да". Это действие приведет к автоматическому формированию базового набора разрешающих правил, обеспечивающих корректную работу системных компонентов Windows и критически важных элементов инфраструктуры.

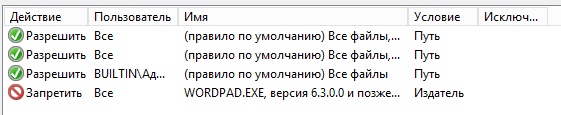


Рисунок 25

После подтверждения создания стандартных правил система автоматически добавляет их в соответствующий раздел политик AppLocker. В редакторе групповых политик теперь можно наблюдать сформированный набор правил для исполняемых файлов, который отображается в разделе:

Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики ограниченного использования программ → AppLocker → Правила для исполняемых файлов

Появившиеся правила включают базовые разрешения для системных директорий, что обеспечивает корректную работу операционной системы. Созданные ранее специализированные правила (включая ограничение для WordPad) также сохраняются и применяются в совокупности с базовыми.

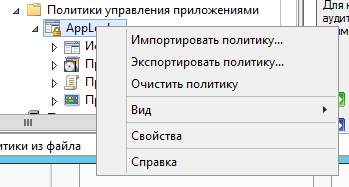


Рисунок 26

На данном этапе необходимо перейти в свойства AppLocker.

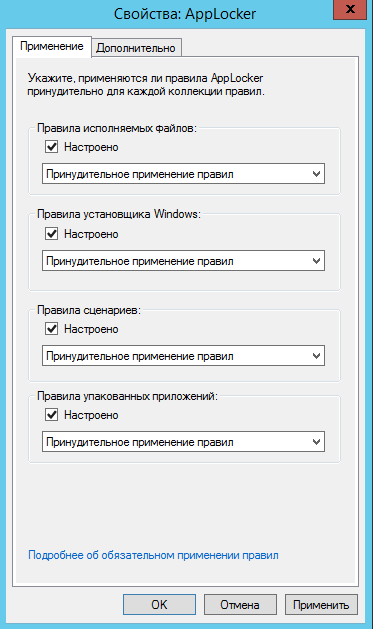


Рисунок 27

Для полной активации всех функций AppLocker необходимо выполнить следующие действия в окне свойств компонента. После перехода в свойства AppLocker следует установить флажки напротив всех доступных параметров на всех вкладках диалогового окна. Это включает принудительное применение правил для всех типов файлов (исполняемые, скрипты, установщики и упакованные приложения), а также активацию режима аудита и расширенных функций.

После установки всех флажков требуется последовательно нажать кнопки "Применить" для сохранения изменений и "OK" для закрытия диалогового окна. Данная конфигурация обеспечивает максимальный уровень контроля выполнения приложений с одновременным ведением подробного журнала событий.

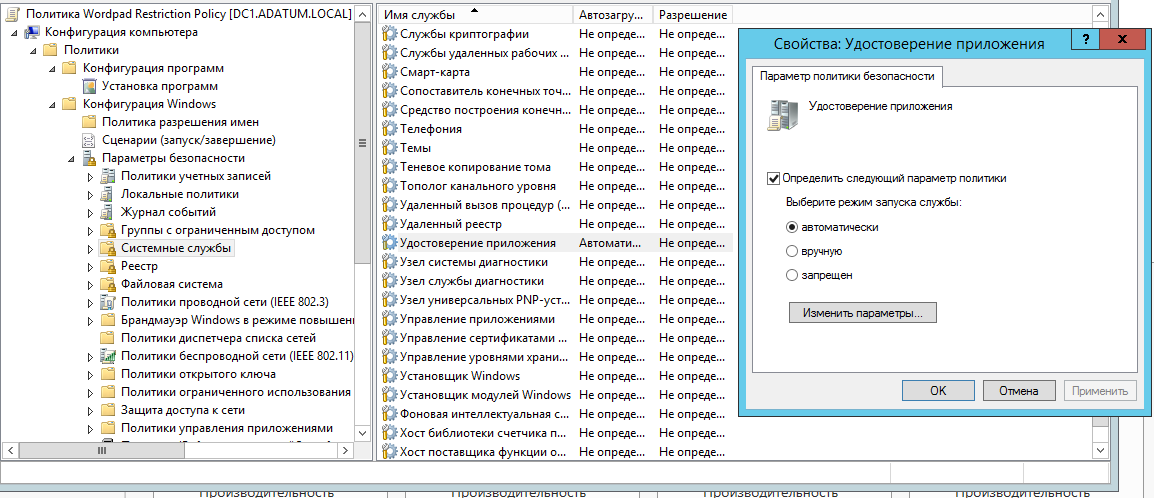


Рисунок 28

Для настройки службы "Удостоверение приложения" через групповые политики необходимо выполнить следующую последовательность действий. В редакторе управления групповыми политиками требуется перейти по указанному пути: Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Системные службы. В данном разделе следует найти службу "Удостоверение приложения" и открыть ее свойства двойным щелчком мыши.

В открывшемся диалоговом окне свойств службы необходимо активировать опцию "Определить следующий параметр политики", установив соответствующий флажок. После активации данного параметра требуется выбрать тип запуска службы - "Автоматически" из выпадающего списка доступных вариантов.

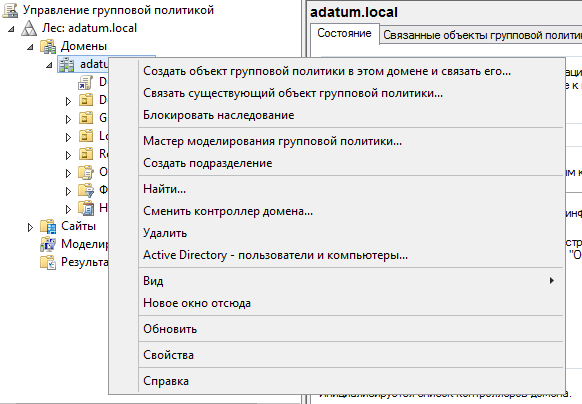


Рисунок 29

Для применения созданного объекта групповой политики к домену Adatum.local необходимо выполнить следующую процедуру. В консоли управления групповыми политиками (GPMC) следует развернуть структуру домена и выбрать целевой домен Adatum.local. После выбора домена необходимо воспользоваться функцией "Связать существующий объект групповой политики", доступной в контекстном меню или панели действий.

В открывшемся диалоговом окне выбора GPO требуется найти и выделить ранее созданный объект групповой политики (например, "Wordpad Restriction Policy" или "AppLocker Policy Enforcement"), после чего подтвердить выбор нажатием кнопки "OK". Это действие создаст связь между выбранным объектом групповой политики и доменом Adatum.local, обеспечивая применение настроенных параметров ко всем компьютерам и пользователям домена.

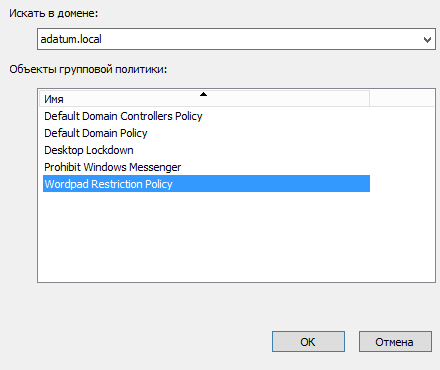


Рисунок 30

В консоли управления групповыми политиками (GPMC) после выбора функции "Связать существующий объект групповой политики" с доменом Adatum.local необходимо в открывшемся диалоговом окне выбрать конкретный объект политики. Следует найти в списке доступных GPO объект с именем "Wordpad Restriction Policy" и выделить его. После выбора указанного объекта групповой политики требуется подтвердить действие нажатием кнопки "OK", что установит связь между данной политикой и доменом Adatum.local.

Данная операция обеспечит применение всех настроек ограничений WordPad, определенных в политике "Wordpad Restriction Policy", ко всем компьютерным объектам и учетным записям пользователей в рамках указанного домена. Особое внимание следует обратить на то, что политика начнет действовать согласно стандартному циклу обновления групповых политик, который по умолчанию составляет 90 минут с случайным смещением от 0 до 30 минут для рабочих станций и 5 минут для контроллеров домена.

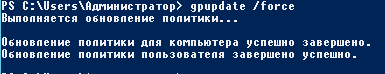


Рисунок 31

Для принудительного обновления групповых политик на целевом компьютере или контроллере домена необходимо выполнить следующую процедуру в Windows PowerShell. Запустите сеанс PowerShell с повышенными привилегиями (от имени администратора) и введите команду gpupdate /force.

Данная команда инициирует немедленный процесс обновления групповых политик без ожидания следующего запланированного цикла. Система обработает как пользовательские, так и компьютерные политики, включая недавно связанную политику "Wordpad Restriction Policy".

# Практическая работа 4: Реализация защищенного сетевого трафика с помощью брандмауэра Windows

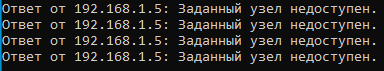


Рисунок 32

Для проверки блокировки ICMPv4 (протокола ping) на клиентской рабочей станции CL1 необходимо выполнить следующую последовательность действий. Авторизуйтесь на компьютере CL1, используя учетные данные администратора домена или локальной системы. После успешного входа откройте командную строку с повышенными привилегиями (нажмите правой кнопкой мыши на значке командной строки и выберите "Запуск от имени администратора").

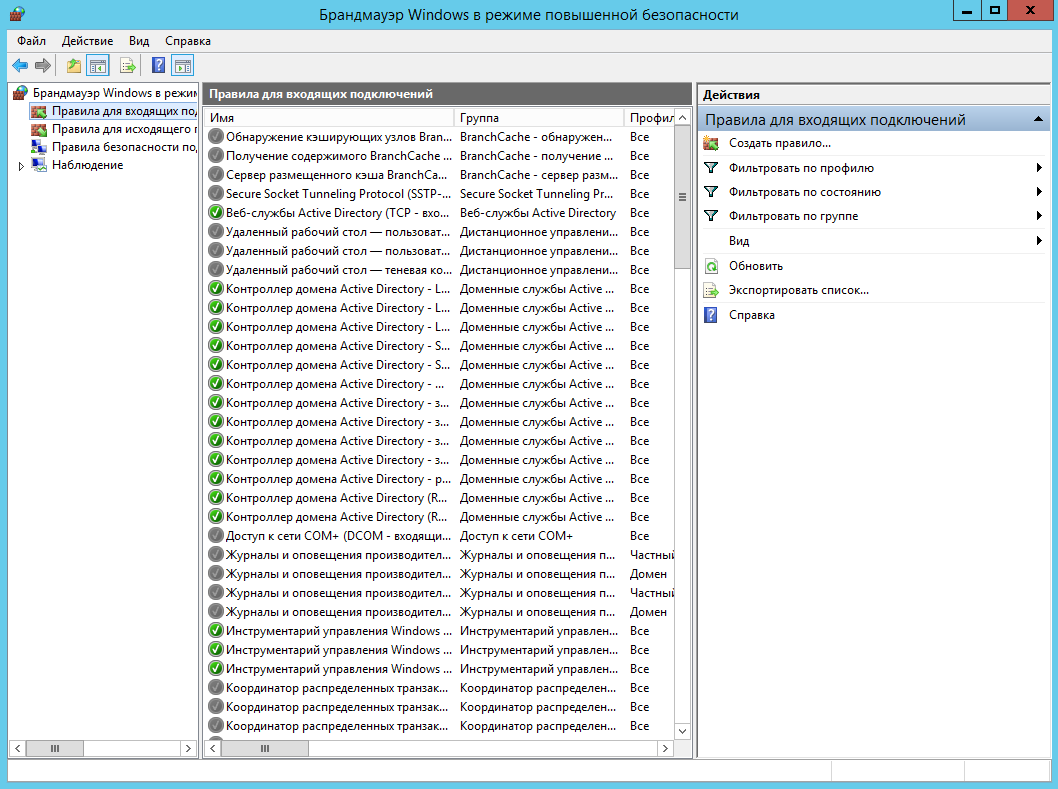


Рисунок 33

Для настройки разрешения ICMPv4 (эхо-запросов ping) на контроллере домена DC1 необходимо выполнить следующие действия. Авторизуйтесь на сервере DC1 с использованием учетной записи администратора домена. После успешного входа откройте консоль управления групповыми политиками (GPMC) через меню "Средства" в Диспетчере серверов либо выполнив команду gpmc.msc в командной строке.

В дереве консоли GPMC найдите созданный ранее объект групповой политики, содержащий настройки брандмауэра, или создайте новый GPO специально для управления сетевыми параметрами. Перейдите в редактор групповых политик, выбрав соответствующий пункт контекстного меню. В редакторе проследуйте по пути: Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Брандмауэр Windows.

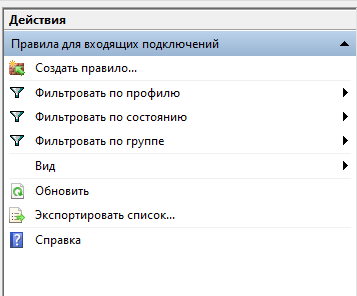


Рисунок 34

Выбираем «Настраиваемое правило»

Для создания нового правила входящих подключений в брандмауэре Windows необходимо выполнить следующую последовательность действий. Откройте Панель управления и перейдите в раздел "Брандмауэр Защитника Windows". В основном окне брандмауэра выберите пункт "Дополнительные параметры", что приведет к открытию оснастки "Брандмауэр Windows в режиме повышенной безопасности".

В левой части интерфейса оснастки выделите раздел "Правила для входящих подключений". В правой панели действий нажмите "Создать правило", что запустит мастер настройки нового правила

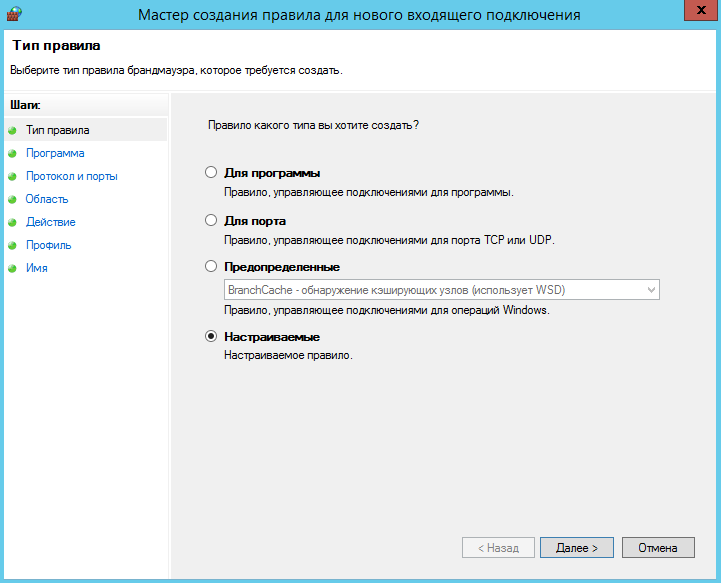


Рисунок 35

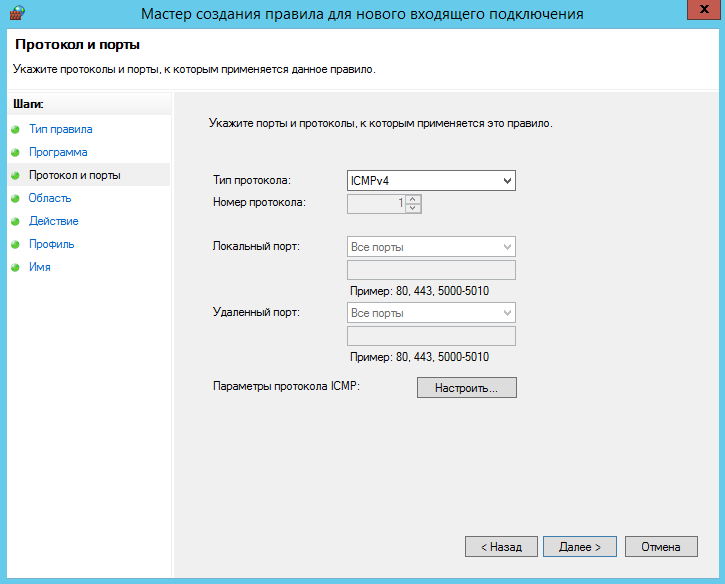


Рисунок 36

При настройке нового правила для входящих подключений в брандмауэре Windows на этапе выбора типа протокола необходимо указать ICMPv4. В мастере создания правила после перехода на страницу "Протокол и порты" следует выбрать вариант "Настраиваемый" в поле "Тип протокола".

После выбора настраиваемого протокола станет доступным поле "Протокол:", где нужно нажать кнопку "Настроить". В открывшемся диалоговом окне настроек протокола необходимо:

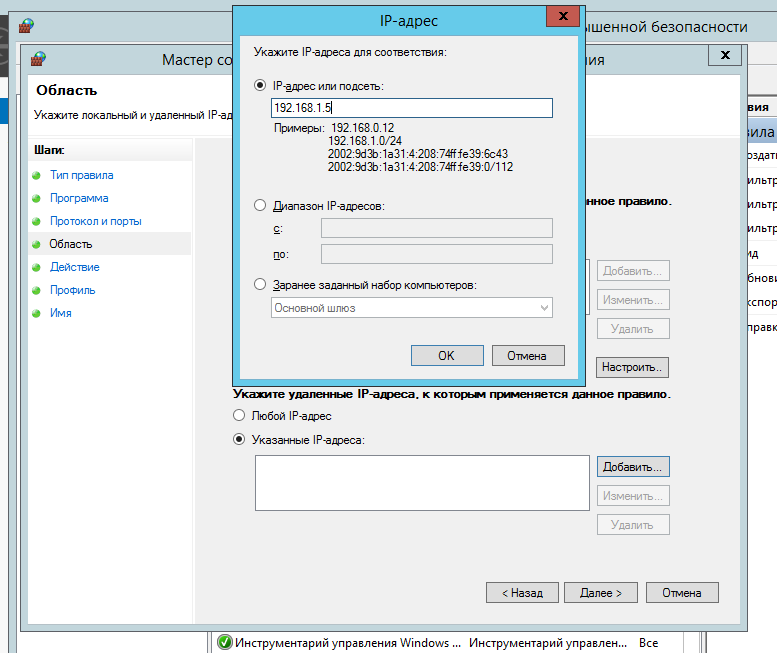


Рисунок 37

На этапе настройки области применения правила в мастере создания правила брандмауэра, после перехода на страницу "Область", необходимо выполнить следующие действия для ограничения доступа по IP-адресам. В разделе "Укажите удаленные IP-адреса, к которым применяется данное правило" следует выбрать опцию "Указанные IP-адреса", что активирует возможность добавления конкретных сетевых адресов.

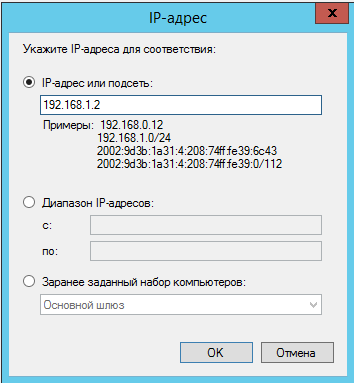


Рисунок 38

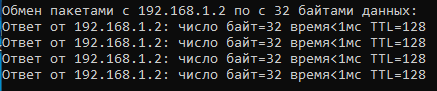


Рисунок 39

На «Рисунке 39» можно наблюдать, что все работает.

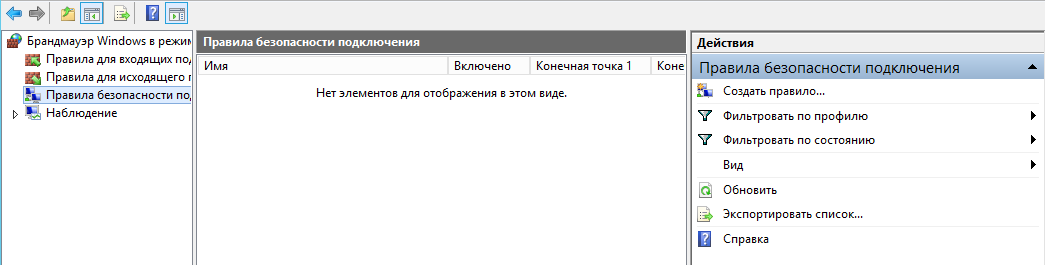


Рисунок 40

Для создания нового правила безопасности подключения в Брандмауэре Windows выполните следующие действия. В оснастке "Брандмауэр Windows в режиме повышенной безопасности" выберите раздел "Правила безопасности подключения" в левой панели. В правой панели действий нажмите "Создать правило безопасности подключения", что запустит соответствующий мастер настройки.

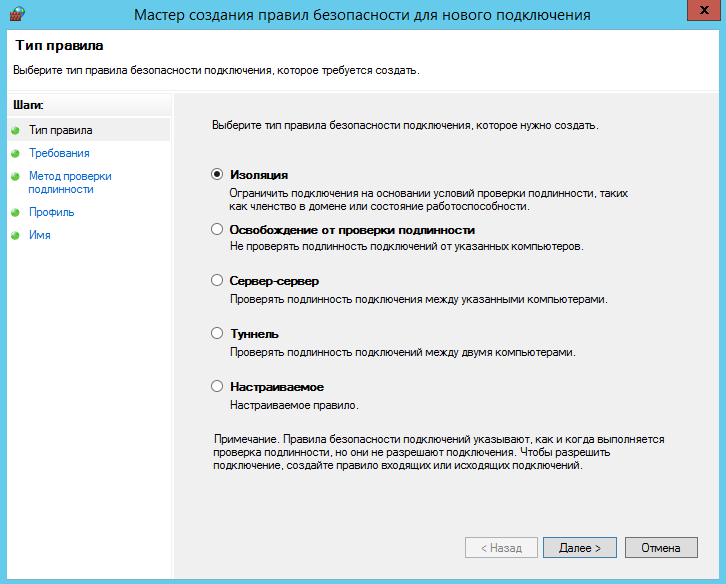


Рисунок 41

Для создания правила безопасности подключения типа "Изоляция" в Брандмауэре Windows необходимо выполнить следующую последовательность действий. В оснастке "Брандмауэр Windows в режиме повышенной безопасности" выберите раздел "Правила безопасности подключения" в левой панели интерфейса. В правой панели действий нажмите "Создать правило безопасности подключения", что запустит соответствующий мастер настройки.

В мастере создания правила выберите тип "Изоляция", который обеспечит ограничение сетевого доступа только для систем, соответствующих заданным требованиям безопасности.

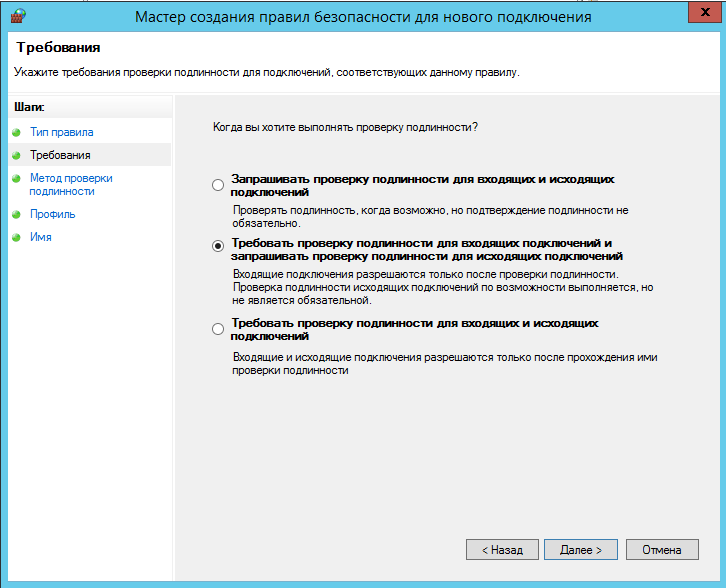


Рисунок 42

При настройке требований аутентификации в мастере создания правила безопасности подключения типа "Изоляция" необходимо выбрать указанный вариант, который обеспечит двустороннюю проверку подлинности сетевых соединений. Данная конфигурация требует, чтобы все входящие подключения проходили обязательную аутентификацию, одновременно запрашивая проверку подлинности для исходящих соединений.

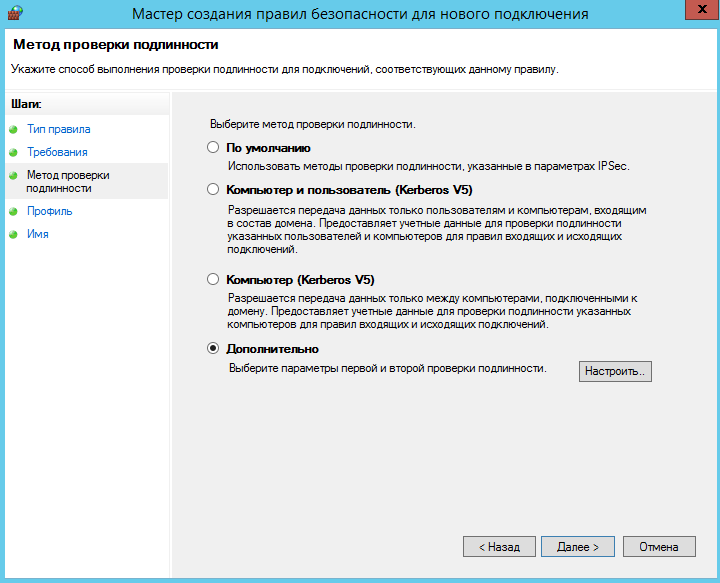


Рисунок 43

При настройке дополнительных параметров аутентификации в мастере создания правила безопасности подключения необходимо выполнить следующие действия. После выбора пункта "Дополнительно" и нажатия кнопки "Настроить" откроется диалоговое окно расширенной конфигурации методов проверки подлинности.

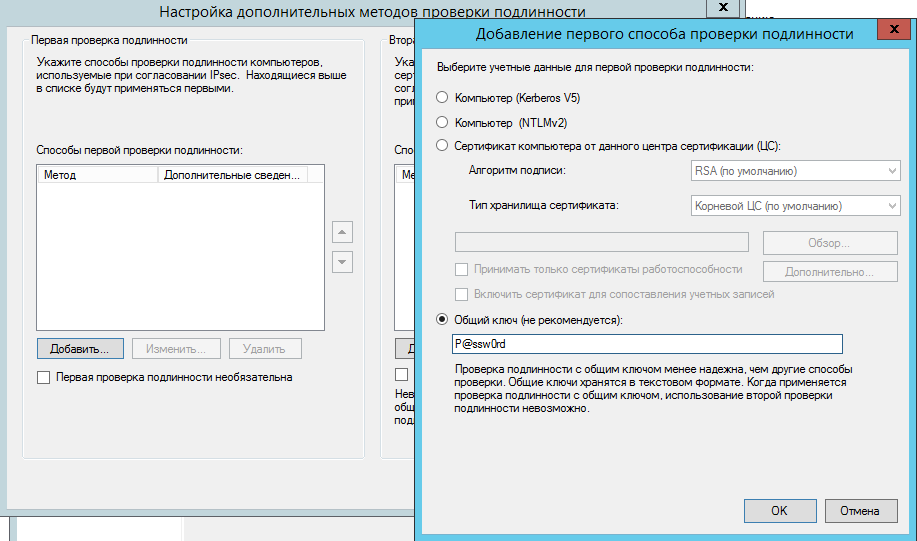


Рисунок 44

При добавлении метода проверки подлинности с использованием общего ключа необходимо учитывать следующие аспекты. В открывшемся диалоговом окне настройки методов аутентификации выберите вариант "Общий ключ" из доступных методов проверки подлинности. В соответствующее поле введите заданную ключевую фразу, в данном случае P@ssw0rd, соблюдая точный регистр и символы.

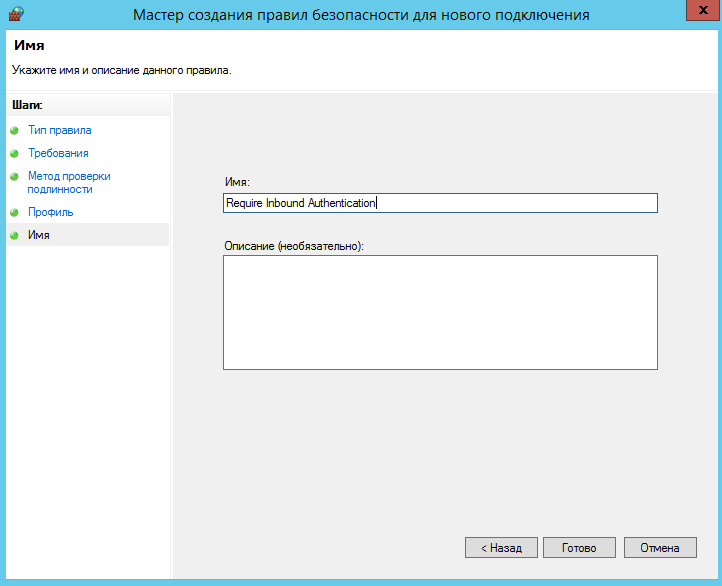


Рисунок 45

При завершении настройки правила безопасности подключения необходимо выполнить следующие действия. В мастере создания правила выберите все доступные профили сети (доменный, частный, общедоступный), чтобы обеспечить применение политики аутентификации для всех типов подключений. Это гарантирует единообразие требований безопасности независимо от того, к какой сети подключен компьютер в данный момент.

В поле имени правила введите четкое и описательное название, в данном случае "Require Inbound Authentication", которое однозначно отражает назначение создаваемого правила.

# Лабораторная работа № 7.1: Реализация групповой политики

## Упражнение 1: Настройка центрального хранилища

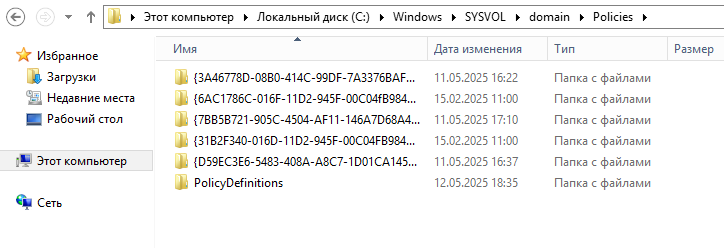


Рисунок 46

Для настройки центрального хранилища административных шаблонов групповых политик необходимо выполнить следующую последовательность действий.

Сначала требуется создать структуру центрального хранилища. В проводнике Windows перейдите по пути C:\Windows\SYSVOL\domain\Policies, где "domain" соответствует имени вашего домена. В данной директории создайте новую папку с именем PolicyDefinitions. Затем скопируйте все содержимое из системной папки C:\Windows\PolicyDefinitions в только что созданную папку PolicyDefinitions. Этот процесс обеспечит централизованное хранение всех файлов ADMX и ADML для административных шаблонов.

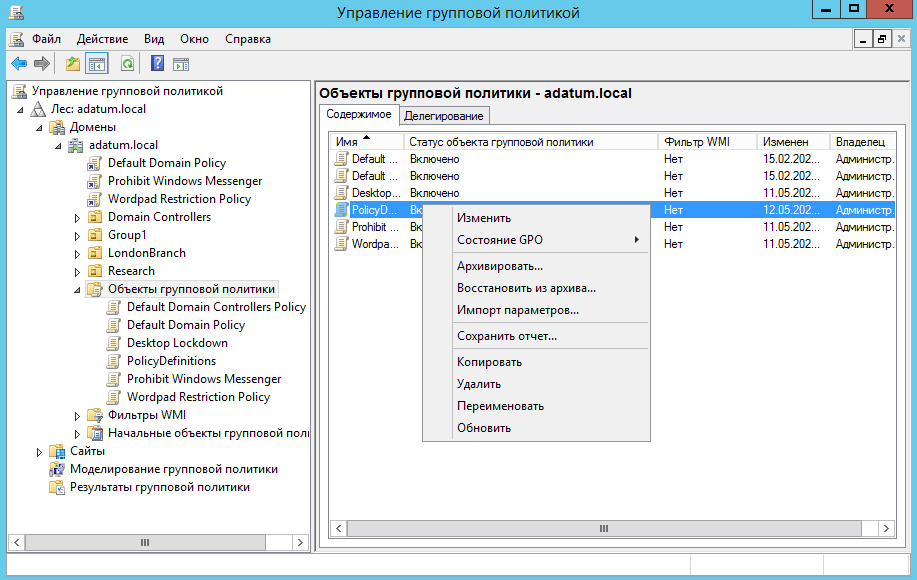


Рисунок 47

Для создания и настройки нового объекта групповой политики выполните следующие действия. В консоли управления групповыми политиками (GPMC) найдите нужное подразделение или домен в древовидной структуре. Щелкните правой кнопкой мыши на выбранном контейнере и выберите пункт "Создать объект групповой политики в этом домене и связать его здесь". В открывшемся диалоговом окне укажите осмысленное имя для нового объекта, например "AppLocker Policy Enforcement", и подтвердите создание нажатием кнопки OK.

После успешного создания объекта групповой политики необходимо перейти к его настройке. Щелкните правой кнопкой мыши на только что созданном GPO и выберите пункт контекстного меню "Изменить". Это действие откроет редактор управления групповыми политиками, где можно производить детальную настройку различных параметров.

В редакторе доступны два основных раздела для конфигурации: параметры компьютера и параметры пользователя. В зависимости от задач можно настроить политики безопасности, установить параметры реестра, определить сценарии входа/выхода или запуска/завершения работы, а также настроить множество других параметров.

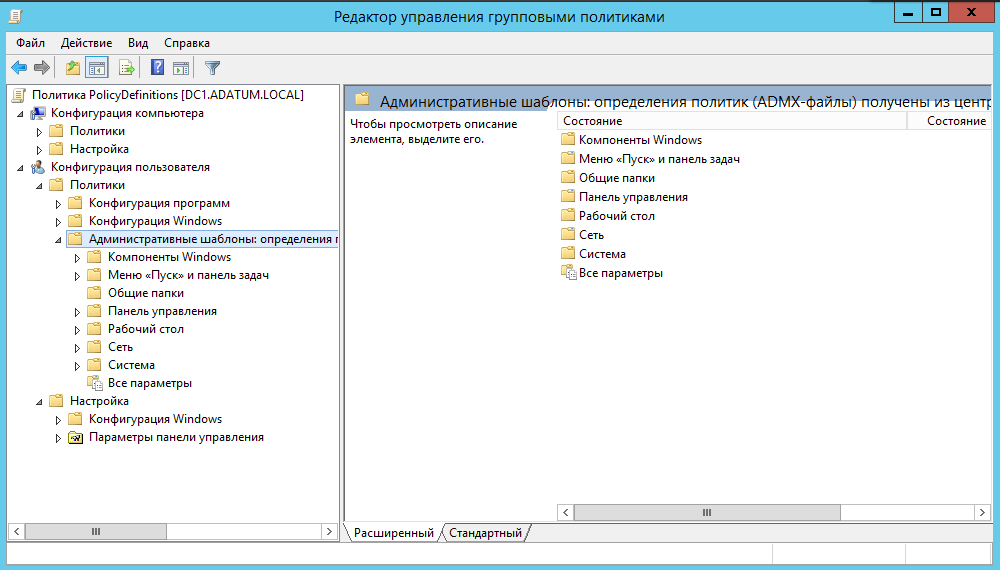


Рисунок 48

## Упражнение 2: Создание объектов групповой политики

## В «Диспетчере серверов» переходим в «Управление групповой политикой» и создаем новый «Объект групповой политики»

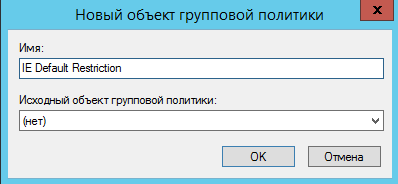


Рисунок 49

Для создания нового объекта групповой политики выполните следующую последовательность действий. В Диспетчере серверов выберите раздел "Средства" и перейдите в оснастку "Управление групповой политикой". В открывшейся консоли GPMC разверните структуру домена и выберите организационное подразделение или домен, с которым необходимо связать новый объект групповой политики.

Щелкните правой кнопкой мыши на выбранном контейнере и в контекстном меню выберите пункт "Создать объект групповой политики в этом домене и связать его здесь". В диалоговом окне создания укажите осмысленное имя для нового GPO, отражающее его назначение, например "Базовые параметры безопасности рабочих станций".

После подтверждения создания щелкните правой кнопкой мыши на новом объекте групповой политики и выберите "Изменить" для перехода в редактор групповых политик.

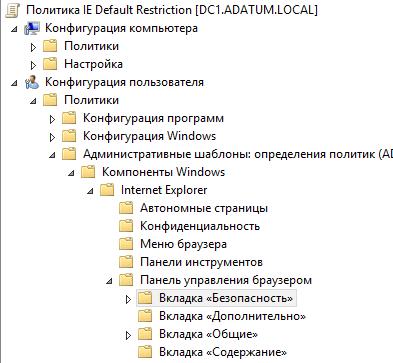


Рисунок 50

После открытия редактора групповых политик для внесения изменений в созданный объект групповой политики необходимо перейти по указанному пути. В левой панели редактора последовательно раскройте ветку "Конфигурация пользователя", затем выберите раздел "Административные шаблоны". Далее перейдите в подраздел "Компоненты Windows", где следует найти и раскрыть категорию "Internet Explorer".

В данном разделе выберите элемент "Панель управления браузера", а затем перейдите на вкладку "Безопасность". Здесь доступны различные политики, позволяющие управлять параметрами безопасности браузера Internet Explorer для всех пользователей, на которых будет распространяться данный объект групповой политики.

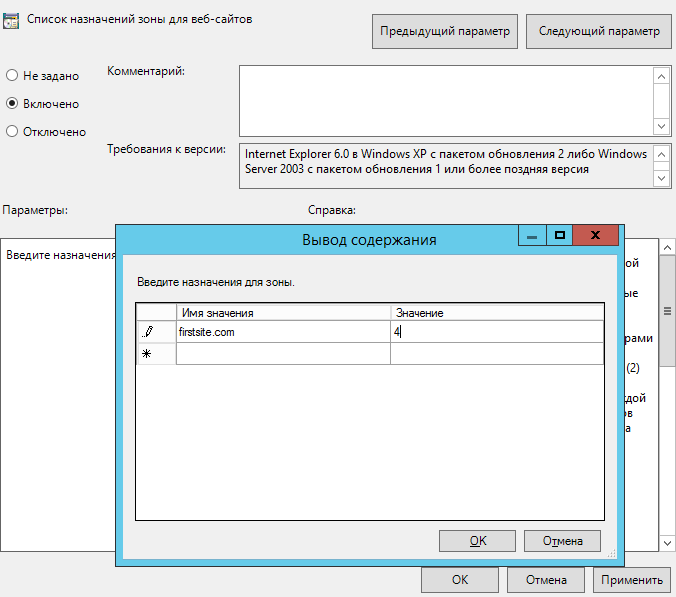
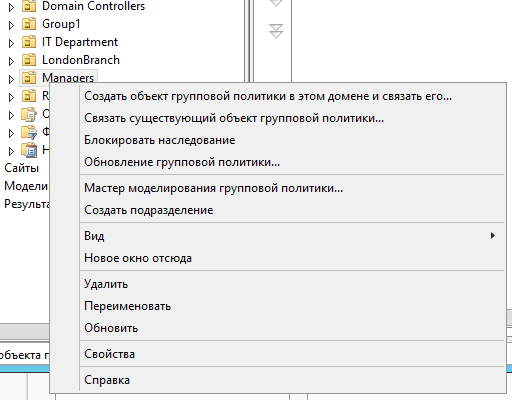
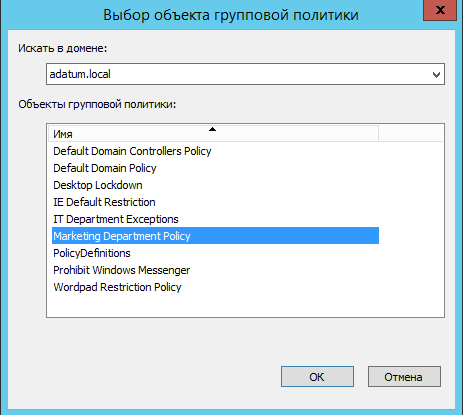


Рисунок 51

Для настройки политики распределения веб-сайтов по зонам безопасности в Internet Explorer необходимо выполнить следующие действия. В редакторе групповых политик после перехода по указанному пути следует активировать параметр "Список назначений зоны для веб-сайтов", установив переключатель в положение "Включено".



Выбираем Marketing Department Policy



Заходим в «Объекты групповой политики → Marketing Department Policy → Делегирование → Добавить»

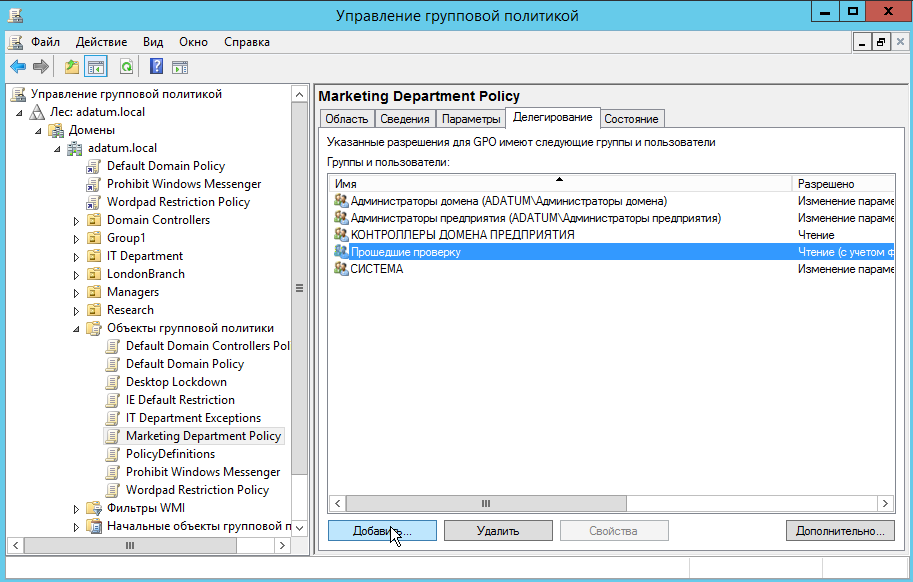


Рисунок 52

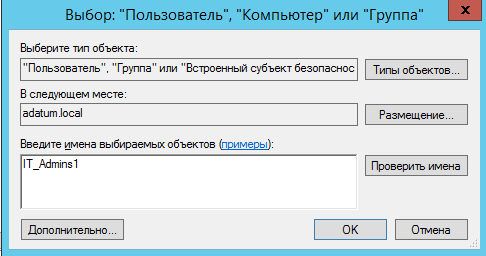


Рисунок 53

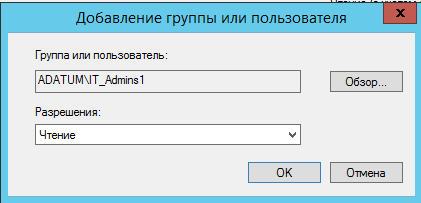


Рисунок 54

# Лабораторная работа 7.2: Повышение безопасности серверных ресурсов

## Упражнение 1. Использование групповой политики для защиты серверов-участников

Создаем новый объект групповой политики Server Local Admins

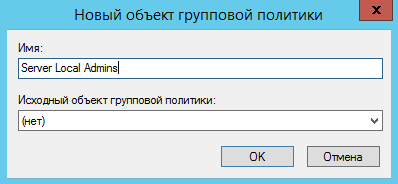


Рисунок 55

Для настройки защиты серверов-участников домена необходимо создать специализированный объект групповой политики. В консоли управления групповыми политиками (GPMC) следует выбрать целевое подразделение, содержащее серверные объекты, и создать новый GPO с понятным именем, например "Server Local Admins".

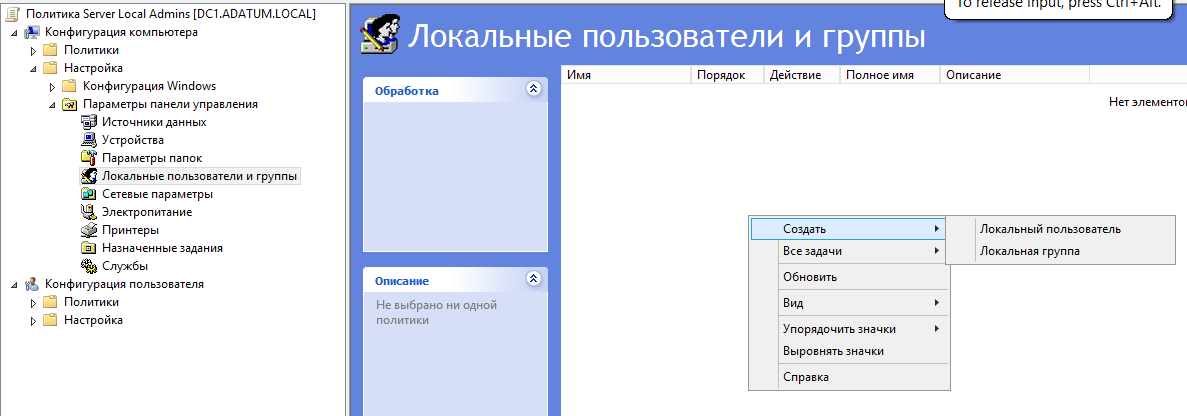


Рисунок 56

Для настройки локальных групп через групповую политику выполните следующие действия.

После создания объекта групповой политики Server Local Admins и перехода к его редактированию, в редакторе GPO необходимо развернуть ветку:

Конфигурация компьютера → Настройка → Параметры панели управления → Локальные пользователи и группы

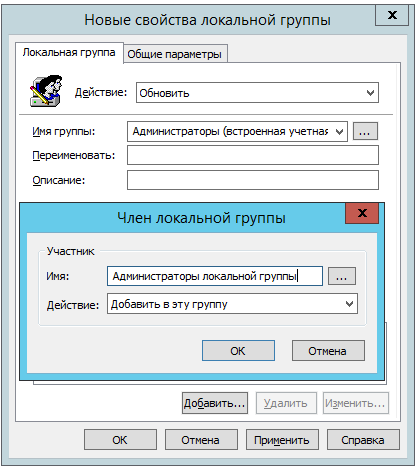


Рисунок 57

## Упражнение 2: Аудит доступа к файлам

Заходим в свойства папки Изображения, после нажимаем «Дополнительно»

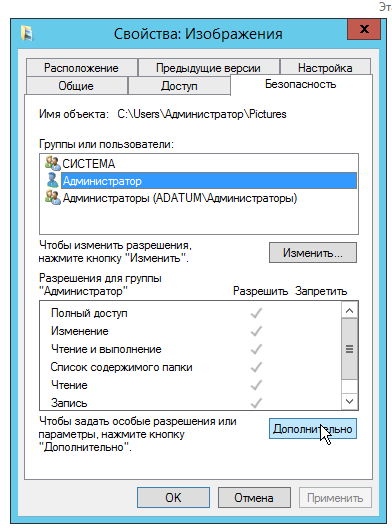


Рисунок 58

Далее заходим во вкладку «Аудит» и нажимаем «Добавить»

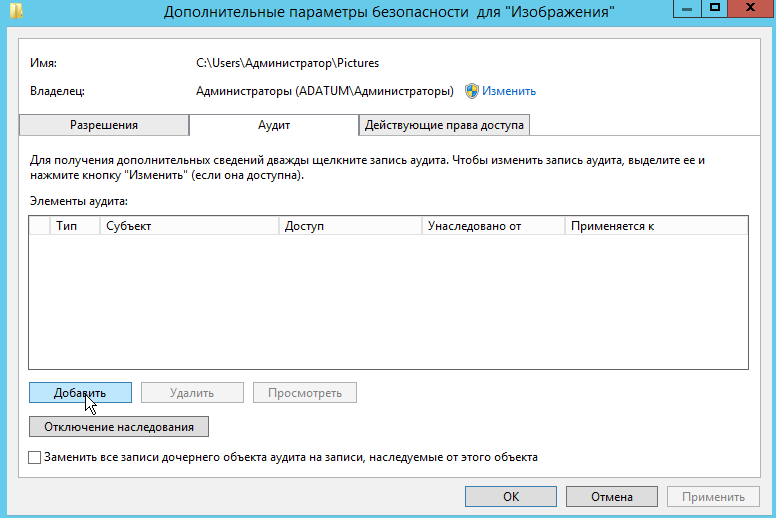


Рисунок 59

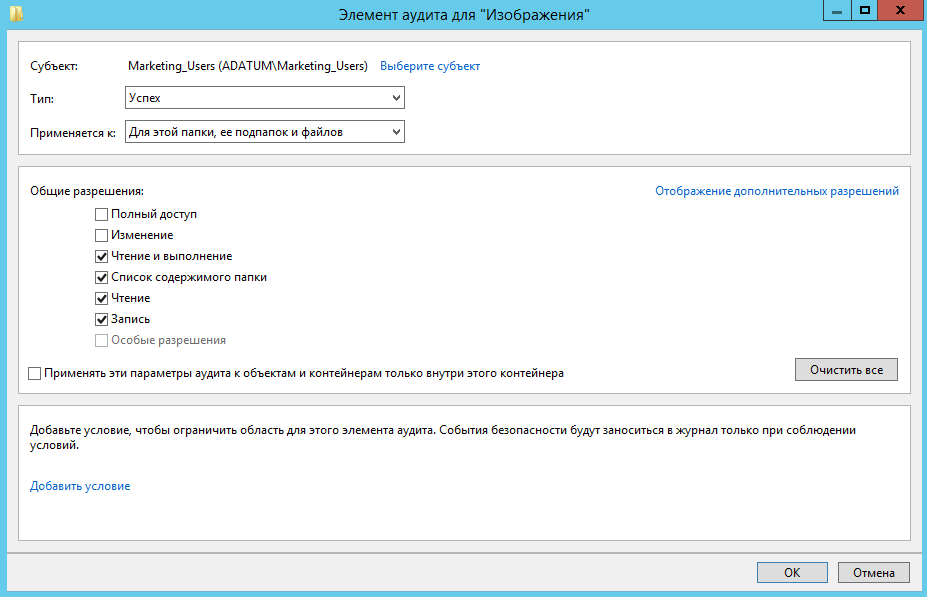


Рисунок 60

## Упражнение 3: Аудит входов в домен

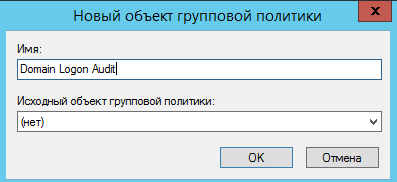


Рисунок 61

Для создания объекта групповой политики Domain Logon Audit, предназначенного для настройки аудита входа в домен, выполните следующие действия.

Откройте консоль Управление групповой политикой (GPMC) через Диспетчер серверов → Средства → Управление групповой политикой. В дереве консоли выберите нужный домен или подразделение, щелкните правой кнопкой мыши и выберите "Создать объект групповой политики в этом домене и связать его здесь". Присвойте имя Domain Logon Audit и нажмите OK.

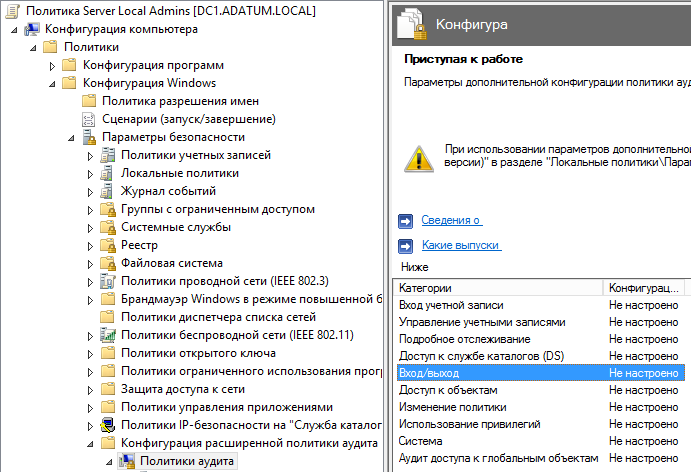


Рисунок 62

При настройке расширенного аудита входа/выхода в системе через объект групповой политики Domain Logon Audit необходимо выполнить следующую последовательность действий. После открытия редактора групповых политик и выбора созданного объекта перейдите по указанному пути: Конфигурация компьютера → Политики → Конфигурация Windows → Конфигурация расширенной политики аудита → Политики аудита → Вход/Выход.

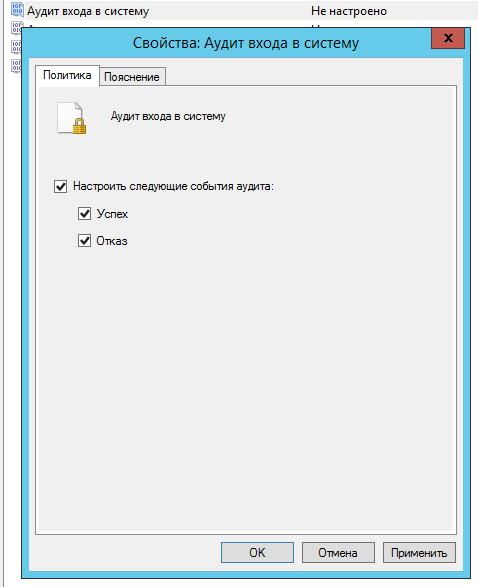


Рисунок 63

При настройке расширенной политики аудита для событий входа/выхода в объекте групповой политики Domain Logon Audit выполните следующие действия. В разделе Конфигурация компьютера → Политики → Конфигурация Windows → Конфигурация расширенной политики аудита → Политики аудита → Вход/Выход выберите категорию "Аудит входа в учетную запись". Необходимо выбрать и «Успех», и «Отказ».

# Лабораторная работа 7.3: AppLocker и Брандмауэр

## Упражнение 1: Настройка AppLocker

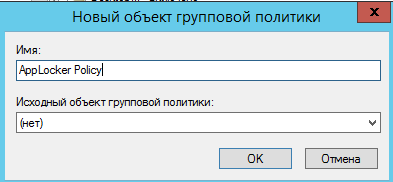


Рисунок 64

Для настройки AppLocker через групповую политику выполните следующие действия. В Диспетчере серверов выберите раздел "Средства" и перейдите в оснастку "Управление групповой политикой". В консоли GPMC найдите нужное подразделение, щелкните правой кнопкой мыши и выберите "Создать объект групповой политики в этом домене и связать его здесь". Присвойте новому объекту имя "AppLocker Policy" и подтвердите создание.

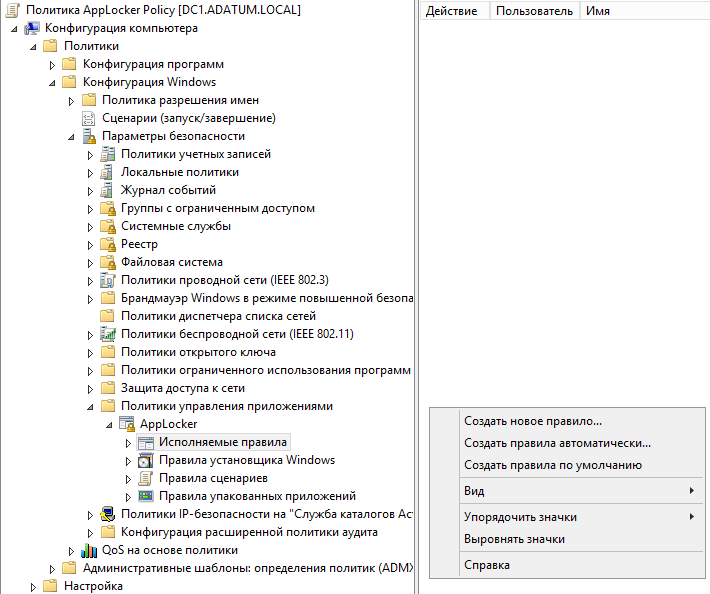


Рисунок 65

После выбора пункта "Создать правила по умолчанию" в разделе "Исполняемые правила" AppLocker автоматически генерирует базовый набор разрешающих правил, обеспечивающих корректную работу операционной системы.

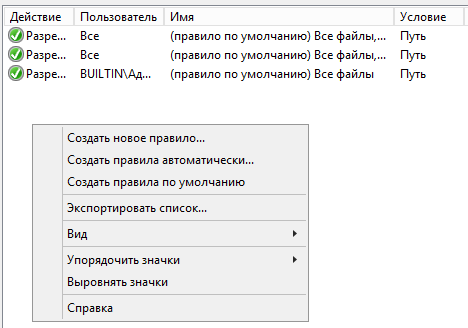


Рисунок 66

Для создания нового правила в разделе "Исполняемые правила" AppLocker выполните следующие действия. В редакторе групповых политик, открытом для объекта AppLocker Policy, перейдите по пути: Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики управления приложениями → AppLocker → Исполняемые правила. В правой панели выберите "Создать правило", что запустит мастер настройки нового правила.

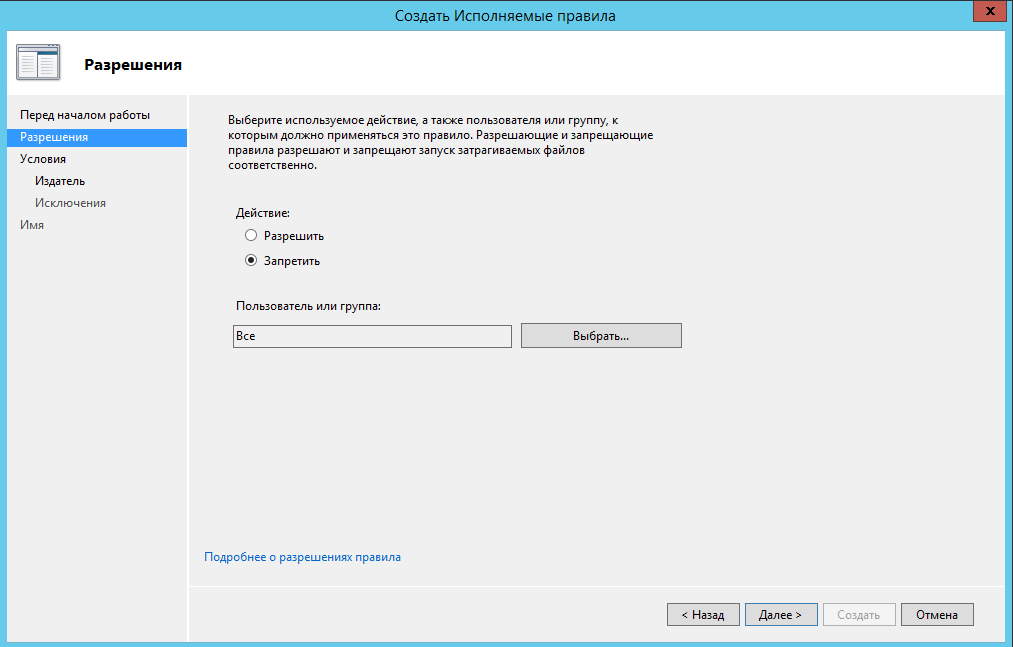


Рисунок 67

При настройке запрещающего правила в AppLocker необходимо выполнить следующие действия. В мастере создания правила на странице "Разрешения" установите переключатель в положение "Запретить", что обеспечит блокировку выполнения файлов, соответствующих заданным условиям. В поле "Пользователь или группа" следует указать "Все", чтобы правило применялось ко всем учетным записям на компьютере, кроме исключений, определенных в других правилах.

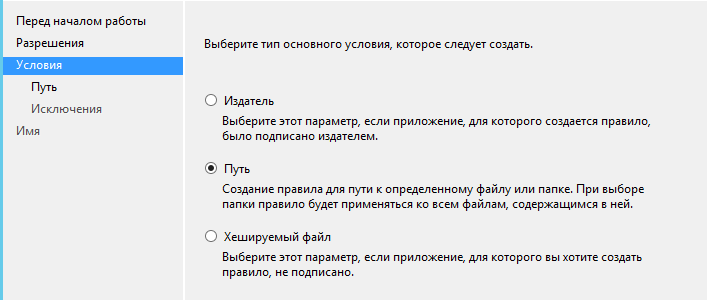


Рисунок 68

При выборе условия "Путь" в мастере создания правила AppLocker необходимо указать конкретные расположения файлов в файловой системе, к которым будет применяться данное правило. В поле ввода следует указать полный путь к папке или конкретному файлу, используя при необходимости стандартные переменные окружения Windows.

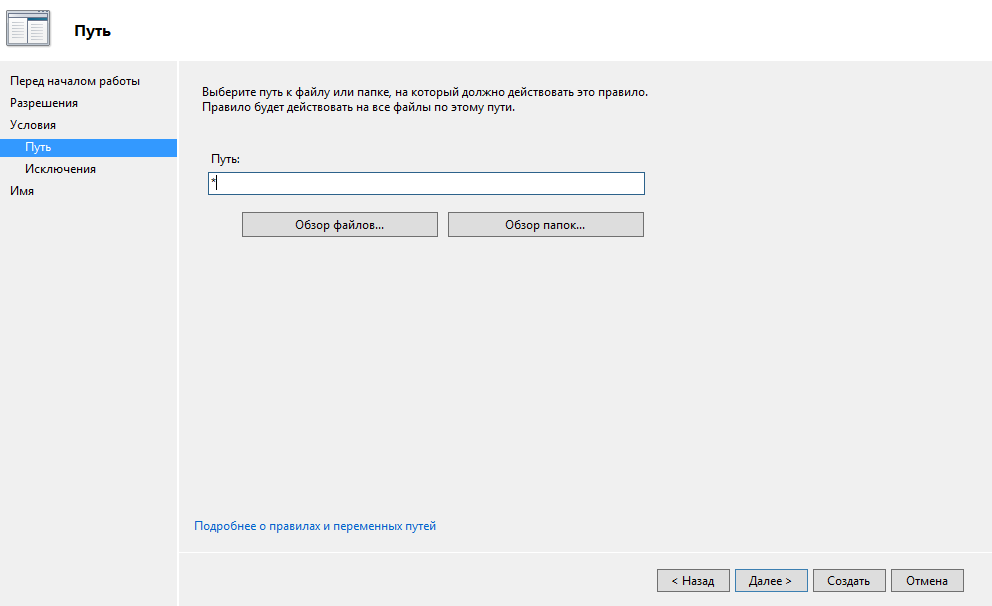


Рисунок 69

При настройке условия "Путь" в мастере создания правила AppLocker указание символа \* в соответствующем поле имеет следующие последствия. Данный символ является подстановочным знаком и означает применение правила ко всем файлам выбранного типа во всех возможных расположениях файловой системы.

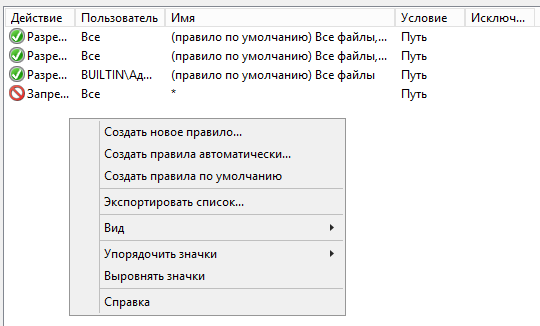


Рисунок 70

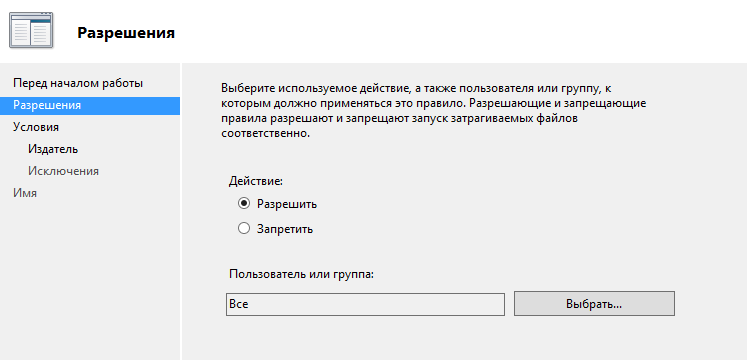


Рисунок 71

При настройке разрешающего правила в AppLocker на странице «Разрешения» необходимо выбрать параметр «Действие: Разрешить», что позволит задать исключения из общих запрещающих политик. После выбора этого действия укажите целевую группу пользователей (например, «Все» или конкретные AD-группы), для которых будет действовать разрешение

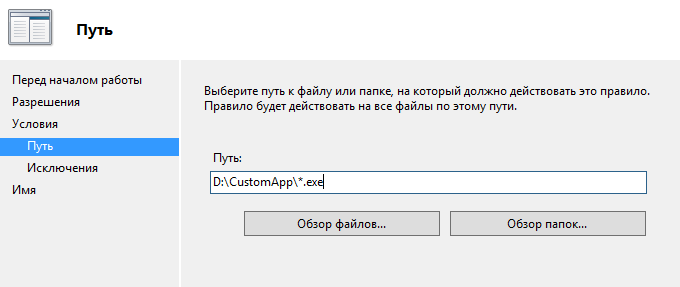


Рисунок 72

При настройке разрешающего правила AppLocker с условием пути необходимо указать точное расположение разрешенных исполняемых файлов. В поле "Путь:" введите значение "D:\CustomApp\*.exe", что позволит выполнять только EXE-файлы, находящиеся в указанной директории и ее подпапках (за счет символа \*).

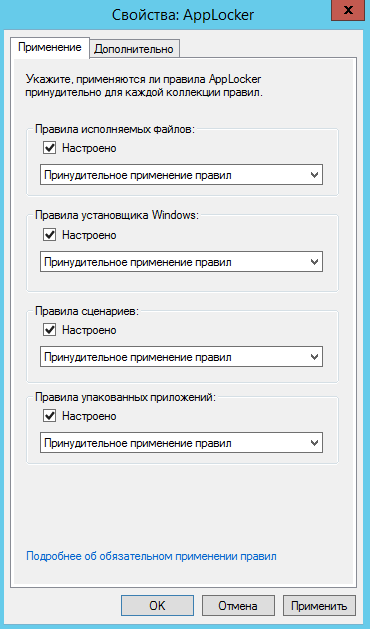


Рисунок 73

# Упражнение 2: Настройка Брандмауэра Windows

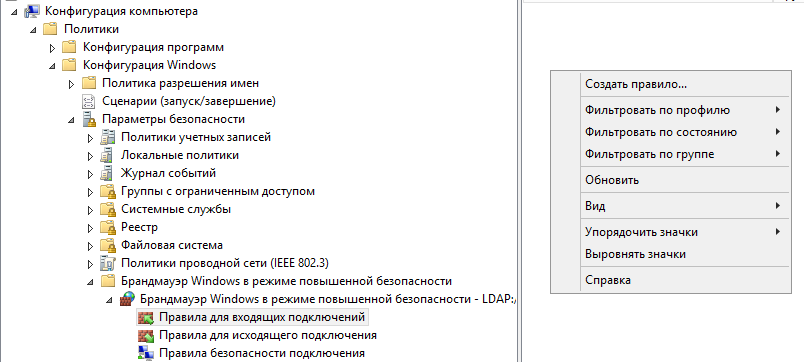


Рисунок 74

Для настройки правил брандмауэра в рамках созданного объекта групповой политики AppLocker Policy выполните следующие действия. После открытия редактора групповых политик для изменения указанного объекта перейдите по пути: Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Брандмауэр Windows в режиме повышенной безопасности → Правила для входящих подключений.

В данном разделе можно создавать и настраивать правила фильтрации входящего сетевого трафика. Для добавления нового правила нажмите правой кнопкой мыши в правой панели и выберите "Создать правило".

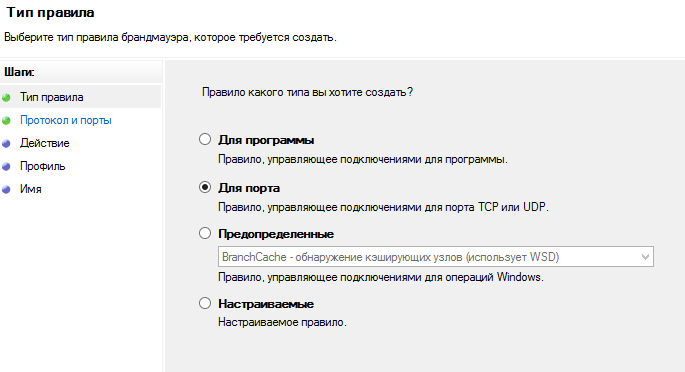


Рисунок 75

При создании нового правила для входящих подключений в рамках групповой политики необходимо выполнить следующую последовательность действий. В мастере создания правила выберите тип "Для порта", что позволит настроить фильтрацию входящего трафика на основе номеров портов.

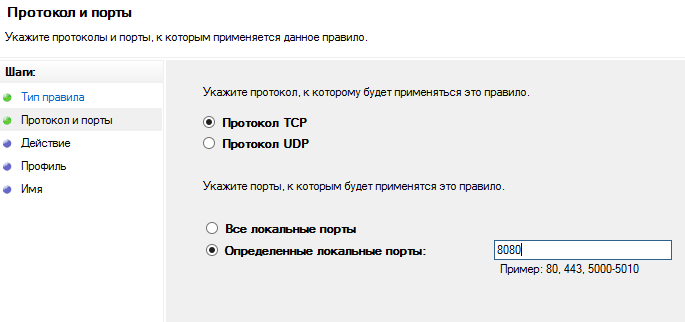


Рисунок 76

На данном шаге следует выбрать протокол TCP и порт 8000.

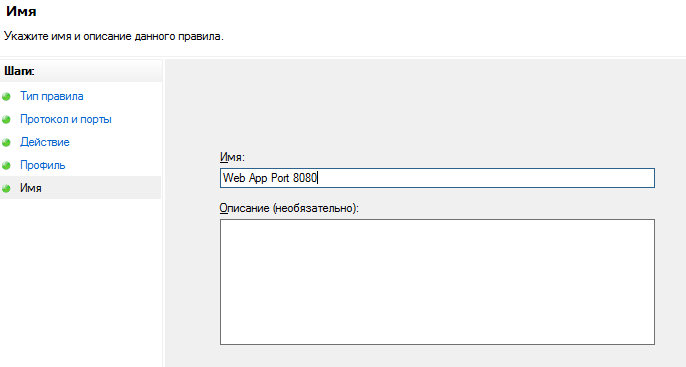


Рисунок 77

Следует указать имя правила.