

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная
безопасность систем и технологий»

Специальность 100502 –

Информационная
безопасность

телекоммуникационных систем

Специализация -

Разработка защищенных
телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

ДИНАМИЧЕСКИЙ КОНТРОЛЬ ДОСТУПА В ОС WINDOWS

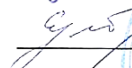
SERVER 2012R2

Студент



Пастухов К.А.

Руководитель



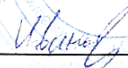
Сулов В.А.

Нормоконтролёр



Фатеев А.Г.

Рецензент инженер 2 категории АО «ПНИЭИ»



Иванов А.Д.

Работа допущена к защите (протокол заседания кафедры от 12.01.17

№ 6)

Заведующий кафедрой



С.Л. Зефирев

Работа защищена с отметкой _____ (протокол заседания ГЭК

от _____ № _____)

Секретарь ГЭК

А.Г. Фатеев

Пенза 2016

 Проверено С.Л. Зефирев

РЕФЕРАТ

Отчет 71 с., 10 источников, 30 рисунков, 1 таблица, 1 приложение.

ОПЕРАЦИОННАЯ СИСТЕМА, ДОСТУП, ОБЪЕКТ, ACTIVE DIRECTORY, КЛАССИФИКАЦИЯ, WINDOWS SERVER 2012, ПРАВИЛА ДОСТУПА, ПОЛИТИКА ДОСТУПА, ТИПОВЫЕ АТАКИ.

Целью дипломной работы является исследование технологии динамического контроля доступа.

В процессе работы был сделан обзор возможностей и преимуществ динамического контроля доступа, рассмотрены серверные роли, описаны отличия динамического контроля доступа от списков контроля доступа, представлены различные виды классификации в автоматическом и ручном режиме.

Также были описаны основные сценарии использования динамического контроля доступа, была реализована настройка требуемой централизованной политики. Далее проведено исследование преимуществ динамического контроля доступа при реализации типовых атак.

В результате работы была исследована данная технология, описана полная пошаговая настройка, включая настройку контроллера домена, представлена база сведений для реализации и внедрения различных централизованных правил и политик доступа, а также описаны достоинства использования данной технологии с точки зрения информационной безопасности.

ОГЛАВЛЕНИЕ

Введение.....	6
1 Возможности и преимущества динамического контроля доступа	8
2 Сценарии использования динамического контроля доступа	15
3 Создание списков свойств ресурсов.....	22
4 Классификация файлов.....	24
5 Настройка и применение централизованной политики доступа.....	27
6 Преимущества динамического контроля доступа при реализации типовых атак.....	60
Заключение	69
Список литературы	70
Приложение А Протокол проверки ВКР в системе «Антиплагиат»	71

ОПРЕДЕЛЕНИЯ

В настоящем отчете применяют следующие термины с соответствующими определениями.

Безопасность информации – состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность [2].

Централизованные политики доступа — политики авторизации, включающие условные выражения [6].

Условные выражения — это усовершенствование управления доступом, разрешить или запретить доступ к ресурсам при выполнении определенных условий, например, членство в группе, расположение или состояние безопасности устройства [6].

Утверждение — это уникальная деталь информации о пользователе, устройстве или ресурсе, опубликованная контроллером домена [6].

Лес — совокупность всех объектов, атрибутов и правил в Active Directory.

Контроллер домена — сервер, контролирующий область компьютерной сети.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ACL	–	access control list
AD	–	active directory
DAC	–	dynamic access control
DHCP	–	dynamic host configuration protocol
DNS	–	domain name system
IT	–	информационные технологии
NTFS	–	new technology file system
ОС	–	операционная система
ТС	–	техническое средство
ЦПД	–	централизованное правило доступа

ВВЕДЕНИЕ

Интенсивное развитие современных информационных ресурсов и технологий в различных сферах жизни общества, привело к появлению в большинстве организаций автоматизированных рабочих мест и организации информационных систем.

В эпоху IT создание и обработка данных происходит с огромной скоростью в различных сетях и системах. Доступ к данным происходит круглосуточно с различных устройств, в том числе и с мобильных.

Конфиденциальная информация является ценным активом многих организаций, и её защита должна обеспечиваться таким образом, чтобы избежать утечек информации за пределы компании. Использование данной информации посторонними лицами может пагубно повлиять на дальнейшую судьбу всей компании. Для решения данной проблемы, нужно контролировать получение доступа к определённой информации, а также следить, чтобы при реализации контроля, сведения о доступе были максимально наглядны.

DAC - это новая система контроля доступа, которая была внедрена в Server 2012. DAC включает в себя модель контроля доступа на основе утверждений-клаймов (claims-based access control — CBAC) с моделью ОС Windows и AD. Клаймы представляют своеобразные утверждения о пользователях или устройствах (например, «моя учебная группа в университете 11ПТ1», «Я работаю на кафедре международных отношений» и т.д.), которые выпускаются проверенными источниками [5].

В данную технологию были добавлены многочисленные изменения в ключевые компоненты, службы и протоколы Windows.

Они затрагивают AD, групповую политику, DNS, Kerberos, Local Security Authority, а также сетевых протоколов и удаленный вызов процедур.

В рамках дипломной работы будут рассмотрены сценарии использования, возможности и преимущества динамического контроля доступа, создание и настройки списков свойств ресурсов, классификация

файлов, правила и политики доступа, а также преимущества динамического контроля доступа при реализации типовых атак.

1 Возможности и преимущества динамического контроля доступа

С помощью доменных служб AD можно проводить эффективное управление доступом и идентификацией. Данная служба представлена в виде пяти ролей. Основной задачей роли «Доменные службы AD» является выполнение операций, обеспечивающей идентификацию и доступ. Данная сфера включает задачи, реализующие проверку подлинности и авторизацию, кроме того, существует возможность создания и управления безопасностью, сайтами, службами, а также доверительными отношениями. Сюда же была отнесена централизованная настройка рабочих мест, реализуемая средствами функциональных возможностей групповой политики.

Кроме того, были рассмотрены следующие четыре роли, с помощью которых можно показать возможности применения доменных служб AD:

- службы сертификации AD, а точнее Active Directory Certification Services (AD CS). Для создания центра сертификации для присвоения цифровых сертификатов, которые привязывают объект идентификации к определенному частному ключу, компании имеют возможность использовать службы сертификации в инфраструктуре Public Key Infrastructure. Данные службы созданы для предоставления эффективного и безопасного метода выдачи сертификатов и управления ими;
- службы управления правами AD – Active Directory Rights Management Services, то есть AD RMS. С помощью данной серверной роли была реализована технология для защиты сведений, и теперь можно применять шаблоны устойчивых политик использования, задающих разрешенное и неавторизованное применение в сети и вне её, а также до и после работы брандмауэра;
- службы федерации AD (Active Directory Federation Services, AD FS). Благодаря данным службам, организация получила возможность развить инфраструктуру идентификации и доступа

на множестве платформ, и работать не только в Windows, а также обеспечивать для проверенных партнеров защиту прав IDA (Identity and Access) за границей периметра безопасности. Также необходимо отметить, что организациям была предоставлена возможность поддержки и контроля своих объектов идентификации;

- службы облегчённого доступа к каталогам, Active Directory Lightweight Directory Services, или AD LDS. Пятая роль представляет собой каталог LDAP, который сохраняет данные приложений, которым нужен доступ к хранилищу ресурсов, но информацию о которых не следует распространять на все контроллеры домена.

Кроме рассмотренных ролей были добавлены возможности развёртывания контроллеров домена только для чтения, виртуализация контроллеров домена, а также такие новые возможности, как активация ОС через AD и историю командлетов Windows PowerShell, был сделан вывод, что возможности Active Directory имеют огромный потенциал. В результате обзора предоставления доступа к информации были отмечены следующие недостатки:

- права на основе NTFS не позволяют контролировать доступ к документам согласно определенной строгой классификации файлов;
- не позволяют проводить аудит согласно каким-либо специфическим политикам;
- не предоставляют возможности генерации «заявок на доступ».

Вышеперечисленные недостатки были устранены с выходом серверной операционной системы Windows Server 2012, так как была внедрена новая технология, называемая динамическим контролем доступа (Dynamic Access Control), позволяющая управлять доступом к информации на основе

конкретных атрибутов, определённых критериев с использованием логических выражений.

Далее были рассмотрены отличия и преимущества динамического контроля доступа от списков контроля доступа. Динамический контроль доступа позволил по-новому взглянуть на механизм предоставления общего доступа к ресурсам организации, расположенным на контроллерах домена и файловых серверах, работающих под управлением операционной системы Windows Server 2012. Для сравнения был выполнен анализ предоставления доступа до выхода DAC.

Общий ресурс — это объект, предполагающий использование несколькими пользователями с разных компьютеров. К общим ресурсам можно отнести как устройства, например, принтер, так и папки с файлами.

В AD регулирование доступом происходило на уровне объектов. Для них назначались разные уровни доступа или разрешения, такие как «Чтение», «Нет доступа», «Полный доступ» или «Запись». Разрешения управления доступом, находятся в их дескрипторах безопасности [8].

В дескрипторе безопасности содержатся два ACL, используемые для назначения и контроля сведений безопасности по каждому объекту. Рассмотрим их более подробно:

- избирательные таблицы управления доступом (Discretionary access control list, DACL). В DACL указываются пользователи и группы, которым разрешён или запрещён доступ к объекту. Если определённый пользователь или группы, в которые он входит, не указаны в DACL, данному пользователю будет запрещён доступ к объекту. По умолчанию DACL управляется владельцем объекта или пользователем, создавшим этот объект, и содержит записи управления доступом (ACE — Access control entries), определяющие доступ пользователя к объекту [9];
- системные таблицы управления доступом (System access control list, SACL). В SACL указываются пользователи и группы, для

которых требуется выполнять аудит успешных и безуспешных попыток доступа к объекту. Аудит необходим для наблюдения за событиями, связанными с безопасностью системы или сети, для обнаружения недостатков в системе безопасности, а также для определения объемов и места нахождения любых повреждений. SACL управляется владельцем объекта или создавшим его пользователем. SACL включает в себя записи управления доступом, определяющие, требуется ли фиксировать любые попытки доступа пользователя к объекту с использованием конкретного разрешения, например, «Чтение» или «Запись» [9].

DACL и SACL связаны с каждым объектом AD, что повышает защиту от сетевых атак злоумышленников и случайных ошибок пользователей домена. Лес станет уязвим в случае, если недоброжелателю станет известно логин и пароль учетной записи администратора AD.

По умолчанию объекты AD наследуют ACE из дескриптора безопасности объекта родительского контейнера. Наследование позволяет использовать сведения управления доступом, которые были определены для объекта контейнера AD, к дескрипторам безопасности любого подчиненного объекта, включая остальные контейнеры и их объекты. Это помогает избежать необходимости применять разрешения к каждому новому дочернему объекту. При необходимости существует возможность изменить наследуемые разрешения.

Далее был рассмотрен процесс авторизации пользователя. Он состоит из двух частей:

- пользователь предоставляет параметры доступа, обычно имя пользователя и пароль, которые затем подвергаются проверке в базе данных AD DS. В случае если данные совпадают с информацией из базы, тогда пользователь получает статус авторизованного, и для него выписывается билет контроллером

домена, с помощью которого он на следующем шаге получит другой билет для доступа к ресурсам сети;

- на данном этапе происходит передача билета контроллеру домена на проверку, а также осуществляется запрос на получение доступа к локальному компьютеру. Далее контроллер домена выдает или не выдает билет на доступ пользователю к ресурсам локального компьютера. После выполнения данных действий, если билет был выдан, то пользователь считается авторизованным в AD DS и зарегистрированным на локальном компьютере.

Компьютер, соединенный с доменом, тоже проходит процедуру авторизации в AD DS при запуске. Транзакции не видно, когда компьютер использует свое имя учетной записи и пароль для авторизации в доменных службах AD. После проверки подлинности, компьютер входит в группу авторизованных пользователей. Процесс авторизации компьютера не имеет визуального подтверждения в графическом интерфейсе пользователя, но существуют протоколы событий, фиксирующие данную активность. Также если включен аудит, в журнале безопасности Event Viewer будет показано больше событий, доступных для просмотра.

Далее более подробно были рассмотрены преимущества DAC.

Рассмотрев способ предоставления доступа на основе ACL можно отметить что данный метод основан на членстве пользователя в той или иной группе в AD. Отсутствует возможность ограничивать или, наоборот, разрешать доступ для определенного устройства пользователя, основываясь на дополнительных характеристиках, а также, отсутствует возможность реализации сложных и нестандартных сценариев.

С помощью динамического контроля доступа появилась возможность снять данные ограничения и создавать более сложные правила и нестандартные правила, опираясь на которые, можно предоставлять доступ согласно различным критериям и атрибутам. В начале было обращено внимание на то, что данная технология позволяет управлять доступом к

файлам и данным посредством создания централизованных политик доступа, позволяя более подробным образом определять, кто получает доступ к определенной информации. Появилась возможность создавать такие политики, которые будут наилучшим образом отражать деятельность организации и полностью соответствовать любым нормативным требованиям. Помимо этого, идентифицировать такую информацию можно при использовании классификации файлов, в различных режимах, о которые будут описаны далее. Учитывая эти возможности, можно увидеть превосходство динамического контроля доступа над управлением доступом при использовании списков ACL.

Наиболее распространенные типы данных, к которым предоставляют доступ, – это офисные документы, то есть файлы, которыми можно управлять при помощи продуктов Microsoft Office. Были изучены способы каким образом ранее использовались уникальные разрешения с шифрованием документов, для каждого такого документа использовалась служба управления правами AD RMS. Даная технология отлично себя показала и сейчас, с появлением DAC, появилась возможность применения защиты RMS, с использованием автоматического шифрования на основе определенных критериев.

В современном мире, конфиденциальная информация является ценным активом многих организаций, и её защита должна обеспечиваться таким образом, чтобы избежать утечек информации за пределы компании. Использование данной информации посторонними лицами может пагубно повлиять на дальнейшую судьбу всей компании. С помощью централизованных политик аудита данной технологии, можно контролировать время и доступ того или иного субъекта к конфиденциальной информации, создавать отчеты для дальнейшего проведения аудита доступа к файлам или же, в случае крайней необходимости, криминалистического анализа. Таким образом повышается вероятность избежать использования сторонних приложений и программных продуктов.

Также было выделено что текущую технологию можно использовать, не внося изменений в схему AD, без развертывания дополнительных ролей и применения специального программного обеспечения. Можно подчеркнуть, что для внедрения DAC компанией Microsoft были созданы новые механизмы аудита и авторизации.

2 Сценарии использования динамического контроля доступа

В данном разделе дипломной работы были выделены и описаны семь основных сценариев использования динамического контроля доступа.

Централизованное развертывание политик авторизации. Одной из главных задач данной технологии является создание централизованных политик доступа для файлов и папок организации, позволяющих предоставлять пользователям или их устройствам доступ к ресурсам на основании конкретных критериев, а также, управление такими политиками. Создаются они индивидуально для каждой компании, что делает эту технологию особенно ценной и гибкой. Далее представлена реализация данного сценария.

Сначала необходимо оценить направление деятельности организации и определиться с тем, каким образом будут работать такие политики. Нужно определить какие именно ресурсы требуется защищать, необходимо локализовать данные ресурсы. Далее требуется создать список всех политик, которые будут применяться в своей среде. Требуется продумать по каким критериям лучше ограничивать доступ, это будет зависеть от количества отделов, физического расположения и так далее.

Потом необходимо политику отразить в форме, понятной для сервера. Таким образом, следующим этапом внедрения сценария является конвертация необходимой политики доступа в выражение, понятное для ОС. Политики, очень легко и быстро преобразуются из обычной, словесной формы, в логическое выражение.

То есть такие политики доступа обладают правами применимости, условиями доступа и исключениями.

Далее необходимо определить следующие параметры для реализации нужной политики:

- группы пользователей;
- составить список используемых утверждений;
- определить свойства ресурсов.

Необходимо провести анализ и сделать соответствия всех защищаемых ресурсов и всех примененных утверждений. В данном случае можно избежать создания и применения излишнего количества утверждений.

Последний пункт включает в себя определение серверов, на которые будут распространяться созданные централизованные политики доступа.

Распространять централизованные политики можно двумя способами, сразу на все серверы, так и на выборочно.

Развертывание заявок на доступ между лесами. ОС Windows Server 2012 была разработана так, что словари утверждений могут быть использованы в нескольких лесах, их определение происходит на уровне доменных служб AD.

Утверждения относятся к объектам, с которыми они связаны, и для каждого леса AD определяются индивидуальные типы утверждений.

Доверяющий лес быть использован для изменения утверждений во избежание атак, связанных с повышенными привилегиями, с помощью фильтрации входящих утверждений согласно определенным значениям. Они по такому же принципу выдают утверждения для принципалов через границы доверия в том случае, если доверенные леса не поддерживают, или не выпускают определенные утверждения.

Доверенные леса могут использовать изменения клэймов с целью помехи определенным типам утверждений.

В формировании политик преобразований утверждений привлечены два компонента, объекты политики преобразования утверждений и ссылки преобразования.

Улучшенная поддержка пользователей, которым было отказано в доступе. Для лучшего понимания представлена стандартная ситуация. Пользователь Петров пришел на работу и получил задачу, которая связана с определенной информацией, имеющей ограниченный доступ и которая расположена на файловом сервере, но у Петрова доступа к ней нет. Затем этот сотрудник открывает общую папку и в процессе открытия появляется следующее сообщение «В доступе отказано». Затем этот сотрудник звонит в

службу поддержки и в понятной для пользователя форме он пытается объяснить, к какой информации ему нужен доступ, с какой целью она ему необходимо, описывает расположение данной документации и так далее.

С помощью правильного применения данной технологии можно дать возможность такому сотруднику и владельцу этих данных справиться подобными проблемами, не прибегая к посторонней помощи. В случае если проблема не была решена, то пользователь может, например, заполнить заранее сформированную веб-форму и передать нужные сведения в определенном виде.

Однако при реализации данного сценария есть свои трудности. Таких сценариев, связанных с отказами в доступе может быть очень много, причем каждая такая ситуация может быть сугубо индивидуальной и не похожей на другие. Поэтому продумать единое решение для всех случаев просто невозможно. Но можно, пойти следующим путем. Первым делом необходимо определиться с тем, как будет предоставляться первичная помощь при возникновении отказа в доступе.

Были рассмотрены возможные варианты. Первый вариант что при возникновении такого сообщения у пользователя сразу отображалось сообщение с соответствующей кнопкой, с помощью которой можно отправить владельцу данной папки письмо по электронной почте.

Второй вариант это вместо кнопки можно сформировать ссылку, сделав переход по которой сотруднику нужно будет заполнить заранее сформированную веб-форму. В данном случае все зависит от структуры и деятельности организации, а также каким образом будет проще реализовать данную поддержку.

После этого нужно указать уполномоченных лиц, например, администраторов, владельцев ресурсов, которым будут доставлены все эти пользовательские запросы.

Далее следует настроить сам шаблон сообщения, которое будет отображено пользователю при отказе в доступе.

В случае необходимости, нужно проработать все возможные исключения. Рекомендуется, чтобы это было сделано на этапе планирования.

В конце концов, нужно продумать план, согласно которому будет оказана помощь на уровне самого файлового ресурса. Таким образом можно указать в выводимом сообщении уполномоченных лиц или выполнить какие-либо дополнительные действия.

Фильтрация конфиденциальной информации при помощи классификации файлов. В современном мире одним из важных активов компаний является их конфиденциальная информация. Как правило, не обычные пользователи, а именно IT-работники отвечают за сохранность такой информации и, естественно, за назначение прав только лишь определенным лицам.

Необходимо контролировать не только чтобы такая документация была всегда доступна пользователям, и они были с ней ознакомлены, и чтобы ресурсы таких хранилищ не истощались, а нужно еще проверять чтобы ресурсы были использованы наиболее эффективно и по назначению. Описанные выше задачи целесообразно реализовывать при определенных политиках, потому что назначать подобные права и остальные возможности необходимо централизованно.

ОС Windows Server 2012 вместе с технологией DAC позволяют использовать классификацию ресурсов, что позволяет получить общую картину среди всех ресурсов организации, причем, можно полностью автоматизировать этот процесс несколькими способами, тем самым сэкономив свое время. Существует несколько способов классификации. Можно выбрать ручной метод, программный, или применять автоматические режимы классификации файлов. Каким образом следует поступать, зависит в частности от организации.

Первым шагом необходимо составить полный список всех возможных файлов, которые можно найти в вашей организации. Такие действия следует

выполнять для того, чтобы в дальнейшем использовать классификацию и знать, какие ресурсы будут подлежать самой классификации.

После выполнения первого шага, следует выбрать способы классификации таких файлов. Существует возможность в ручном режиме провести классификацию файлов, используя соответствующие средства, можно сделать классификацию на основе расположения, причем выполнять это все можно как в ручном режиме, так и в автоматическом с помощью классификатора папок. Также предусмотрено выполнение классификации на основе содержимого.

Защита конфиденциальной информации на основе классификации документов Microsoft Office. AD RMS. Для компании может быть важно не только предоставление доступа к различной конфиденциальной информации, но также очевидно и то, что информацию нужно хранить в защищенном виде. Общепринятым методом защиты секретной информации является шифрование.

Для шифрования текстовых документов хорошо показала себя служба управления правами Active Directory. А сейчас, с выходом Windows Server 2012, появилась возможность автоматизировать процесс шифрования документов, основанных на классификации файлов Microsoft Office, практически в прозрачном режиме, причем сразу же после создания данных файлов. Необходимые действия для настройки данного сценария описаны далее.

Сначала необходимо определиться с файлами, которые шифроваться в автоматическом режиме. Файлы на ресурсах могут быть не только конфиденциальными, а они еще и могут обладать личностным характером. Таким образом в первую очередь необходимо определить какие именно файлы должны подлежать автоматическому шифрованию. После этого требуется определить согласно каким именно свойствам ресурса будут определяться такие типы файлов. Для этого нужно воспользоваться предустановленными свойствами ресурсов, либо создать свои собственные, уникальные свойства

ресурсов, которые и будут использоваться для определения файлов, которые подлежат шифрованию.

Далее требуется определить шаблоны политики прав, которые будут использоваться при шифровании таких файлов. Они уже используются непосредственно службой AD RMS. Таким образом нужно выбрать принципы безопасности и указать права, которые для них будут доступны при использовании таких файлов. Здесь уже многое зависит от требований самой организации, от разрешений групп пользователей, а также от того, насколько большую ценность имеют такие файлы. Например, возможно разрешить просматривать определенные документы группе менеджеров, но ограничить им возможности изменения и печати. Вариантов применения службы управления правами для файлов неограниченное множество, все зависит от бизнес-требований организации.

Кроме этого, используя данную технологию, можно ознакомить партнеров со своими файлами, не беспокоясь, что с файлами будут выполнены неправомерные действия.

Создание периодов хранения информации на файловых серверах. Период хранения — это время в течении которого происходит хранение документа, после чего он будет считаться просроченным. Таким образом, этот период может быть различен у разных файлов.

Файлы можно классифицировать как кратко-, средне- и долгосрочные для хранения, а после этого уже можно для определенного периода отметить временные рамки. Следовательно, для управления периодами хранения, технология динамического контроля доступа использует инфраструктуру классификации файлов совместно с диспетчером ресурсов файлового сервера. Если срок хранения заканчивается, владелец получит по электронной почте соответствующее уведомление.

Реализация такого сценария выглядит следующим образом. Первым делом, необходимо определить, как долго смогут храниться различные файлы на ресурсах компании, учитывая повышение отказоустойчивости, а также

сокращение объема сохраненных данных. Это важные факторы, и поэтому при разработке такого расписания обязательна консультация с уполномоченными членами организации.

Затем следует определить тип хранимых данных на своих файловых ресурсах. Далее требуется задать свойства, согласно которым файлы не могут быть случайно удалены конечными пользователями, а также определить свойства классификации.

Аудит доступа к файлам. Также, очень важным сценарием выступает аудит безопасности, позволяющий поддерживать порядок и благополучие в вашей среде. Основная задача данного сценария - это соблюдение порядка в компании и исключение неправомерных действий, которые могут происходить в файловой системе в организации.

Аудит безопасности позволяет отслеживать соблюдение установленных политик, а также позволяет выявлять и предотвращать вероятностные уязвимости, а также предоставляет возможность в случае необходимости выполнять криминалистический анализ.

С DAC для соблюдения аудита безопасности можно выполнять следующие действия:

- производить настройку политики аудита с помощью выражений;
- фиксировать события аудита при каждой попытке доступа к конкретным ресурсам.

3 Создание списков свойств ресурсов

В файловых серверах, работающих под управлением Windows Server 2008 R2 классификация файлов представляет собой инфраструктуру, отвечающую за автоматизацию процессов классификации. Это позволяет определять степени важности, сроки действия, создавать различные отчёты, а также использовать настраиваемые задачи, таким образом понижая возможные риски хранения файлов на файловых серверах. Проводить управление такой классификацией можно было с помощью диспетчера ресурсов файлового сервера (File Server Resource Manager, FSRM). Классификацию можно использовать лишь после установки данной консоли. Таким образом классификация файлов позволяет создавать политики управления файлами для более эффективного управления данными.

С выходом ОС Windows Server 2012, возможности авторизации стали еще больше расширены с помощью добавления к существующей инфраструктуре классификации файлов свойств ресурсов. Для реализации сложных сценариев, связанных с авторизацией, можно использовать несколько условных выражений. Другими словами, теперь администраторы с помощью условных выражений могут производить настройки авторизации доступа к файлам на основании одного или нескольких значений свойств ресурсов.

Далее был рассмотрен пример. На файловых серверах содержится скрытая от большинства пользователей документация, которая так и классифицируется, как Secret. Таким образом, ОС Windows Server 2012 необходимо предоставить доступ к таким файлам, основываясь на секретной информации, которая фигурирует в метаданных самих файлов либо в свойствах ресурса самого файла. Следовательно, если классификация файла включает в себя Secret, но пользователь не обладает разрешениями на просмотр таких данных, ему будет отказано при попытке доступа к последним. Свойства ресурсов бывают двух видов, а именно, свойство ресурса, а также свойство ссылочного ресурса.

Свойство ресурса представляет собой описание конкретной характерной особенности ресурса, в качестве объекта могут выступать файлы или папки. Данное свойство имеет важное значение при создании централизованных правил доступа, а именно служит для определения самих целевых ресурсов, а также непосредственно разрешений. В данных свойствах ресурса отражаются предполагаемые значения, которые определены для самого объекта, и хранятся они в атрибуте `msDS-ClaimPossibleValues` объекта. Также свойство ресурса используется для классификации самого ресурса.

Ссылочное свойство ресурса, представляет собой, свойство ресурса, использующее существующий тип утверждения в качестве своих предложенных значений. Можно выделить следующее, отличием между обычных свойств ресурса и ссылочных то, что ссылочные не хранят свои значения. Они его получают из ссылающегося объекта утверждения.

4 Классификация файлов

Как правило, администраторы при обслуживании своих файловых серверов сталкиваются с разными проблемами, связанными с тем, что увеличение количества сохраняемых данных может влиять на расходы по хранению и управлению такими данными, а также с тем, что на файловых серверах сотрудники организации все чаще вместе с данными компании сохраняют свои личные файлы и документы.

Таким образом был внедрён специфический механизм в серверные ОС, позволяющий локализовать на основании содержимого среди тысяч файлов, сохраненных на файловых серверах, файлы, относящиеся к организации напрямую[1]. На основе проблем, выявленных в ОС Windows Server 2008 R2 впервые появилось такое нововведение, как инфраструктура классификации файлов, которая позволила компаниям проводить классификацию своих файлов путем назначения конкретных свойств, а затем, используя конкретные механизмы ОС Windows, выполнять определенные действия с такими файлами на основе готовой классификации.

Классификация ресурсов включает в себя возможность определения свойств классификации, автоматической классификации файлов, классификации, основанной на сценариях, расположении или содержимом, а также применении задач управления файлами, к которым можно отнести определение срока действия файла, разных пользовательских команд на основании выполненной классификации, а также создание разных отчетов, показывающих распределение классифицированных ресурсов на данном файловом сервере.

Классификация файлов представляет собой рекомендуемый процесс при полноценной реализации такой технологии, как динамический контроль доступа. Благодаря классификации файлов появилась возможность отслеживать использование корпоративных ресурсов только по назначению и наиболее эффективным образом. Таким образом, на данном этапе необходимо определить информацию, которая будет классифицирована, и выбрать

подходящий метод классификации для частного случая. Это тот процесс, во время которого практически не нужно использовать функциональные возможности консоли центра администрирования Active Directory.

Далее рассмотрим, какая может быть связь между такими объектами, как свойства ресурсов, а также классификацией файлов. Ведь сами свойства ресурсов позволяют устанавливать проверочные утверждения для файлов и папок организации. Данные проверочные утверждения, представляют собой некоторые значения, которые самостоятельно указываются при создании свойств ресурсов. Стоит отметить, что у свойств ресурсов есть такая особенность, она состоит в том, что настроенные проверочные утверждения для определенного файла будут с ним связаны даже если данный файл будет скопирован или вообще перемещен из одной файловой системы NTFS на другую, так как сами значения свойств ресурсов сохраняются в альтернативных данных этого файла.

Таким образом можно отметить, что для настройки определенных файлов метаданных для целевых файлов используются именно свойства ресурсов, которые в свою очередь напрямую связаны с инфраструктурой классификации файлов. А уже классифицированными файлами можно управлять в соответствии с требованиями организации, а также существует возможность использовать все возможности динамического контроля доступа.

После успешной установки Windows Server 2012 R2 был установлен контроллер домена. Данный сервер будет выполнять следующие роли:

- доменные службы Active Directory;
- DHCP – сервер;
- DNS – сервер.

Для настройки доменных служб AD были добавлены роли и компоненты в диспетчере серверов.

В меню выбора ролей сервера были выбраны следующие компоненты:

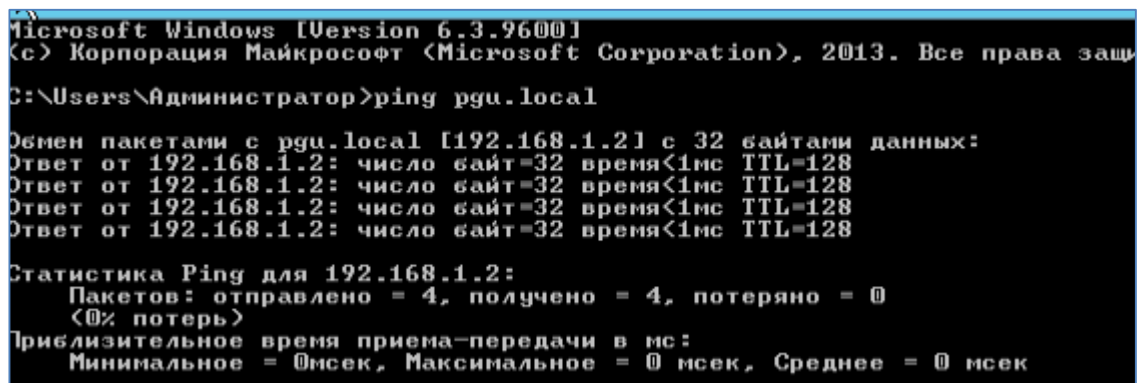
- доменные службы Active Directory;
- DHCP – сервер;

- DNS – сервер;
- файловые службы и службы хранилища.

Далее была повышена роль данного сервера до уровня контроллера домена. Был создан новый лес и указано имя нового корневого домена – PGU.local.

Затем была завершена настройка DHCP-сервера. Была создана область, задан начальный (192.168.1.1) и конечный (192.168.1.254) адрес сети, а также маска /24 (255.255.255.0). После того, как, в данной области был указан срок действия аренды адреса – 8 дней, была выполнена настройка DNS-сервера.

Проверка данного сервера представлена на рисунке 1.



```
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Администратор>ping pgu.local

Обмен пакетами с pgu.local [192.168.1.2] с 32 байтами данных:
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 1 – Проверка DNS-сервера

5 Настройка и применение централизованной политики доступа

В данном случае речь идет о компании с распределенной структурой с множеством филиалов и сотрудников финансовых отделов.

С помощью динамического контроля доступа была организована следующая политика доступа:

- доступ на чтение финансовой информации должны иметь только сотрудники финансового департамента с привязкой к офису сотрудника;
- руководители финансового департамента должны иметь права на чтение и изменение любой финансовой информации;
- руководители организации имеют право на чтение всей финансовой информации.

Другими словами, на файловом сервере к документам, которые относятся к финансовому отделу доступ на чтение должен иметь тот человек из финансового отдела, который работает в этом же городе.

Стоит отметить, что данная задача также решается классическим способом с помощью пользователей и групп, но количество групп, которые необходимо создать (особенно при большом числе городов), будет весьма велико.

Были созданы следующие пользователи:

- Иванов Иван, сотрудник финансового отдела из г. Пенза;
- Сидоров Алексей, сотрудник финансового отдела из г. Москва;
- Афанасьев Андрей, руководитель финансового отдела;
- Орлов Николай, сотрудник операционного отдела из г. Москва;
- Царегородцев Михаил, руководитель организации.

Перед настройкой динамического контроля доступа был настроен контроллер домена для того чтобы он мог формировать расширенные маркеры доступа с заявками и рабочие станции пользователей. Данные действия были выполнены в групповой политике.

Необходимо открыть политику контролера домена по умолчанию и в папке «административные шаблоны» в подпапке «система» на вкладке «Центр распространения ключей» включить настройку, представленную на рисунке 2.

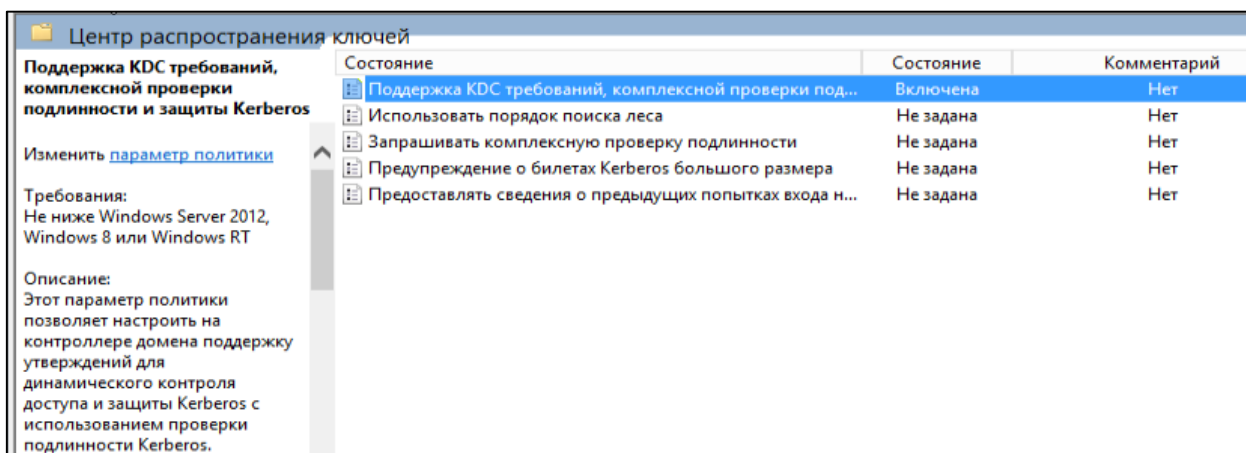


Рисунок 2 – Центр распространения ключей

Таким образом, был настроен контроллер домена на формирование маркеров с учетом заявок. Затем была выполнена настройка рабочих станций в объекте групповой политики папке «административные шаблоны» в подпапке «система» на вкладке «Kerberos» включена настройка, представленная на рисунке 3.

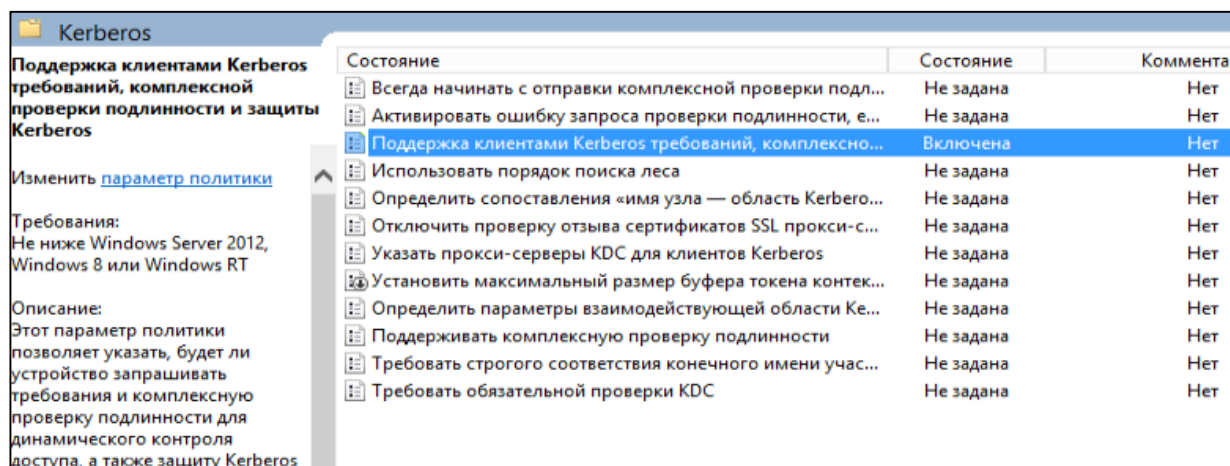


Рисунок 3– Настройки Kerberos

После выполнения предварительных действий, была выполнена настройка политики динамического контроля доступа через консоль Active Directory Administrative Center (AD AC).

Данная настройка выполняется в несколько этапов:

- создание типа утверждений;
- создание свойства ресурса;
- создание централизованного правила доступа;
- создание централизованной политики доступа;
- распространение политики на файловом сервере;
- классификация файлов и папок;
- применение политики доступа к файлам и папкам.

Тип утверждения – это проверочное утверждение об объекте, с которым оно связано. Оно основано на атрибуте Active Directory и служит для определения разрешений при разработке централизованных политик доступа.

Поэтому на *первом этапе* были определены, какие атрибуты учетных записей пользователей или компьютеров будут использоваться при настройке контроля доступа. В данной дипломной работе использовались следующие атрибуты: отделение (department) и город (city). На рисунке 4 продемонстрирован выбор из списка доступных атрибутов атрибута department.

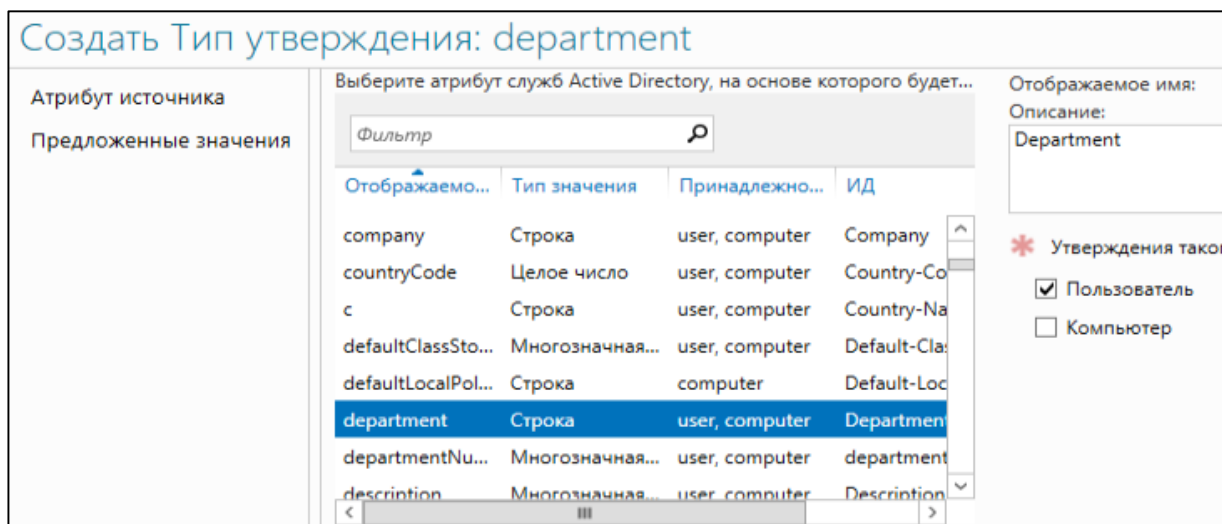


Рисунок 4 – Выбор атрибута

Далее из списка был выбран атрибут Locality-Name, который представляет собой город, в качестве значений использовались города Москва

и Пенза. Результат создания типов утверждений продемонстрирован на рисунке 5.

Отображаемое имя	ИД	Тип исходног...	Источник	Тип знач
Department	ad://ext/department:88d4...	Атрибут	Department	Строка
City	ad://ext/Город:88d4124aa...	Атрибут	Locality-Name	Строка

Рисунок 5 – Результат создания типов утверждений

На *втором этапе* были созданы свойства ресурса. Они описывают характерную особенность ресурса, такого как файл или папка. Свойства ресурса нужны для определения целевых ресурсов и разрешений при создании централизованных правил доступа. Также они используются для классификации ресурсов. Списки свойств ресурсов в какой-то степени можно сравнить с группами безопасности в доменных службах Active Directory. По аналогии с группами безопасности, списки свойств ресурсов позволяют логически сгруппировать созданные ранее объекты свойства ресурса.

С помощью логически сгруппированных созданных списков свойств ресурсов обеспечивается наиболее простая и быстрая настройка DAC. Например, можно для каждого файлового сервера создать свой список свойств ресурсов и в дальнейшем при повторной настройке или восстановлении сократить немало времени.

Открыв центр администрирования AD ОС Windows Server 2012 и Windows Server 2012 R2 было сделан вывод, что по умолчанию системой формируется первый объект, называемый Global Resource Property List. Данный список свойств ресурсов создается для всего леса AD и, так как Global Resource Property List используется на всех файловых хранилищах компании, включенные в этот объект свойства ресурсов, применяются всегда.

Таким образом по этой причине файловые серверы Windows Server 2012/2012 R2 могут включать по несколько списков свойств ресурсов, которые

создаются и настраиваются вручную. С помощью этих списков свойств ресурсов в дополнительных параметрах безопасности и редакторах условных выражений можно увидеть объекты свойств ресурсов безопасности, добавленные в списки свойств ресурсов.

Конфигурируются данные списки свойств ресурсов на файловых серверах, с помощью функциональных возможностей групповой политики.

В целях реализации заданной политики были добавлены свойство ресурса Department и ссылочное свойство ресурса Sity.

Демонстрация второго свойства представлена на рисунке 6.

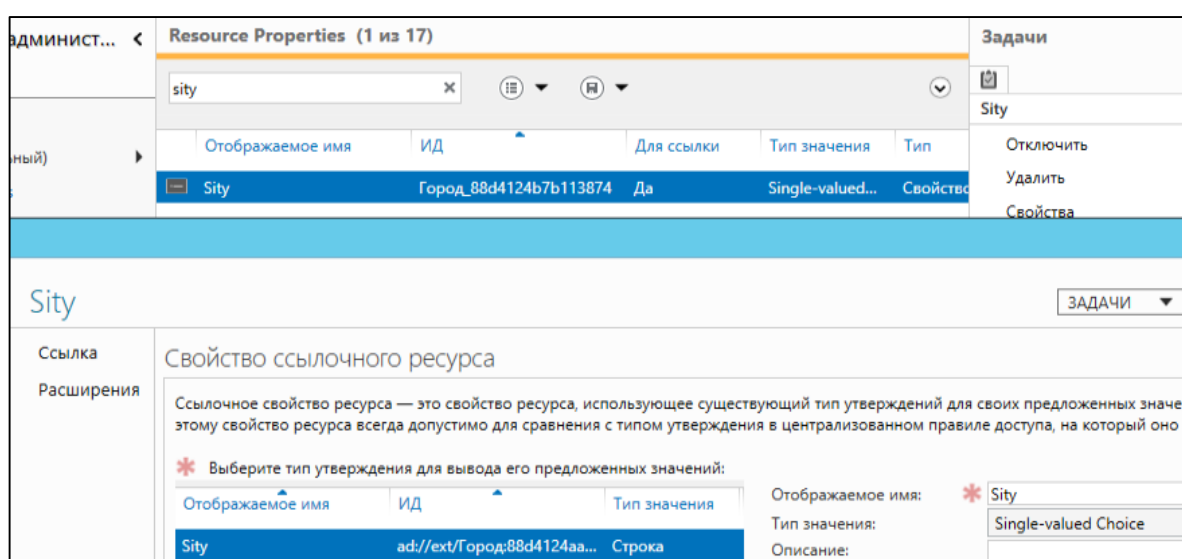


Рисунок 6 – Добавление ссылочного ресурса

После того, как были указаны атрибуты пользователя, которые будут использованы и заданы теги которые должны быть доступны на файловом сервере необходимые для маркировки ресурсов, был сформирован список свойств ресурсов, в котором указаны необходимые для решения задачи атрибуты.

Для реализации заданной политики были заданы следующие атрибуты:

- город;
- отдел.

Создание списка свойств ресурсов продемонстрировано на рисунке 7.

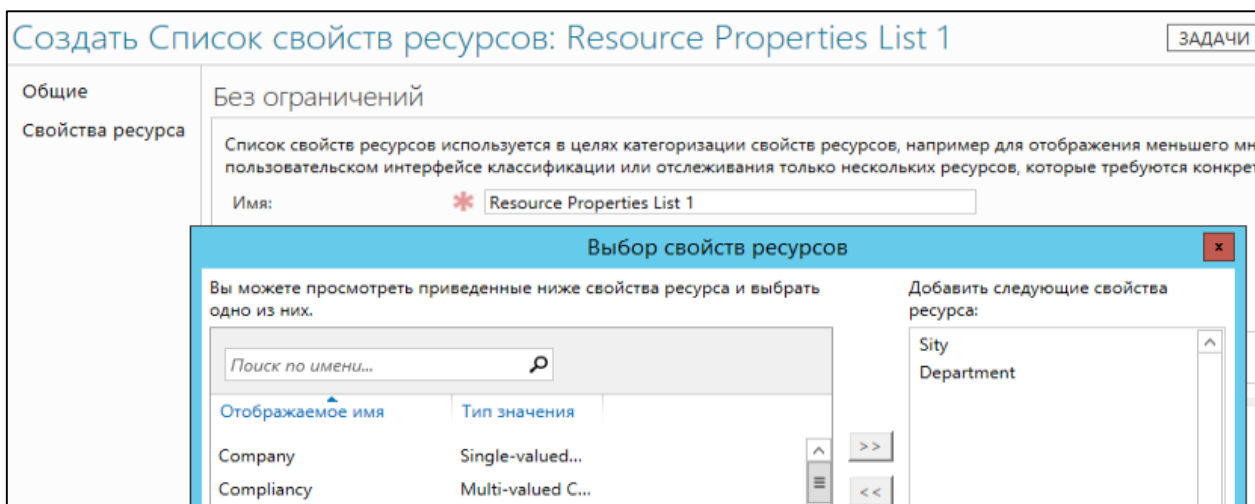


Рисунок 7 – Создание списка свойств ресурсов

Был выполнен переход к *третьему этапу* – созданию правил доступа.

Централизованное правило доступа — это выражение правил авторизации, которые могут включать одно или несколько условий, затрагивающих группы пользователей, требования пользователей и устройств, а также свойства ресурсов. Созданное централизованное правило доступа служит для того чтобы определить, каким пользователям и с каких устройств будет предоставлен доступ к определённым ресурсам.

Данные правила содержат особые имена и соответствующие описания. Такие правила ещё могут хранить в себе определенные условные выражения, написанные на языке SecurityDescriptorDefinitionLanguage.

Централизованные правила доступа можно объединять в централизованную политику доступа. Если для домена созданы одно или несколько централизованных правил доступа, администраторы файловых серверов имеют возможность сопоставить определенные правила с определенными ресурсами и требованиями организациями.

В отличие от списков свойств ресурсов на серверах не создается ни одного централизованного правила автоматически, по умолчанию. Поэтому для реализации требуемой политики и использования централизованных правил доступа, они были созданы в ручном режиме. Создание уникальных централизованных правил доступа было выполнено с помощью центра

администрирования Active Directory. Процесс создания выглядит следующим образом:

На контроллере домена в консоли «Центр администрирования Active Directory», где в области узлов перехода был выделен узел «Динамический контроль доступа», а затем выбрано «Central Access Rules».

На втором шаге данной процедуры из контекстного меню области сведений последовательно выбраны опции «Создать», а также «Централизованное правило доступа» данные действия продемонстрированы на рисунке 8.

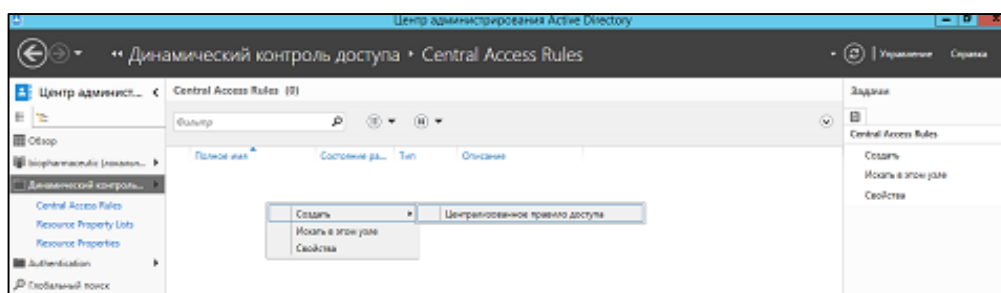


Рисунок 8 – Создание централизованного правила доступа

Далее было рассмотрено диалоговое окно, представленное на рисунке 8, в нем были определены значения требуемых управляющих элементов в трех различных группах, причем для создания нового правила достаточно заполнить только первый контроль верхней группы. Были описаны настройки, представленные на рисунке 9.

Группа «Общие». Данная группа имеет стандартный набор параметров для большинства создаваемых объектов технологии динамического контроля доступа. В данной группе возможно определение следующих трех основных параметров:

- «Имя». Для создания каждого подобного правила необходимо задать ему собственное имя. Имя должно быть уникальным, указано в буквенно-цифровом формате. Максимально допустимое число знаков для имени правила – 64 знака. В данном примере правило было названо «Finance Rule»;

- «Описание». Необязательное для заполнения текстовое поле, но наличие описания может помочь в том случае, если будут сгенерированы десятки, а то и больше централизованных правил доступа. Как и в случае с именем, количество символов в этом поле также лимитировано. Описание своего правила нужно уместить максимум в 1024 символа. В данной дипломной работе используется одно правило, поэтому описание отсутствует;
- «Защита от случайного удаления». Этот параметр представляет собой флажок для объектов центра администрирования AD, который запрещает всем удалять текущее правило. Даже создатель и администратор перед удалением должны снять данный флажок, иначе эту операцию не выполнить.

Группа «Целевые ресурсы». Служит для определения области действия ЦПД. Данная область действий формируется с помощью определения созданных ранее объектов свойств ресурсов в качестве условных выражений. Таким образом, для созданного правила была определена область применения.

Обычно централизованные правила доступа применяются исключительно к малым группам этого же дискового пространства, несмотря на это, можно оставить значение по умолчанию, и с помощью данного действия правило будет применено ко всем целевым ресурсам.

Производить группировку таких условных выражений можно при помощи стандартных операторов И либо ИЛИ. Более того, для создания более сложных сценариев можно одновременно группировать по нескольку условных выражений, объединяя области действия таких результатов. Для изменения установленной по умолчанию области действия правила, нужно нажать на кнопку «Изменить».

Группа «Разрешения». С помощью данной группы можно определить разрешения для формируемого правила благодаря двум различным функциональным возможностям:

- «Использовать следующие разрешения как предложенные». С помощью данного параметра можно производить аудит результатов запросов на доступ к нужным объектам, не влияя работу самой системы. При выборе данного параметра, можно добавлять записи разрешений из определенного списка в список предлагаемых записей разрешений для создаваемого централизованного правила доступа. Данный список сочетается с файловой системой аудита для моделирования доступа. Представленные разрешения создают определенное событие аудита, отраженное в журнале событий, таким образом можно проанализировать и зафиксировать все попытки доступа, выполняемые пользователями;
- «Использовать следующие разрешения как текущие». Благодаря данному параметру, обеспечивается доступ к целевым ресурсам после распространения централизованной политики доступа, где будет указано это правило. Текущий список разрешений включает в себя дополнительные разрешения, с которыми будет работать ОС Windows при развертывании централизованного правила доступа на файловом сервере. Эти правила не заменяют существующие параметры безопасности, поэтому ОС Windows обязательно будет оценивать записи разрешений централизованного правила доступа, текущий список разрешений NTFS, а также списки разрешений общего ресурса.

В данном случае был сделан выбор в пользу второго варианта и после нажатия на кнопку «Изменить» в диалоговом окне дополнительных параметров безопасности добавлена требуемая группа «Все пользователи домена», над которой были выполнены проверки. На рисунке 9 изображено поле, с помощью которого было указано, к каким ресурсам будет применено правило доступа. Для реализации политики описанной выше необходимо в ресурсах указать все файлы и папки, помеченные тегом «Finance».

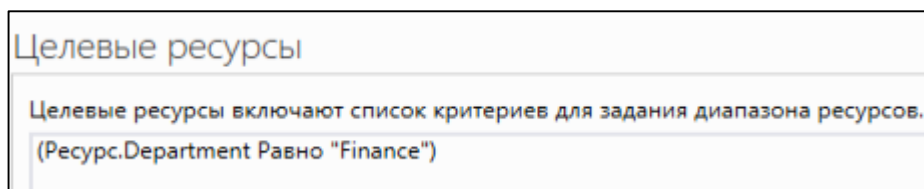


Рисунок 9 – Целевые ресурсы

Далее было указано, какие права доступа получают пользователи при подключении. Список пользователей и разрешений представлен на рисунке 10.

Элементы разрешений:

Тип	Субъект	Доступ	Условие
Разр...	ПРАВА ВЛАДЕЛЬЦА	Полный до...	
Разр...	Администраторы (РГ...	Полный до...	
Разр...	СИСТЕМА	Полный до...	
Разр...	Михаил Царегородце...	Чтение и в...	
Разр...	Пользователи домена...	Чтение, зап...	((Пользователь.Department Равно Ресурс.Department...

Рисунок 10 – Элементы разрешений

Таким образом, полный доступ к ресурсам помеченным тегом «Finance» получают:

- создатель ресурса;
- администраторы;
- система.

Руководитель организации, Михаил Царегородцев, обладает правами чтения и выполнения.

В последнем правиле было указано, что пользователь получает права доступа на чтение, выполнение и запись, если выполняются следующие условия:

- пользователь, у которого значение атрибута Sity совпадает со значением тега Sity в ресурсах;
- пользователь, у которого значение атрибута Departament совпадает со значением тега Departament в ресурсах.

Только при одновременном выполнении этих условий происходит доступ пользователя к ресурсам, помеченным тегом «Finance». Настройка данного правила представлена на рисунке 11.

Субъект: Пользователи домена (PGU\Пользователи домена) Выберите субъект

Тип: Разрешить

Общие разрешения:

- ☐ Полный доступ
- ☐ Изменение
- ☒ Чтение и выполнение
- ☒ Чтение
- ☒ Запись
- ☐ Особые разрешения

Добавьте условие, чтобы ограничить доступ. Субъекту указанные разрешения будут предоставлены только при соблюдении условий.

Управление группировкой

Пользовател	Department	Равно	Ресурс	Departm
И				
Пользовател	Sity	Равно	Ресурс	Sity

Рисунок 11 – Настройка правила доступа

Часто бывают такие ситуации, когда после создания нового объекта возникает необходимость в его изменении. Например, при создании была допущена ошибка, либо не было добавлено требуемое разрешение. Вариантов может быть много. Централизованные правила доступа модифицируются и для изменения существующего объекта не требуется никаких сверхъестественных действий. Нужно сделать переход к тому же узлу, в котором было создано само правило, найти такое правило в списке области сведений, а затем из контекстного меню такого объекта выбрать опцию «Свойства».

В отобразившемся диалоговом окне изменения созданного правила, предоставляются практически те же возможности, что и при создании такого правила, за исключением трех моментов:

- невозможно изменять наименование своего правила;
- кроме редактирования текущих разрешений, также предоставлена возможность настроить предложенные разрешения. Список разрешений включает в себя записи, определяющие доступ к ресурсам для ЦПД. Эти разрешения вступают в силу после того, как развернуто централизованное правило доступа с помощью

централизованной политики доступа. Такие разрешения обнаруживаются только если посмотреть параметры или исправить действующее правило доступа. В списке предоставленных разрешений можно увидеть все изменения в разрешениях, между действующими участниками безопасности со списком существующих разрешений. Этот список разрешений не влияет на работающие разрешения пользователей. Чтобы была возможность просмотреть и проанализировать промежуточные разрешения, нужно поставить флажок «Включить поэтапную настройку разрешений». При работе с существующими разрешениями уделялось особое внимание на следующие возможности. Кнопка «Изменить». Этот параметр позволяет вызвать список дополнительных параметров безопасности, а также позволяет изменять или добавлять разрешения в группу существующих разрешений. Параметр «Применить предложенные». С помощью настройки данного параметра можно заменить существующие разрешения такими разрешениями, которые были определены в группе существующих разрешений. Параметр «Копировать из текущих». С помощью данного параметра можно выполнить обратное действие, таким образом это действие, заменяет разрешения в списке существующих разрешений разрешениями из действующего списка разрешений;

- возможности группы «Предыдущие разрешения» станут доступны (при просмотре свойств ЦПД) если были модифицированы установленные при первой настройке разрешения. При изменении разрешений ЦПД ОС сохраняет изначальные действующие разрешения в список группы «Предыдущие разрешения», а потом копирует новый список работающих разрешений и список предыдущих разрешений. Необходимо отметить что данный список содержит только одну копию записей предыдущих

разрешений. Таким образом, функциональные возможности центра администрирования AD не хранят полной истории всех сделанных изменений в разрешениях действующего списка разрешений.

Чтобы удалить существующие правила доступа, необходимо выполнить следующие действия. В узле Central Access Rules центра администрирования Active Directory необходимо выделить ненужное более правило доступа, а затем из контекстного меню выбрать команду «Удалить».

В появившемся диалоговом окне нужно сделать клик по кнопке «Да», правило будет моментально удалено. Если будет показано сообщение, в котором указано о нехватке прав, следует открыть окно со свойствами удаляемого правила, далее убрать флаг с опции «Защита от случайного удаления». После этого вновь попробовать провести удаление правила, оно должно быть успешно удалено.

Четвёртым этапом является создание централизованной политики доступа.

Централизованные политики доступа — политики авторизации, включающие условные выражения. Данные политики были внедрены в ОС Windows Server 2012 и представляют собой совокупность объектов ЦПД. Создание таких политик осуществляется с помощью центра администрирования AD. Распространение таких политик происходит средствами функциональных возможностей групповой политики. Данные политики можно применять как на отдельных файловых серверах, так и на всех сразу, настройка осуществляется с помощью групповых политик. Централизованные политики доступа могут состоять из одного или нескольких ЦПД. Стоит отметить что ЦПД могут в составе нескольких разных централизованных политик доступа.

Централизованные политики доступа призваны повысить безопасность и улучшить контроль доступа к ресурсам, расположенных на файловых серверах организации. Стоит отметить, что данные политики не замещают

существующие до этого локальные политики доступа, списки контроля доступа и другие средства контроля доступа которые действуют в организации.

Например, в централизованной политике доступа явно указано, какой пользователь может использовать определенный файл, размещенный по конкретному адресу, однако, в избирательной таблице управления доступом доступ пользователя к файлу запрещен. Другими словами, будет ограничен доступ пользователя к данному ресурсу. С подобными проблемами можно столкнуться потому что правила запрета всегда имеют высший приоритет над разрешающими правилами. Таким образом, чтобы избежать данных ситуаций, требуется планировать, настраивать и проверять все действующие средства контроля доступа.

Перед внедрением, централизованных политик доступа должны быть соблюдены следующие предварительные требования:

- необходимо создать такие утверждения, которые будут подключены к объектам учетных записей пользователей или компьютеров с помощью определенных атрибутов;
- требуется создание определения свойств файла;
- нужно сформировать одно или несколько ЦПД, в зависимости от стратегии организации;
- создать и определить параметры централизованной политики доступа;
- развернуть созданные политики на нужные файловые серверы с помощью возможностей групповой политики. После выполнения данных операций, файловые сервера под управлением ОС Windows Server 2012/2012 R2 узнают о существовании DAC и о том, что в организации существуют централизованные политики доступа;
- на файловых серверах нужно включить данные политики на ресурсы, требующие контроля.

Далее было рассмотрено, как создаются, добавляются, изменяются или удаляются к такому объекту ЦПД. Было рассмотрена возможность удаления объектов централизованных политик доступа, с помощью консоли центра администрирования AD.

Все действия, связанные с централизованными политиками доступа схожи с ЦПД. Ниже приведен пример, в котором продемонстрировано конфигурирование центральной политики доступа, основанное на созданном в данной работе правиле доступа «Finance Rule». Для создания данной политики, были выполнены действия, описанные ниже.

В окне центра администрирования AD выполнен переход к узлу «Динамический контроль доступа» далее к «Central Access Policies». Затем на панели задач была выбрана опция «Создать» и «Централизованная политика доступа», как показано на рисунке 12.

С помощью вышеперечисленных действий был выполнен первый шаг к созданию и настройке централизованной политики доступа.

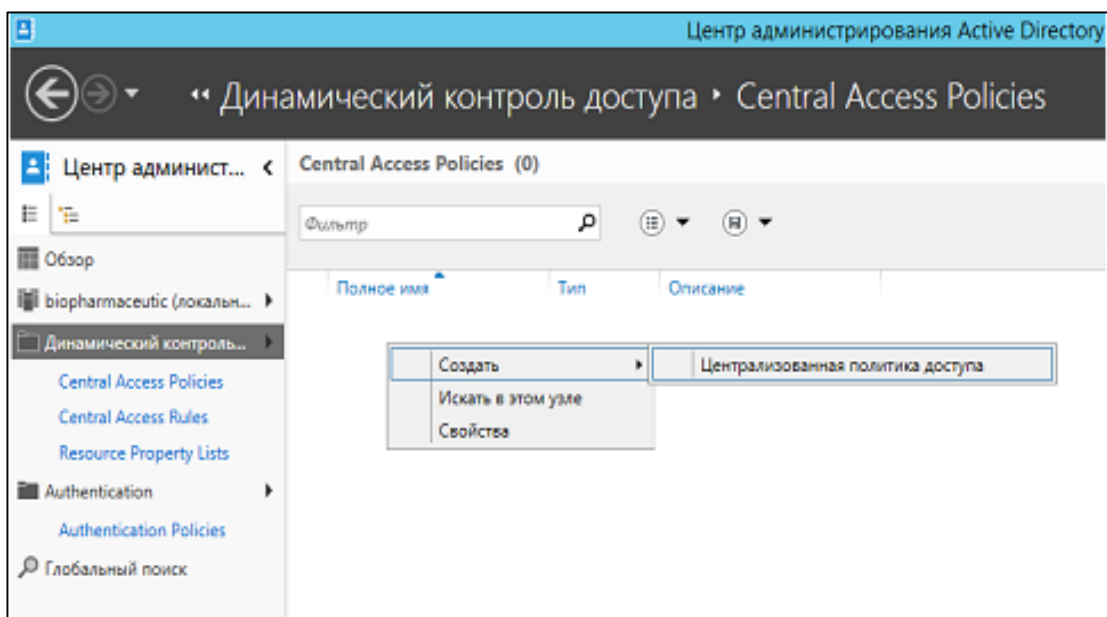


Рисунок 12 – Создание централизованной политики доступа

Затем, открыв консоль «Создать Централизованная политика доступа» были выбраны все необходимые параметры для будущей централизованной политики доступа. В отличие от изменения или создания ЦПД, при

формировании политик предоставлялась возможность изменения параметров только двух групп.

Группа «Общие». Это общие параметры, позволяющие должным образом охарактеризовать политику.

Здесь определяются три параметра:

- «Имя». В данном поле указывается имя для создаваемой политики. В данной дипломной работе правило носит название «Central Politican»;
- «Описание». В данном поле, если требуется, можно указать описание политики DAC. Так как в дипломной работе использовалась только одна централизованная политика доступа и единственное правило нельзя перепутать, данное поле оставлено пустым;
- «Защита от случайного удаления». Если данный флаг установлен, то перед удалением, необходимо зайти в параметры политики и его снять, иначе политику нельзя будет удалить, даже создателю и администратору. В данном случае флажок установлен.

Группа «Участник». В этой группе создаваемой централизованной политики доступа были указаны ЦПД. Они и стали структурой данной политики. После нажатия кнопки «Добавить» было отображена консоль, с помощью которой можно добавлять ЦПД. Происходит это путем выбора правила из соответствующего списка с левой стороны (см. рисунок 13).

В данной работе было выбрано созданное ранее централизованное правило доступа «Finance Rule». Далее был сделан клик по верхней кнопке «>>».

В результате данное правило отобразилось в диалоговом окне справа и стало в списке добавленных.

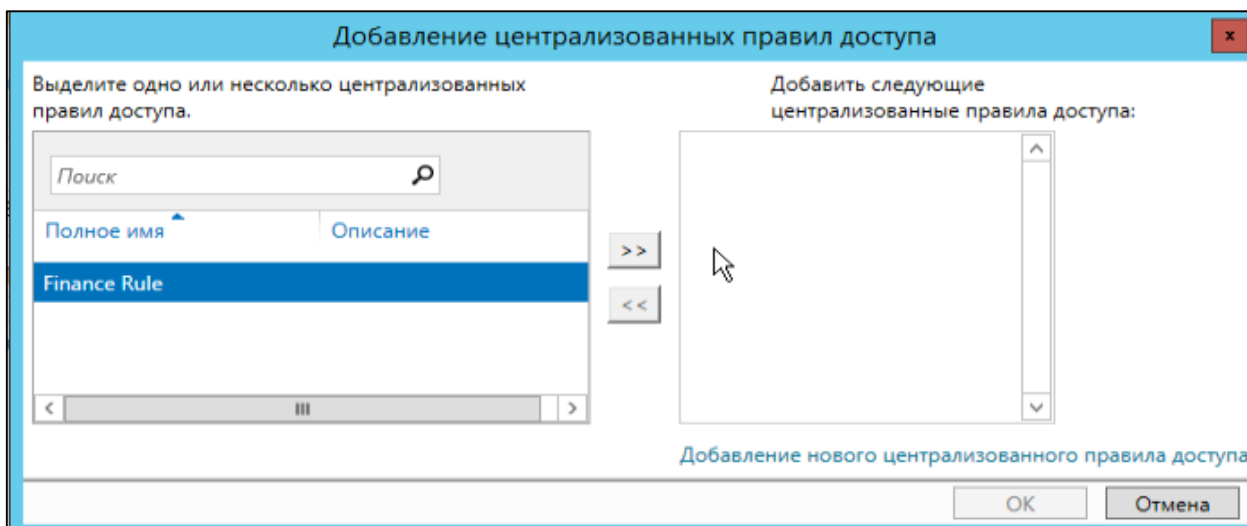


Рисунок 13 – Добавление централизованных правил доступа

Для изменения существующей политики доступа, нужно в центре администрирования AD сделать переход к DAC и выбрать «Централизованная политика доступа», далее сделать клик по требуемой политике доступа и из контекстного меню сделать клик по команде «Свойства».

Для добавления нового правила к действующей централизованной политике доступа, из контекстного меню необходимо выбрать команду «Добавить централизованные правила доступа».

Затем выбрав этот параметр было отображено диалоговое окно добавления ЦПД, ранее упомянутом выше.

Для удаления централизованной политики доступа нужно в узле Central Access Policies выбрать требуемый объект, а затем выполнить команду «Удалить» из контекстного меню.

Далее был выполнен переход к *пятому этапу* – «Распространение политики на файловом сервере». Опубликовать настроенную политику для того чтобы она стала доступной на файловых серверах. Для этого в управлении групповой политикой была открыта политика контроллера домена по умолчанию. В ней был найдена категория «Файловая система», содержащая директорию «Централизованная политика доступа», которая находится по адресу Конфигурация компьютера\Политики\Конфигурация

Windows\Параметры безопасности\Файловая система. Данные директории продемонстрированы на рисунке 14.

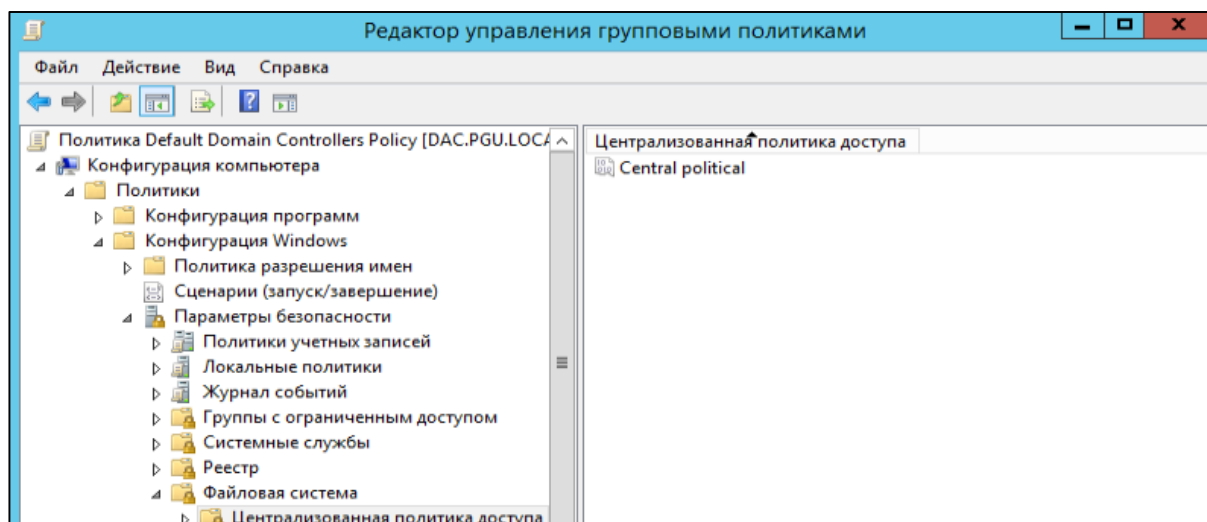


Рисунок 14 – Централизованная политика доступа

Открыв конфигурацию централизованных политик доступа, была добавлена созданная ранее политика доступа «Central political». Данные действия представлены на рисунке 15.

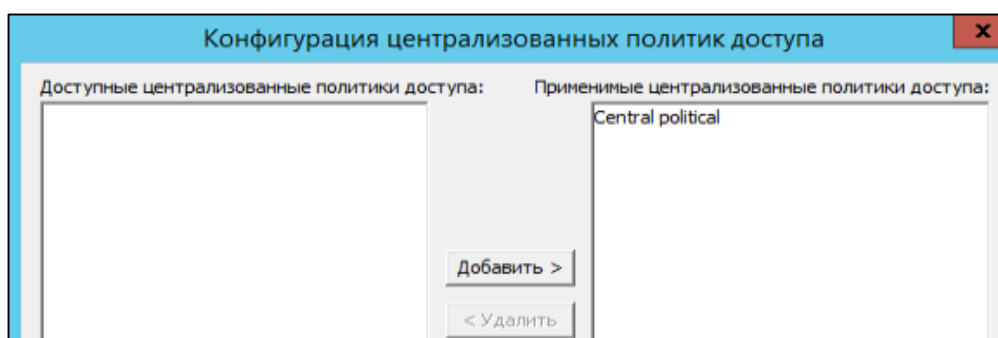


Рисунок 15 – Добавление новой политики доступа

В результате выполненных действий файловый сервер сможет применять созданную ранее политику доступа.

Этап шестой – классификация ресурсов.

Были выделены следующие способы, при помощи которых проведена классификация. К ним можно отнести:

- классификация в ручном режиме. Этот способ является самым простым. При его использовании была предоставлена возможность классифицировать ресурсы организации вручную, с помощью вкладки «Классификация»;

- классификация на основе расположения. Данный метод классификации файлов используется, как для классификации файлов вручную благодаря специальной вкладке диалогового окна свойств нужного файла, так и при использовании классификатора папок в создаваемом правиле классификации;
- классификация на основе содержимого. Данный метод является наиболее распространенным, так как позволяет классифицировать текстовые документы при отображении в них определенной информации. Например, если документ содержит слово «Секретно», то ему автоматически может быть присвоен статус секретного документа и данный файл будет доступен только определенной группе пользователей.

Далее был рассмотрен пошаговый процесс классификации файлов вручную.

В первую очередь была открыта оснастка «Управление групповой политикой» и сформирован для нужного подразделения объект групповой политики, определяющий два параметра, которые имеют непосредственное отношение к классификации ресурсов в ручном режиме. В данной работе этим объектом стал объект групповой политики «File Classification», который был связан со всем доменом.

Процесс создания представлен на рисунке 16. После создания объекта групповой политики он был выделен и открыт в редакторе управления.

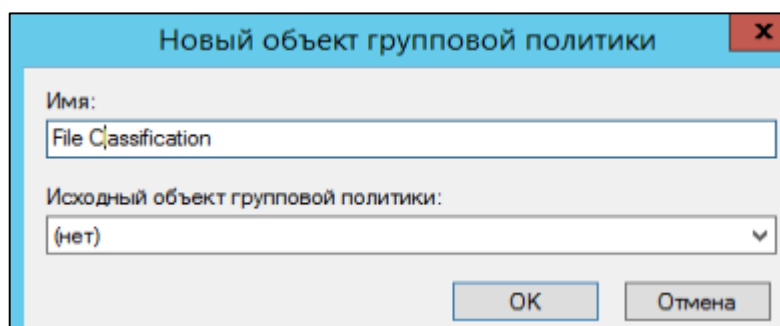


Рисунок 16 – Создание нового объекта групповой политики

В появившемся окне был сделан переход к узлу «Конфигурация компьютера\Политики\Административные Шаблоны\Система\Инфраструктура классификации файлов» в данном окне были отображены два параметра, они и были настроены как описано далее.

«Инфраструктура классификации файлов. Отображение вкладки «Классификация» в проводнике». Данное свойство позволило включить для конечных компьютеров возможность обязательного отображения вкладки «Классификация» в диалоговом окне свойств выбранных файлов. У этого свойства отсутствуют опции, поэтому для его настройки нужно поставить состояние с «Не задана» на «Включено». Настроенный параметр политики продемонстрирован на рисунке 17.

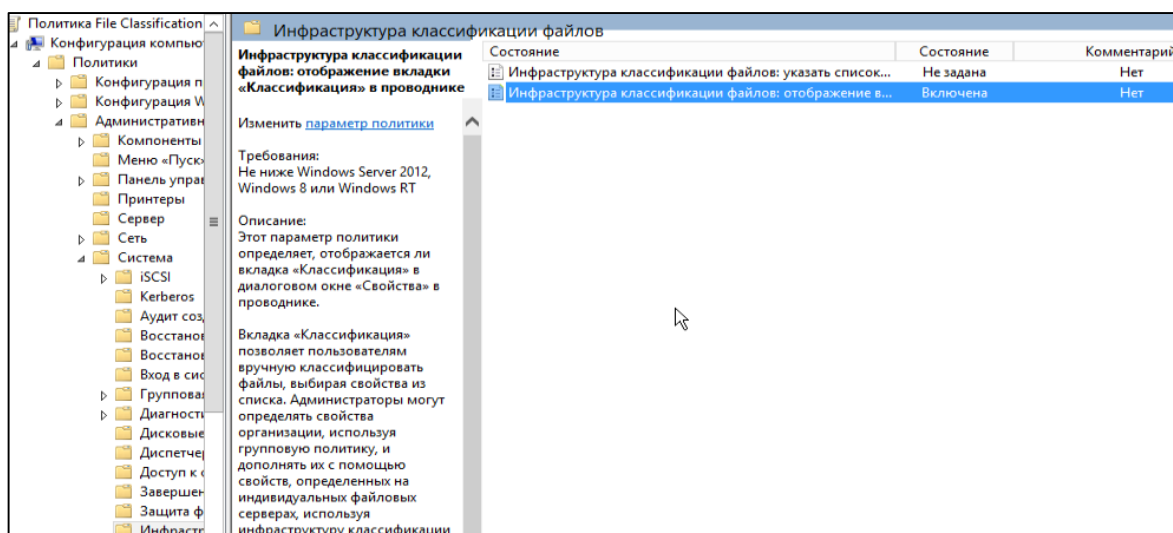


Рисунок 17 – Инфраструктура классификации файлов

«Инфраструктура классификации файлов: Указать список свойств классификации». С помощью данного параметра групповой политики можно определить конкретный список свойств ресурсов, который применяется для выбранного ранее подразделения с определенными компьютерами. Включив данный параметр, в соответствующем текстовом поле было указано наименование интересующего списка свойств ресурсов. Например, как видно на рисунке 18, в этом примере указывается Resource Properties List 1, сконфигурированный ранее.

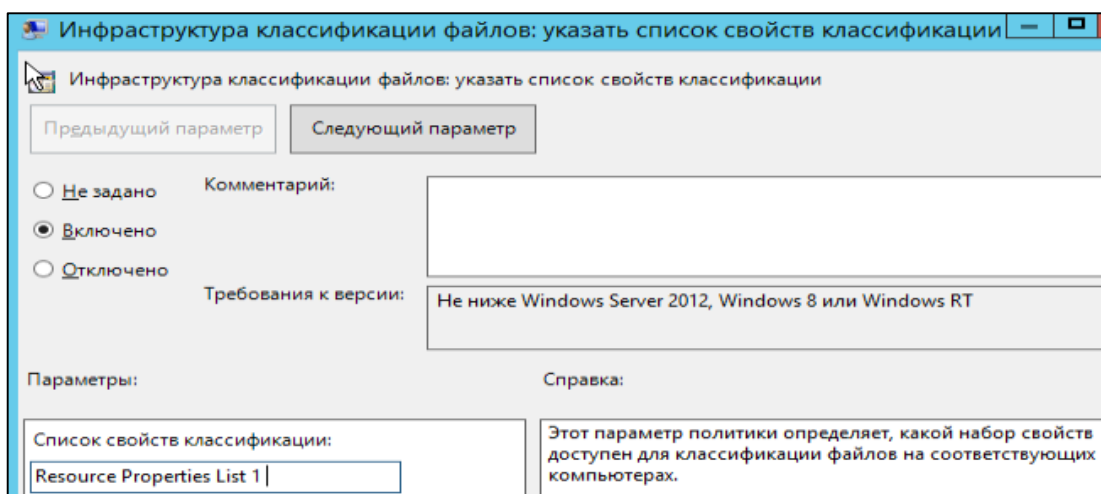


Рисунок 18 – Определение списка свойств классификации файлов

После настройки данных параметров на нужных компьютерах была обновлена групповая политика с помощью команды «Обновление групповой политики».

Был выполнен переход на целевом компьютере к проводнику Windows и выбран файл, для проверки классификации. После этого сделан вызов для файла контекстного меню и открыто диалоговое окно свойств файла. Далее выполнен переход на вкладку «Классификация» и здесь, стали доступны те же свойства ресурсов, которые были настроены для созданного ранее объекта Resource Properties List 1. Например, можно настроить значение для свойства Sity или Department, как показано на рисунке 19.

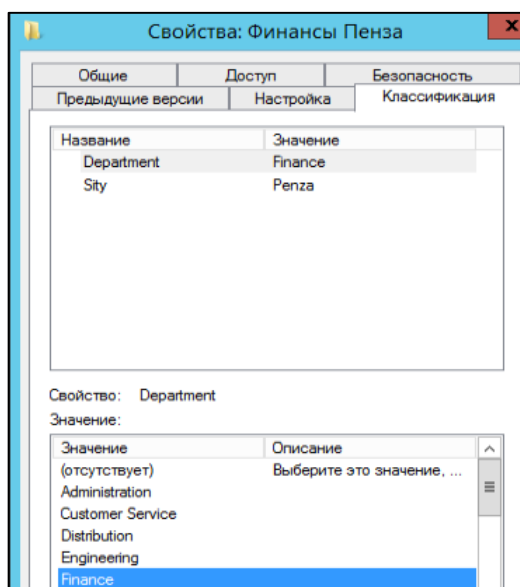


Рисунок 19 – Классификация ручным способом

Процесс классификации файлов на основе содержимого.

Необходимо отметить, что для работы данного метода был предварительно установлен диспетчер файлового сервера.

В диспетчере ресурсов файлового сервера для управления классификацией можно выделить два основных понятия, а именно: свойства классификации, а также правила классификации.

Свойства классификации используются для определения значений файлам в указанной директории. В зависимости от деятельности можно выбрать подходящий тип свойства. Данные свойства классификации — это свойства ресурсов, которые были созданы в узле Resource Properties консоли центра администрирования AD и были добавлены в списки свойств ресурсов.

Таким образом, можно сделать вывод что существует множество типов свойств, доступных для выбора. Также, с помощью диалогового окна можно формировать свои локальные типы свойств, в зависимости от стратегии организации.

Были выделены следующие типы свойств классификации:

- дата-время;
- числовой;
- строка;
- да или нет;
- упорядоченный список;
- множественный выбор;
- несколько строк.

Как видно на рисунке 20, в узле «Свойств классификации» диспетчера ресурсов файлового сервера были сразу обнаружены все те свойства ресурсов, использованные ранее. Например, созданное ранее свойство Sity. Правила классификации назначают свойства классификации для файлов. Каждое правило классификации, которое было создано, включало в себя конкретную информацию, которая определяла то, какие файлы будут применены к данному правилу и какое будет назначено для них свойство классификации.

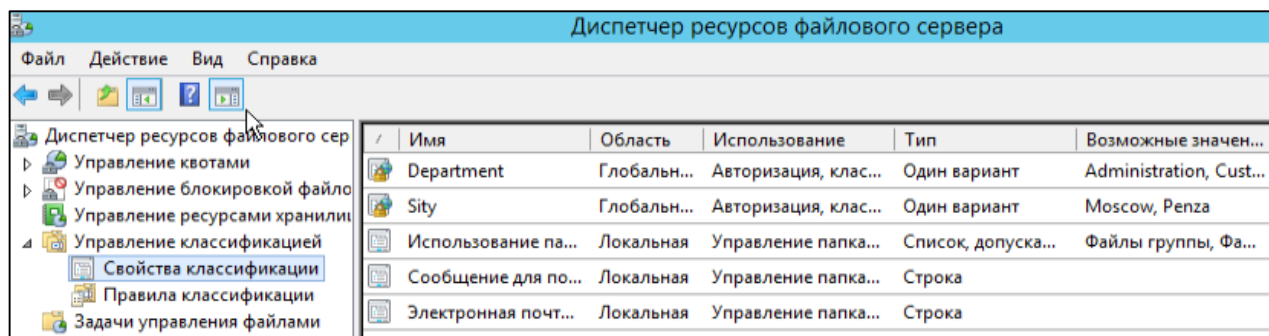


Рисунок 20 – Свойства классификации

В каждое правило включены уникальные свойства классификации и определены значения для таких свойств. Правила классификации запускаются двумя способами: по расписанию или по запросу. Благодаря настройке расписания классификации возможно установление промежутка времени, в который будут выполняться правила классификации файлов, сохраняя файлы сервера регулярно классифицированными. С помощью этого администратор всегда осведомлен о классификационных файлах и их количестве.

Для создания первого правила классификации, были выполнены действия, описанные ниже.

В консоли диспетчера файлового сервера выполнен переход к узлу «Правила классификации», в области сведений было вызвано контекстное меню, а затем выбрана опция «Создать правило классификации» как показано на рисунке 21:

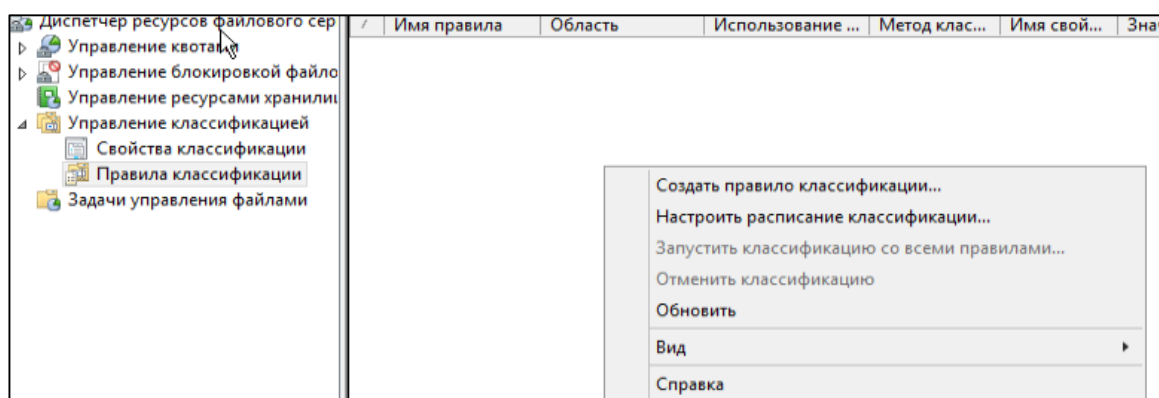


Рисунок 21 – Создание правила классификации

Далее была отображена консоль «Создать правило классификации» в которой было обнаружено четыре вкладки, при помощи которых происходит создание правила.

Была рассмотрена по порядку каждая вкладка.

Вкладка «Общие». На этой вкладке можно указать некоторые общие параметры, которые будут лишь характеризовать это правило. Из таких параметров можно выделить:

- «Имя правила». Это текстовое поле отвечает за будущее имя правила. Соответственно, в этой работе в данном текстовом поле было указано «First rule»;
- «Включено». Создаваемое правило будет применяться только в том случае, если установлен соответствующий флажок;
- «Описание». В том случае, если будет создано много правил, описание будет полезным. Так как у нас было применено только одно правило, данное поле осталось пустым.

Данная вкладка изображена на рисунке 22.

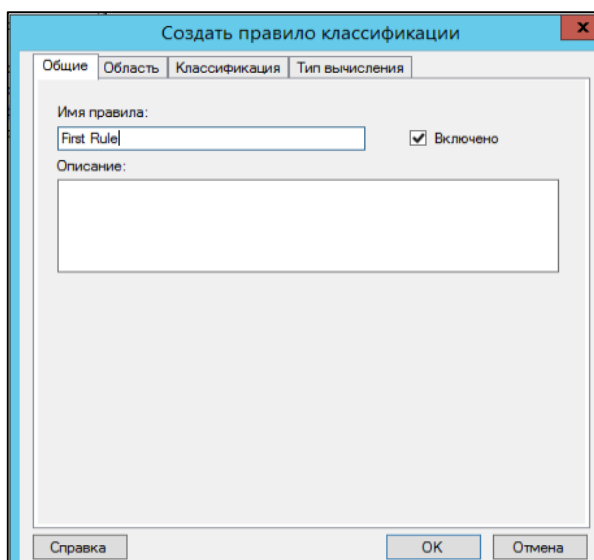


Рисунок 22 – Вкладка «Общие»

Вкладка «Область». На этой вкладке можно определить расположение, для которого будет применяться созданное ранее ЦПД. На данной вкладке имеется возможность, удаления и добавления нескольких выбранных

расположений при помощи кнопок «Удалить» и «Добавить». В данной работе правило классификации применялось ко всем директориям из списка и применялась наследование к вложенным папкам и файлам. Дополнительно имеется возможность сделать переход по ссылке «Задать свойства управления папками», с целью указания дополнительных значений для нужных папок. В качестве свойств может быть указано назначение папки, содержимое. Также есть возможность выводить настраиваемое сообщение сотруднику при получении ошибки отказа в доступе, позволяющее отображать для конечного пользователя настраиваемое сообщение. В данном сообщении может содержаться электронный адрес владельца папки, что позволяет напрямую к нему обратиться и быстрее решить возникшую проблему.

Чтобы понять нужно ли включать данную папку в правила классификации нужно чтобы само создаваемое правило классификации использовало значение свойства управления папками, предназначенное для данной папки. Например, как видно на рисунке 23, было добавлено для папки C:\Shares\Share_PGU свойство использования папки со значением файлов группы и файлов пользователя.

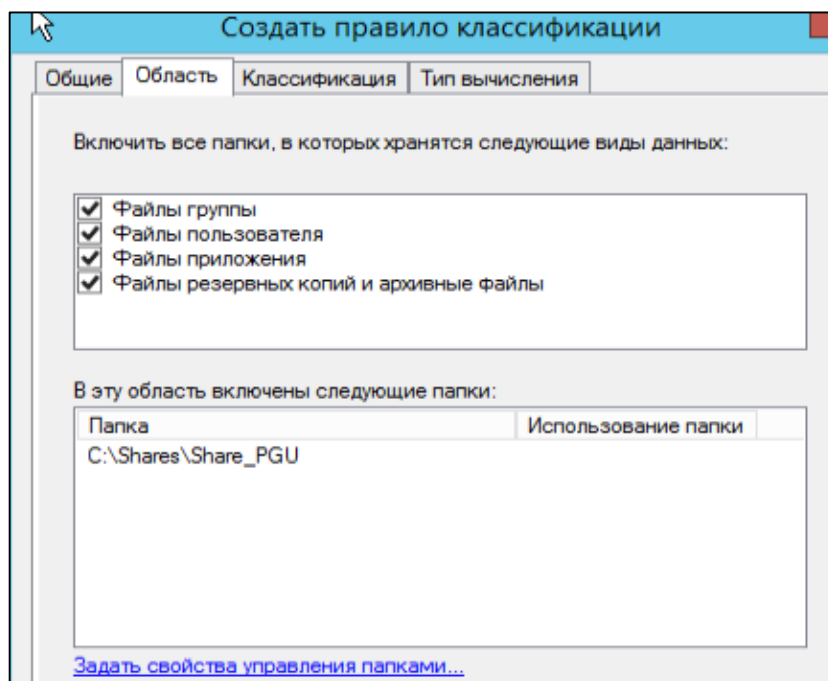


Рисунок 23 – Область классификации

Вкладка «Классификация». Данная вкладка предназначена именно для определения непосредственно самой классификации файлов. Она включает в себя ниже описанные параметры.

Группа механизм классификации с параметром «Выберите метод назначения свойства файлам». Механизмы классификации включают в себя наборы модулей, которые входят в состав ОС Windows Server 2012/2012 R2. На данной вкладке есть возможность выбрать:

- классификатор Windows PowerShell. С помощью данного метода можно реализовать классификацию файлов в автоматическом режиме методом выполнения специального скрипта Windows PowerShell, определяющего классификацию файлов. При использовании данного метода было обращено внимание на то, что классификатор Windows PowerShell упрощает применение алгоритма настраиваемой классификации. Таким образом, появляется возможность фильтровать файлы в зависимости от сотрудника, который последним работал с файлом;
- классификатор папки. Данное правило использует специальный классификатор папок, назначающий указанное значение свойства классификации для всех ресурсов в области действия создаваемого правила. Все данные в папке, указанной на вкладке область, будут помечены, например, файлы со значением Penza для созданного нами ранее свойства Sity;
- классификатор содержимого. Является заключительным методом классификации и производит поиск текста или используются специальные шаблоны, с помощью которых можно использовать определенный механизм в качестве индексатора поиска. Если описанный выше механизм находит искомое выражение, то файлу присваивается указанное значение. Для использования данного метода необходимо произвести переход в соответствующее диалоговое окно, сделав клик по кнопке «Настроить»;

- группа «Свойство» и параметр «Выберите назначаемое свойство». При помощи данного списка существует возможность выбрать свойство, которое присваивается создаваемым правилом. В данной работе было выбрано созданное ранее свойство ресурса «Sity»;
- параметр «Укажите значение». Если механизм классификации требует установки для файлов определенного значения, можно выбрать значение свойства, которое будет присвоено этим правилом. В данном случае было выбрано значение «Penza».

Кнопка «Настроить» и диалоговое окно «Параметры классификации». В открывшейся консоли классификатор содержимого использует параметры классификации. Они предназначены для определения шаблона искомого содержимого документа. Существует возможность определить следующие параметры, перечисленные ниже:

- регулярное выражение. Данный параметр описывает одну или несколько строк, с помощью которых происходит сопоставление при поиске в тексте. Совпадение регулярного выражения выполняется с помощью синтаксиса .NET. Регулярное выражение имеет в своей структуре обычное и специальные знаки которые известны как метасимволы. Например, «\d\d» соответствует любому двухзначному числу;
- строка с учетом регистра. Данный параметр следит за совпадением строк с учетом регистра. Например, была указана искомая фраза ПеНзА, тогда будут соответствовать только значения с идентичным регистром и количеством;
- строка. Данный параметр отвечает за совпадение строки, независимо от регистра. В данной работе используется данный метод с искомой фразой 58_rus.

Минимальное и максимальное число вхождений. Данные параметры отвечают за количество элементов, срабатывающих во время регистрации совпадения. В данной работе это число имеет значение один.

В данном примере вкладка классификации с диалоговым окном параметров классификации будет выглядеть так, как показано на рисунке 24:

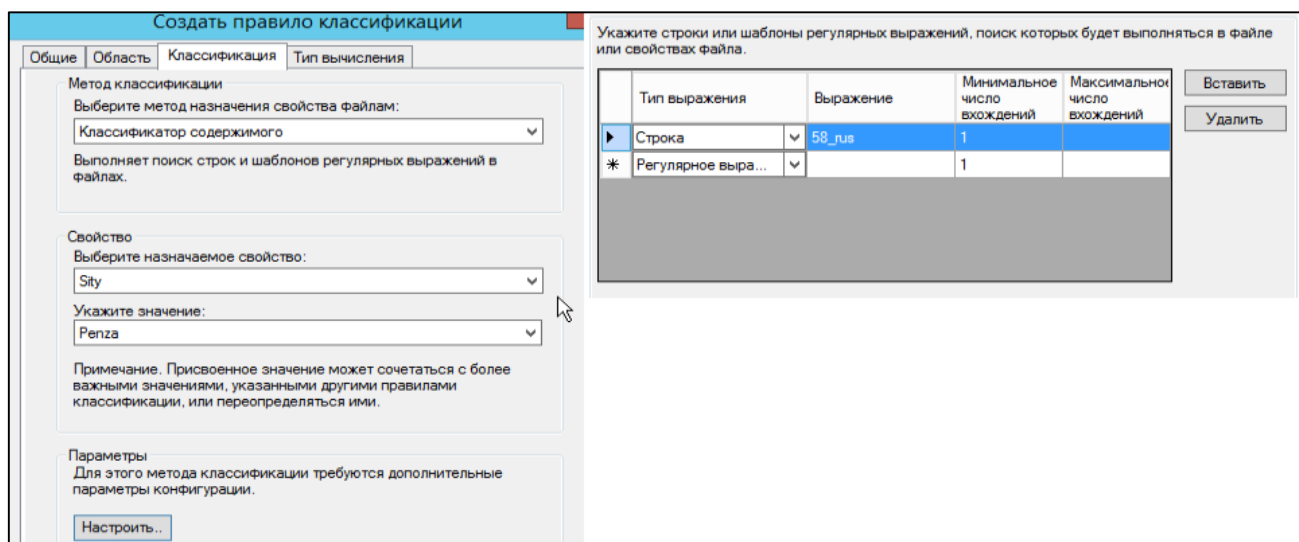


Рисунок 24 – Правило классификации

Вкладка «Тип вычисления». На данной вкладке был обнаружен флажок «Заново определить существующие значения свойств», который по умолчанию не установлен. Данное правило применяется к не классифицируемым файлам по свойству, которое устанавливается этим правилом. Таким образом, изначальные значения свойств, которые были определены ранее, не классифицируются повторно. Если нужно изменить такое поведение, то настраиваются следующие параметры:

- перезаписать существующее значение. Если сделать остановку на данном параметре, тогда правило будет применено ко всем документам. В случае если документ или механизм классификации будет обновлен тогда действующие значения и значения, заданные по умолчанию для свойства, определенного правилом, будут игнорироваться. Таким образом, файл имеющий логическое свойство, с установленным значением «Да», правило, использующее классификатор папок для установки

значения «Нет» для всех файлов, изменяет значение свойства на «Нет». Кроме того, были обнаружены два флага – «Очистить классифицированное пользователем свойство» и «Очистить автоматически классифицированное свойство», с помощью которых можно очистить определенное значение свойства если это свойство больше не применяется к файлам;

- агрегировать значения. Это правило применяется в том случае, если файл или механизм классификации были обновлены. Тогда при каждом запуске классификации в автоматическом режиме, измененные файлы будут вновь подвергаться фильтрации. Стоит отметить, если правило определяет значение классификации для файла, это значение объединяется с уже имеющимся в файле значением. В данной работе были установлены параметры, изображенные на рисунке 25.

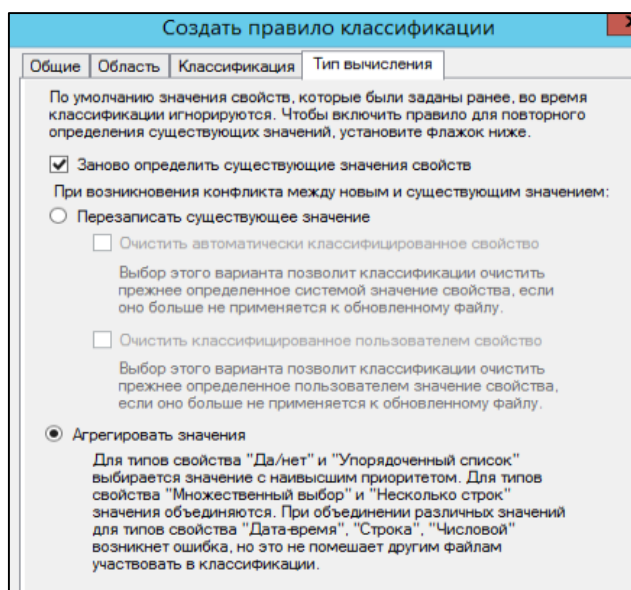


Рисунок 25 – Тип вычисления

Далее было выбрано созданное ранее правило классификации и в области «Действия» консоли FSRM выбрана опция «Запустить классификацию со всеми правилами». После данных действий отобразилось диалоговое окно «Запуск классификации», где в качестве теста была выбрана опция «Дождаться завершения классификации» после чего нужно была нажата кнопка ОК, как показано на рисунке 26.

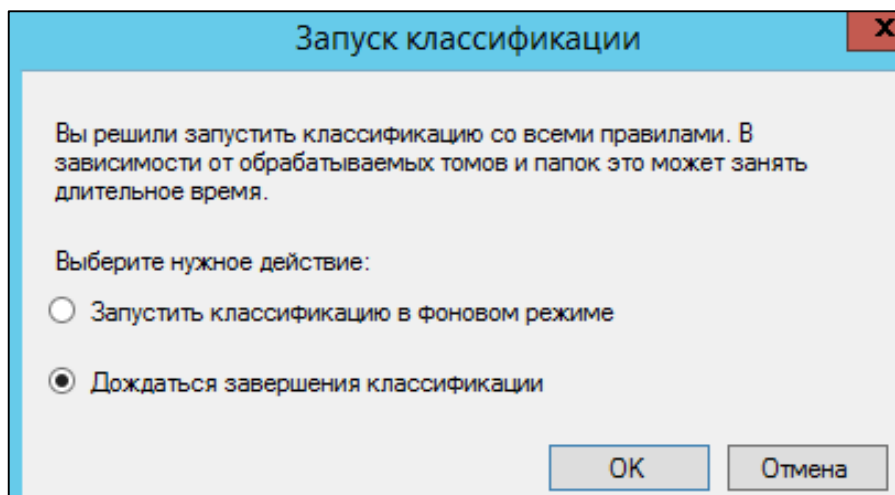


Рисунок 26 – Запуск классификации

В браузере открылся отчет классификации, где были показаны все операции, которые выполнялись с файлами. Так как заранее было создано два файла с требуемым текстом, в отчете, представленном на рисунке 27, показано, что были проклассифицированы только 2 файла.

Итоги отчета					
Файлы, показанные в отчете			Все файлы, отвечающие условиям отчета		
Свойства	Файлы	Общий размер на диске	Свойства	Файлы	Общий размер на диске
1	2	0,00 MB	1	2	0,00 MB

Рисунок 27 – Отчет об автоматической классификации

Далее был выполнен переход к последнему этапу настройки динамического контроля доступа – применения политики доступа к файлам и папкам.

Так как общий ресурс находится по адресу C:\Shares далее описаны действия по применению политики именно для этой директории.

Первым действием были открыты свойства папки, выполнен переход на вкладку «Безопасность» и сделан клик по кнопке «Дополнительно». Появилась новая вкладка «Централизованная политика» что является доказательством что предыдущие этапы настройки выполнены успешно.

В данной вкладке была выбрана созданная ранее политика доступа, указана область применения как показано на рисунке 28.

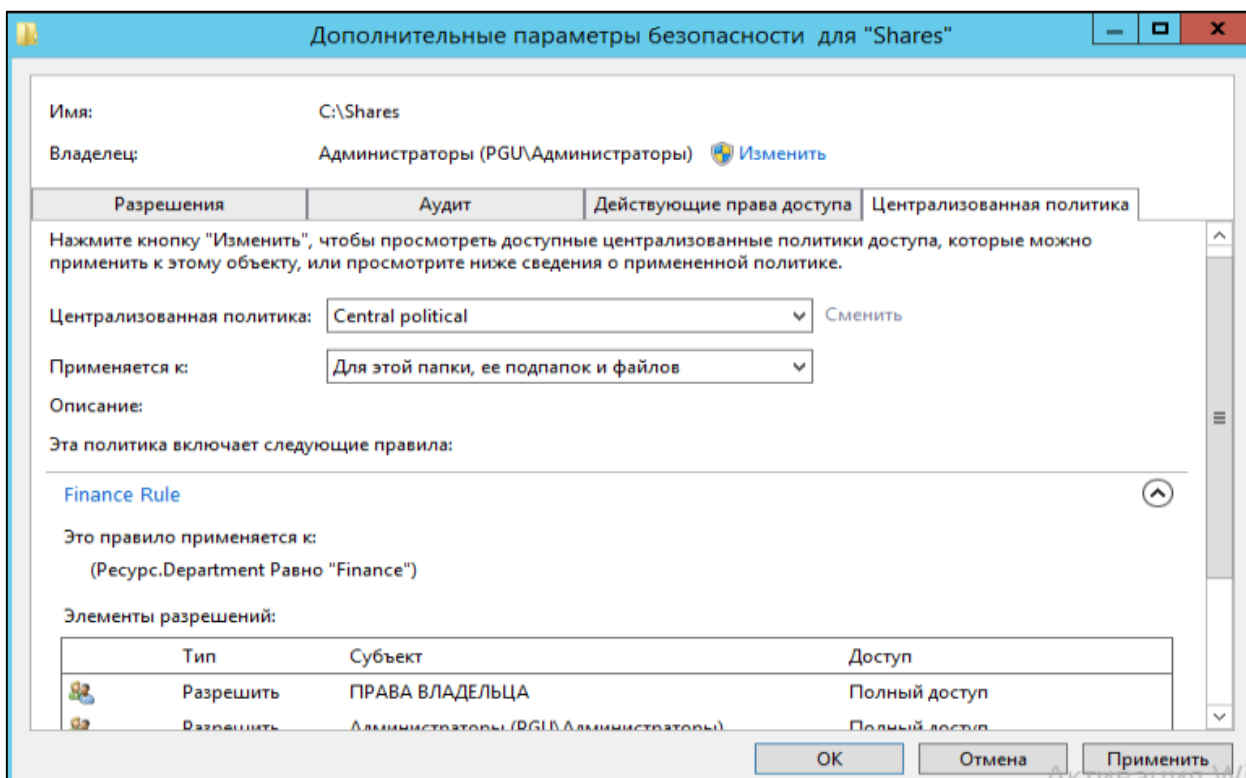


Рисунок 28 – Централизованная политика

После данных действий была проведена проверка. Стоит напомнить, что в данной работе с помощью динамического контроля доступа была организована следующая политика доступа:

- доступ на чтение финансовой информации должны иметь только сотрудники финансового департамента с привязкой к офису сотрудника;
- руководители финансового департамента должны иметь права на чтение и изменение любой финансовой информации;
- руководители организации имеют право на чтение всей финансовой информации.

Другими словами, на файловом сервере к документам, которые относятся к финансовому отделу доступ на чтение должен иметь тот человек из финансового отдела, который работает в этом же городе.

При проверке принимали участие следующие пользователи:

- Иванов Иван, сотрудник финансового отдела из г. Пенза;
- Сидоров Алексей, сотрудник финансового отдела из г. Москва;
- Афанасьев Андрей, руководитель финансового отдела;
- Орлов Николай, сотрудник операционного отдела из г.Москва;
- Царегородцев Михаил, руководитель организации.

На рисунке 29 показано, как при помощи консоли AD – пользователи и компьютеры, Иванову Ивану был присвоен город Пенза и установлен финансовый отдел.

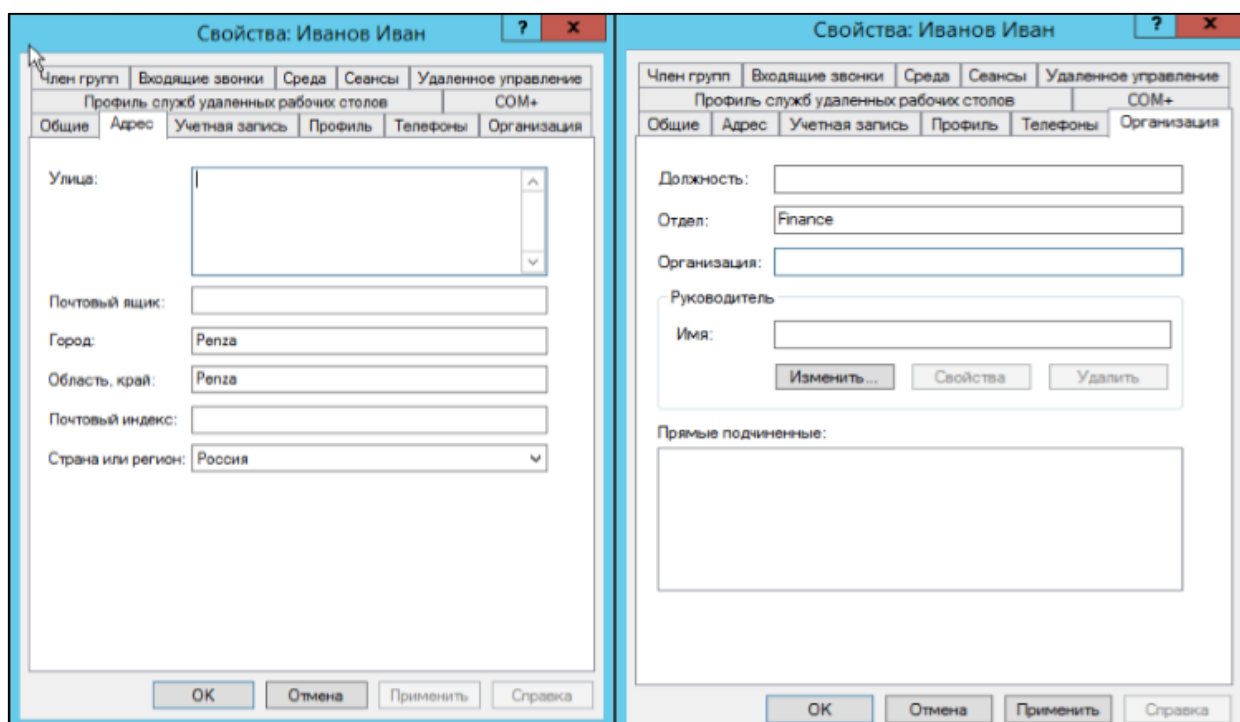


Рисунок 29 – Свойства работника финансового отдела, г. Пенза

Аналогичным образом осуществлялась настройка всех сотрудников в соответствии с требованиями политики доступа.

Далее был осуществлен вход под различными учетными записями, попытки доступа к ресурсам с разными классификационными признаками. В

итоге был сделан вывод, что система полностью соответствует требованиям политики.

Убедиться в правильности настройки можно с помощью рисунка 30, на котором выполнен вход за Иванова Ивана, сотрудника финансового отдела города Пензы, на котором доступ к финансовой информации города Пензы разрешен, но при попытке просмотра финансовой информации для города Москвы, было получено соответствующее сообщение об ограничении доступа. Как показано на вкладке классификация, настройки папки «Финансы_Пенза» видны, а при попытке просмотреть вкладку классификация папки «Финансы_Москва» была получено предупреждение о том, что для этой операции не хватает определенных прав.

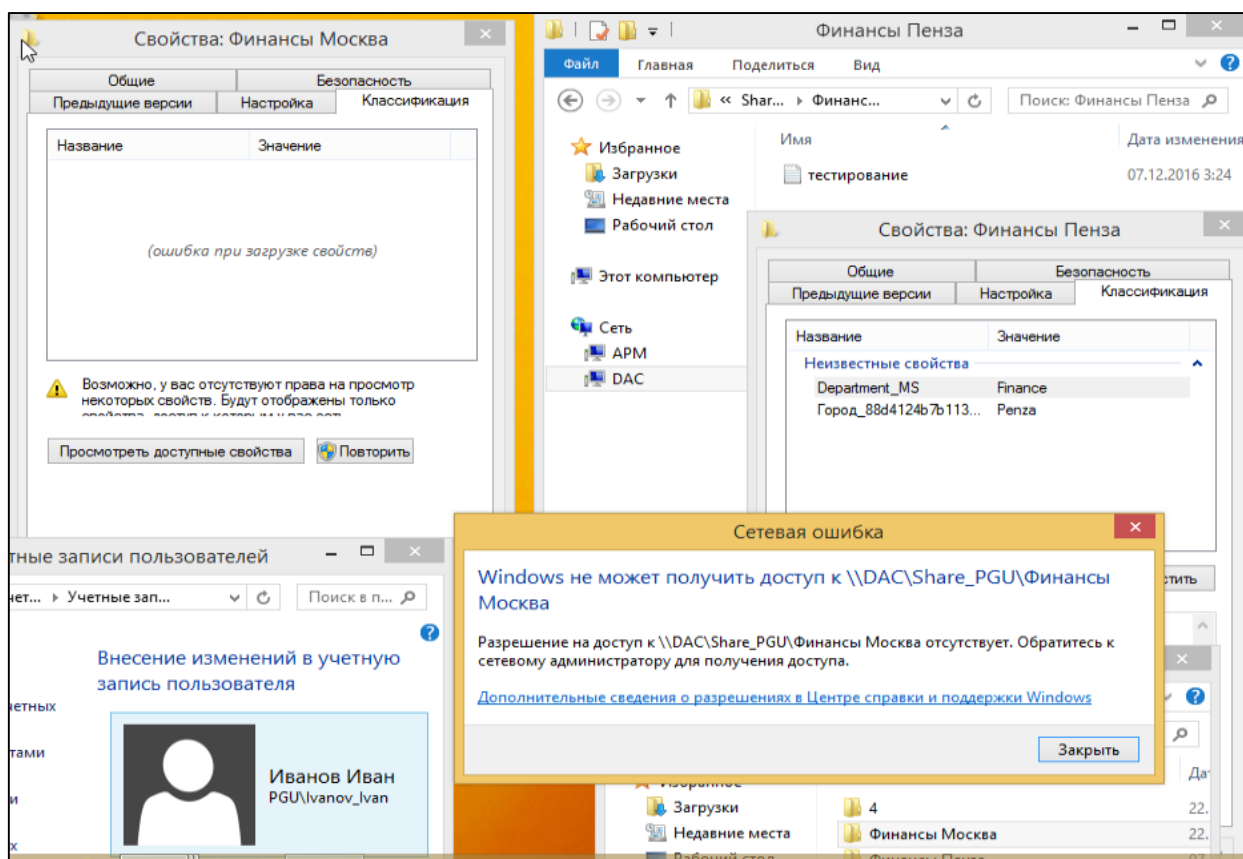


Рисунок 30 – Проверка работы DAC

6 Преимущества динамического контроля доступа при реализации типовых атак

В данной работе рассматривались следующие виды атак:

- анализ сетевого трафика;
- подмена;
- внедрение ложного объекта;
- модификация информации;
- отказ в обслуживании.

Далее был сделан обзор вышеприведенных атак.

Анализ сетевого трафика. Основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве, подключены по физическим каналам и взаимодействие между ними осуществляется программно. С помощью программно-аппаратных устройств или программного обеспечения (ПО), позволяющего анализировать передаваемые и поступающие пакеты по сетевому соединению, появляется возможность скомпрометировать циркулирующую по каналу информацию.

В современном мире, программы для анализа трафика получили название снифферы и могут работать в сетях во благо организации. Таким образом специалисты могут проследить весь трафик и сделать соответствующие выводы. Но есть сетевые приложения, которые передают данные в текстовом формате и без шифрования или другой защиты.

Нарушитель, используя сниффер, может получить нужные пакеты, перехватив поток передаваемых данных. Дальнейший их анализ позволит извлечь необходимую информацию, такую как используемые протоколы, статические пароли пользователей к удаленным хостам, доступные порты сетевых служб и другую в зависимости от конкретного случая. При проведении анализа сетевого трафика нарушитель пытается понять, как устроена сеть и, в случае успеха, может скомпрометировать информацию.

По характеру воздействия анализ сетевого трафика является пассивным воздействием (возможность изменения трафика отсутствует), осуществляется внутри одного сегмента сети на канальном уровне *OSI*. Реализация данной атаки без обратной связи ведет к нарушению конфиденциальности информации.

Подмена доверенного объекта сети.

Под доверенным объектом понимается элемент сети (компьютер, межсетевой экран, маршрутизатор и т.п.), имеющий легальное подключение, и которому присвоены права для доступа к сетевым ресурсам информационной системы.

Осуществление атаки "подмена доверенного объекта сети" и передача по каналам связи сообщений от его имени с присвоением его прав доступа возможна в системах, где используются нестойкие алгоритмы идентификации и аутентификации хостов. Типичным примером является перехват TCP-сессии.

Протокол TCP наиболее используемый в настоящее время протокол транспортного уровня глобальной сети. Он служит для исправления ошибок, возникающих в процессе передачи пакетов, устанавливая виртуальный канал. По данному каналу принимаются и передаются пакеты и регистрируется их последовательность, происходит управление информационным потоком. Если пакет был искажен, то создается повторная передача и ко окончанию передачи канал закрывается.

Существуют две разновидности процесса осуществления удаленной атаки типа "подмена доверенного объекта сети":

- атака с установлением виртуального канала;
- атака без установления виртуального канала.

Процесс осуществления атаки с установлением виртуального канала состоит в присвоении прав доверенного пользователя, что позволяет злоумышленнику вести сеанс работы с объектами системы от имени доверенного пользователя. Для формирования ложного TCP-пакета

атакующему достаточно подобрать соответствующие текущие значения идентификаторов TCP-пакета для данного TCP-соединения (например, FTP-или TELNET-подключение).

Так как для служебных сообщений в распределенных сетях часто используется передача одиночных сообщений, не требующих подтверждения, виртуальное соединение не создается. *Атака без установления виртуального канала* заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) о ложном изменении маршрутно-адресных данных. Идентификация передаваемых сообщений осуществляется только по сетевому адресу отправителя, который легко подделать. Типовая удаленная атака, использующая *навязывание ложного маршрута*, основана на описанной идее.

Подмена доверенного объекта сети является *активным воздействием*, совершаемым с целью нарушения *конфиденциальности и целостности информации*. Данная удаленная атака может являться как *внутрисегментной*, так и *межсегментной*, как с *обратной связью*, так и *без обратной связи* с атакуемым объектом и осуществляется *на сетевом и транспортном уровнях модели OSI*.

Внедрение ложного объекта. Архитектура Интернета создавалась в условиях, когда внутри сети существовало доверие к действиям отдельных участников. В распределенных сетях механизмы идентификации сетевых управляющих устройств (маршрутизаторов) не обеспечивают безопасное использование протоколов управления сетью. Если участник сети (маршрутизатор) заявляет, что он владеет блоком адресного пространства, остальная часть IP-сети верит ему на слово и адресует ему весь соответствующий трафик. Значит, можно создать любой сетевой блок и запустить его в IP-сети, придав анонимность любой атаке, связанной с изменением маршрутизации и внедрением в систему ложного объекта. Такой тип воздействия на сетевую информационную систему ещё называют атакой типа MITM (man in the middle, "человек посередине").

Для перехвата трафика злоумышленники используют уязвимости, присущие протоколам различных уровней стека TCP/IP: сетевому, транспортному и прикладному. На сегодняшний день в подавляющем большинстве применяются стандартные протоколы семейства TCP/IP, среди которых к наиболее уязвимым относятся следующие: протокол управления передачей TCP, межсетевое взаимодействие IP, эмуляции терминала Telnet, передачи файлов FTP, разрешения адресов ARP, службы доменных имен DNS, управляющих сообщений сети Интернет ICMP и сетевого управления SNMP. Кроме того, для обеспечения эффективной и оптимальной маршрутизации в сетях применяются динамические протоколы RIP и OSPF, позволяющие маршрутизаторам обмениваться информацией друг с другом и обновлять таблицы маршрутизации.

Атакующий ставит целью внедрение ложного объекта в сеть путем изменения таблиц маршрутизации и навязывания ложного маршрута. Основная задача злоумышленника – не только прервать сообщение между сетями, а в первую очередь перевести трафик через свой хост, чтобы извлечь полезную информацию.

Реализация атаки основывается на уязвимостях или ошибках настройки протоколов маршрутизации (RIP, OSPF) и управления сетью (ICMP, SNMP).

Отказ в обслуживании (DoS, DDoS-атаки). Одной из возможностей сетевой ОС установленной на каждом объекте распределенной сети, является наличие сетевых служб, позволяющих удалённым пользователям использовать ресурсы данного объекта. Программа-сервер (например, FTP-сервер или Web-сервер), запущенная в сетевой ОС компьютера, обеспечивает удаленный доступ к FTP- или Web-ресурсам этого компьютера. Пользователь отправляет запросы на предоставление услуги, ОС обрабатывает приходящие извне запросы, пересылает их на соответствующий сервер (FTP или Web), а сервер отвечает на них по созданному виртуальному каналу.

Любая операционная система имеет ограничения по количеству открытых виртуальных соединений и существует предел ответов на

поступающие запросы. Данные ограничения зависят от системных ресурсов, основными из которых являются вычислительные мощности, оперативная память, дисковое пространство или пропускная способность каналов связи. Если какой-то из ресурсов достигнет максимальной загрузки, приложение будет недоступно.

Как правило, атаки типа DoS (Denial of service) направлены на истощение критичных системных ресурсов, что приводит к прекращению функционирования системы, т.е. к отказу в обслуживании и невозможности доступа к серверу удаленных пользователей.

Выделяется два типа отказа в обслуживании: первый, основанный на ошибке в приложении, и второй, основанный на плохой реализации или уязвимости протокола [10].

Отказ в обслуживании приложения становится возможен, если уязвимости приложения ведут к получению контроля над машиной (например, с помощью переполнения буфера обмена). Приложение станет недоступным либо из-за нехватки ресурсов, либо из-за аварийного завершения. Уязвимость приложения может быть использована и для нарушения работоспособности других компонентов системы, таких как сервер СУБД или сервер аутентификации [7].

Сетевой отказ в обслуживании основывается на особенностях стека протоколов TCP/IP.

Если атака выполняется одновременно с большого числа хостов, говорят о *распределённой атаке типа "отказ в обслуживании"* – DDoS-атаке (Distributed Denial of Service). В некоторых случаях к DDoS-атаке приводит легальное действие, например, на популярном Интернет-ресурсе указана ссылка на сайт, размещённый на не очень производительном сервере (так называемый слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер, и он очень быстро становится недоступным или доступ к нему затрудняется в результате перегруженности. Ниже представлены некоторые типы подобных атак, однако, это всего лишь

малая часть от существующих на сегодняшний день вариантов DoS-атак, информация о которых постоянно обновляется на специализированных Web-сайтах:

- SYN-flood;
- UDP-flood;
- ICMP-flood (ICPM-smurfing);
- Mailbombing.

В результате исследования динамического контроля доступа при реализации описанных типовых атак были выделены следующие преимущества, представленные в таблице 1.

Таблица 1 – Преимущества динамического контроля доступа при реализации типовых атак

Название атаки	Преимущества
Анализ сетевого трафика	<p>Благодаря введению безопасного туннелирования для гибкой аутентификации (Flexible Authentication Secure Tunneling, FAST) используется защищенный канал, который обеспечивает защиту от сетевого мониторинга.</p> <p>С помощью динамического контроля доступа стал возможным контроль устройства, с которого выполнен вход. Таким образом можно запретить подключение к серверу с мобильных устройств, тем самым уменьшив область возможного перехвата информации.</p>

Продолжение таблицы 1

Название атаки	Преимущества
Подмена	<p>Образованный с помощью безопасного туннелирования для гибкой аутентификации защищенный канал, позволяет системам, подключенным к домену, защищать проверку подлинности пользователей Kerberos от спуфинга ошибок центра распространения ключей Kerberos, связанных с переходом на использование NTLM или менее надежного шифрования.</p> <p>Благодаря комплексной проверке подлинности, центр распространения ключей может создавать билеты служб с данными авторизации не только для конкретных пользователей, но еще и для устройств, для которых настроена поддержка данных авторизации.</p>
Внедрение ложного объекта	<p>После настройки динамического контроля доступа добавляются маркеры к пользователям и ресурсам. Поэтому это усложняет работу злоумышленника внедрение ложного объекта. Дополнительно появилась возможность контроля</p>

Продолжение таблицы 1

Название атаки	Преимущества
Внедрение ложного объекта	<p>устройства, с которого выполнен вход, что также повышает защиту от данной атаки. Благодаря комплексной проверке подлинности злоумышленнику потребуется потратить намного больше времени чтобы понять алгоритм защиты, маркировку и классификацию, используемую в организации.</p>
Модификация информации	<p>С помощью динамического контроля доступа, автоматической классификации файлов и службы Active Directory Right Management Services (AD RMS) появилась возможность</p> <p>Защищать файлы “на лету”, т.е. при появлении нового файла на сервере, он автоматически классифицируется, ему присваиваются метки и он тут же защищается.</p>
Отказ в обслуживании	<p>При реализации данной атаки динамический контроль доступа преимуществ не дает, т.к. не способен отражать атаки типа «отказ в обслуживании»</p>

Таким образом был сделан вывод, что переход на ОС Windows Server 2012R2 и использование динамического контроля доступа повышает безопасность при реализации следующих атак:

- анализ сетевого трафика;
- подмена;
- внедрение ложного объекта;
- модификация информации.

Так же было выявлено что при реализации атак типа «отказ в обслуживании» данная технология преимуществ не дает.

Далее DAC был рассмотрен как механизм повышающий обеспечение конфиденциальности значимой информации в организации. Нужно отметить что после внедрения DAC добавляется новый уровень контроля доступа к ресурсам домена. Списки контроля доступа и все остальные разрешения работают без изменений. При доступе пользователя к ресурсам добавляется возможность учитывать:

- устройство с которого выполняется попытка получения доступа;
- место положение пользователя;
- проверка дополнительной информации о личности пользователя;
- данные аутентификации.

Также с помощью DAC можно строить гибкие системы, что в целом, повысит уровень защиты информации от несанкционированного доступа.

ЗАКЛЮЧЕНИЕ

В рамках дипломной работы была рассмотрена технология, внедренная в Windows Server 2012, позволяющая управлять доступом к информации на основе конкретных атрибутов или определенных критериев, именуемая как динамический контроль доступа.

На первом этапе был сделан обзор возможности и преимущества динамического контроля доступа, рассмотрены серверные роли, описаны отличия динамического контроля доступа от списков контроля доступа.

На втором этапе были описаны основные сценарии использования динамического контроля доступа. Также была рассмотрена их реализация.

На третьем этапе были рассмотрены и описаны свойства ресурсов и свойства ссылочного ресурса. А также объяснены их различия и особенности использования.

На четвертом этапе сделано описание классификации файлов различными способами.

На пятом этапе произведена настройка и применение централизованной политики доступа с помощью динамического контроля доступа.

За заключительном, шестом этапе, было проведено исследование в ходе которого были выявлены преимущества использования динамического контроля доступа при реализации типовых атак.

Таким образом, техническое задание на дипломную работу выполнено в полном объёме.

СПИСОК ЛИТЕРАТУРЫ

- 1 Динамический контроль доступа -
<http://windowsitpro.com/security/windows-server-2012-active-directory-security-changes>
- 2 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
- 3 ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту.
- 4 Введение в динамический контроль доступа -
<https://habrahabr.ru/company/netwrix/blog/145881/>.
- 5 Изменение в AD Windows server 2012 - <https://technet.microsoft.com/ru-ru/windowsserver/dn167669.aspx>.
- 6 Обзор динамического контроля доступа -
[https://msdn.microsoft.com/ru-ru/library/dn408191\(v=ws.11\).aspx](https://msdn.microsoft.com/ru-ru/library/dn408191(v=ws.11).aspx)
- 7 Основные понятия в области ИБ -
<http://www.intuit.ru/studies/courses/16655/1300/lecture/25504?page=3>
- 8 Управление ресурсами по-новому - <https://habrahabr.ru/post/176467/>
- 9 Служба каталогов AD. Разграничение прав доступа -
<http://studopedia.org/9-11886.html>
- 10 Классификация и описание некоторых удаленных атак -
<http://www.nestor.minsk.by/sr/2004/06/40613.html>

ПРИЛОЖЕНИЕ А

Результат проверки дипломной работы по системе «Антиплагиат»

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Динамический контроль доступа в ОС Windows Server 2012 R2» студента 6 курса К.А. Пастухова направления 10.05.02, направление подготовки информационная безопасность телекоммуникационных систем.

Руководитель ВКР В.А. Сулов.

Информация о документе:

Имя исходного файла: VKR_Pastukhov.docx
Имя компании: Пензенский гос. Университет
Тип документа: Прочее
Имя документа: Группа 11ПТ1 ВКР Пастухов КА
Дата проверки: 12.01.2017 19:19
Модули поиска: Интернет (Антиплагиат), Диссертации и авторефераты РГБ, Университетская библиотека онлайн, Модуль поиска ЭБС "Лань", Модуль поиска ЭБС БиблиоРоссика, Пензенский гос. Университет, Кольцо вузов

Текстовые

статистики:

Индекс читаемости: сложный
Неизвестные слова: в пределах нормы
Макс. длина слова: выше нормы!
Большие слова: в пределах нормы

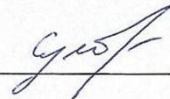
Оригинальные блоки: 74,95%

Заимствованные блоки: 25,05%

Заимствование из "белых" источников: 0%

Итоговая оценка оригинальности: **74,95%**

12.01.2017



В.А. Сулов

