МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Исследование недокументированных возможностей Active Directory

Специальность Системы Информационной Безопасности

Выполнил(а) Ермощенко Анастасия Юрьевна Группа СИБ-16-2
(Ф.И.О.)

Научный руководитель к.т.н. доцент Сатимова Елена Григорьевна
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных_____

Кафедра «Системы Информационной Безопасности»_____

Специальность «Системы Информационной Безопасности»_____

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Ермощенко Анастасии Юрьевне_____
(Ф.И.О.)

Тема проекта «Исследование недокументированных возможностей Active Directory»_____
_____

Утверждена приказом по университету № _____от «___» _____2020 г.

Срок сдачи законченного проекта «____» _____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – Доменная структурная схема предприятия, сервер Windows 2012 R2, средства Active Directory для организации безопасности, Backup-сервер Windows Server 2012 R2, расширение PowerShell, BAT._____

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Целью данной работы является проектировка и организация защиты Active Directory для мероприятия дополняя стандартные средства недокументированными возможностями. Акцент в данной работе делался на восполнение проблем безопасности Active Directory используя недокументированные возможности Windows Server. Так же целью работы является автоматизация процессов в работе AD используя те же недокументированные возможности.

Перечень графического материала (с точным указанием обязательных чертежей): исходная Доменная структурная схема предприятия__

Основная рекомендуемая литература: Александр Кенин Практическое руководство системного администратора, веб-сайт https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory, Робби Аллен Active Directory. Сборник рецептов для Windows Server 2003 и Windows 2000. _____

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Проектирование AD предприятия	17.02.2020 – 20.02.2020	
Настройка клиентов, Поднятие домена	21.02.2020 – 28.02.2020	
Создание пользователей. Предоставление привилегий и ролей	01.03.2020 – 08.03.2020	
Создание групп, компьютеров. Настройка разрешений	09.03.2020 - 18.03.2020	
Организация различных видов аудита AD	19.03.2020 – 27.03.2020	
Организация защиты удаленного рабочего стола	28.03.2020 - 07.04.2020	
Настройка и применение групповых политик	08.04.2020 - 18.04.2020	
Организация резервного копирования	19.04.2020 - 30.04.2020	
Анализ рисков ИБ. БЖД.	01.05.2020 - 09.05.2020	

Аннотация

Целью данной работы является проектировка и организация защиты Active Directory для мероприятия дополняя стандартные средства недокументированными возможностями.

Акцент в данной работе делался на восполнение проблем безопасности Active Directory используя недокументированные возможности Windows Server. Так же целью работы является автоматизация процессов в работе AD используя те же недокументированные возможности. Входные данные работы – спроектированная мною незащищенная учебная Active Directory.

Итогами работы станут:

1) PowerShell-скрипты для автоматизации процесса сбора данных по пользователям, а так же по защите домена
2) Групповые политики для защиты домена
3) Метод защиты от атак на AD

Annotation

The purpose of this work is to design and organize Active Directory security for an event, supplementing standard tools with undocumented features. The emphasis in this paper was on addressing Active Directory security issues using the undocumented features of Windows Server. In addition, the goal of the work is to automate the processes in the work of AD using the same undocumented features. The input to the job is an unprotected Active Directory tutorial that I designed.

The results of the work will be:

1) PowerShell scripts to automate the process of collecting data by users, as well as to protect the domain.
2) Group policies for domain protection.
3) Method of protection against attacks on Active Directory.

Аннотациясы

Бұл жұмыстың мақсаты стандартты құралдарды құжатсыз мүмкіндіктермен толықтыра отырып, оқиға үшін Active Directory қауіпсіздігін жобалау және ұйымдастыру болып табылады. Бұл жұмыста Windows Server-тің құжатсыз мүмкіндіктерін қолдана отырып, Active Directory қауіпсіздігі мәселелерін шешуге баса назар аударылды. Сондай-ақ жұмыстың мақсаты бірдей құжатсыз мүмкіндіктерді пайдалана отырып, AD жұмысындағы процестерді автоматтандыру болып табылады. Жұмысқа кіріспе - мен жасаған қорғалған емес Active Directory оқулығы.

Жұмыстың нәтижелері:

1) PowerShell сценарийлері пайдаланушылардың деректерді жинау процесін автоматтандыруға, сонымен қатар доменді қорғауға арналған.
2) Домен қорғаудың топтық саясаты.
3) Active Directory-ге шабуылдардан қорғау әдісі.

Содержание

Введение

Данный дипломный проект посвящен актуальной проблеме построения надежной и безопасной службы каталогов Active Directory.

Атаки различной сложности на вычислительные системы существуют с момента появления компьютеров. Каждый день растет число организаций, безопасность которых была атакована различными способами, которые значительно изменили характер угроз. Атаки на различного рода учреждения с целью получения их интеллектуальной собственности стали обычной практикой во всем мире. Электронные войны растут рекордными темпами.

Актуальность данного проекта в разработке новых методов и стратегии использования Active Directory (AD), для повышения уровня защиты Информационных систем, а также в своевременном реагировании на события, происходящие в системе.

Active Directory (AD) – это хранилище информационных ресурсов множества предприятий, и оно должно быть надежно защищено. Безопасность непредотвратимо требует компромисса. Способы повысить уровень защиты существуют всегда, но они чаще всего требуют для этого неопределенных затрат либо снижают гибкость и функциональность системы. В данном проекте представлены примеры, не связанные с затратами, но которые могут значительно повысить безопасность общей инфраструктуры AD.

Служба каталогов (СК) является основой для построения информационных систем огромного количества организаций и его безопасность становится одним из ключевых вопросов, независимо от масштабов и деятельности организаций.

Уровень защищенности службы каталогов соизмерим с уровнем безопасности всей компании. Рационально проводить регулярный мониторинг системы в целях выявления умышленных действий нарушителя и всегда быть готовым к их отражению, имея детальный план действий для различных ситуаций, чтобы максимально усложнить работу злоумышленнику.

Первый основополагающий закон информационной безопасности (ИБ) гласит: «Никто не верит, что может произойти что-то плохое до тех пор, пока оно на самом деле не происходит» [1]. Администраторы ИТ и ИБ-отделов не уделяют должного внимания защите AD DS, будучи уверенными, что их системе ничего не угрожает, например, от «внутреннего» злоумышленника, что часто приводит к печальным последствиям. Таким образом, не следует заботиться только об одних аспектах информационной безопасности и пренебрегать другими. Необходимо учитывать все особенности системы чтобы подход к обеспечению ИБ был комплексным.

1 Теоритическая часть

1.1 Введение в Active Directory

Active Directory (сокращенно AD) - это иерархическая система хранения данных об объектах сети, предоставляющая механизмы для поиска, использования и управления этими данными, выступая средством для построения крепкого фундамента IT-инфраструктуры организации вне зависимости от размера и вида деятельности. Active Directory обеспечивает решение практически всех административных задач функционирования корпоративной сети. AD предоставляет возможность администраторам использовать групповые политики для стандартизации настроек пользовательской рабочей среды, выполнять развертывание и последующее обновление программного обеспечения на множестве компьютеров в сети и т.д. Впервые продукт был представлен в 1999 году с выходом Windows 2000 Server и создавался изначально, как LDAP-совместимая реализация службы каталогов. Однако с выходом Windows Server 2008 AD поддерживает взаимодействие с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль [2].

Технология Active Directory основана на стандартных Интернет - протоколах и помогает четко определять структуру сети. В версиях Windows ниже Windows 2000 для сетевого взаимодействия использовался в основном протокол NetBIOS, в то время как служба Active Directory интегрирована с DNS, работая поверх TCP/IP.

Логическая структура Active Directory.

Логическая структура AD не привязана к топологии корпоративной сети и выстраивается исходя из требований решения административных и организационных задач. Логическими компонентами являются:

- объект;
- организационное подразделение;
- домен;
- дерево;
- лес;

Объекты (Object) представляют из себя ресурсы Active Directory, хранящиеся в виде иерархической структуры контейнеров и подконтейнеров, выступающей набором идентифицирующих атрибутов. Для объекта пользователя, например, таковыми являются: имя, пароль, членство в группе и т.д. Образующие объект атрибуты определяются классом объекта. Класс пользователя, в частности, описывает образующие объект пользователя атрибуты.

Таким образом объекты классифицируются по сходным характеристикам, автоматически наследуя атрибуты своего класса при создании. Хотя в базовой структуре Active Directory определен исходный набор классов объектов и описываемых ими атрибутов, администраторы и приложения могут модифицировать доступные классы и определяемые ими

атрибуты объектов в Active Directory Schema. В терминологии баз данных схема является структурой таблиц и полей, а также их взаимосвязей. Active Directory Schema выступает неким набором данных (классов объектов), определяющим организацию и хранение реальной информации (атрибутов объекта) в каталоге.

Организационное подразделение (Organization Unit) - объект-контейнер, предназначенный для группировки ресурсов AD в логические группы администрирования в рамках домена. Элементами группировки могут являться компьютеры, учетные записи пользователей или другие организационные подразделения. Именно подразделения зачастую являются объектами применения групповых политик. С появлением Active Directory организационные подразделения выступают наименьшим контейнером, которому могут быть назначены административные разрешения.

Домен (Domain) — это основная логическая единица сетевой модели организации, в которую входят все сетевые объекты, такие как пользователи, компьютеры, принтеры, общие ресурсы и т.д. Домен в AD является своего рода границей административной безопасности для объектов и содержит собственные политики безопасности. Домен в AD использует пространство имен, соответствующее системе именования DNS.

Деревом (Domain tree) называется один или несколько организованных в иерархическую структуру доменов, использующих общее пространство имен. Домены внутри дерева соединены двунаправленными транзитивными отношениями доверия. Каждый домен в дереве AD использует общую схему и глобальный каталог.

Лес (Domain forest) - это высший уровень логической иерархии Active Directory. Лес объединяет деревья, которые поддерживают общую схему и общий глобальный каталог. Лес обладает определенным набором атрибутов и является основной единицей административной безопасности в AD. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом. Именно в корневом домене хранится схема AD. Следует отметить, что использование общего пространства имен в рамках леса не обязательно. В сети всегда есть как минимум один лес, так как он автоматически создается при установке первого контроллера домена AD.

Поскольку домены разграничивают зоны безопасности, специальный механизм, называемый доверительными отношениями, обеспечивающий возможность объектам в одном домене (доверяемом) обращаться к ресурсам в другом (доверяющем).

В Active Directory поддерживаются следующие типы доверительных отношений [3].

1) Доверие к родительскому и дочернему доменам, а также к корневому домену дерева.

Данный тип доверия Active Directory выстраивает автоматически между родительскими и дочерними доменами в дереве. Эти отношения являются двусторонними. Это означает, что запросы на доступ к ресурсам

могут поступать от одного из данных доменов к другому и наоборот. Также отношения являются транзитивным, т. е. контроллеры доверяемого домена пересылают запросы на аутентификацию контроллерам доверяющих доменов.

Двусторонние транзитивные доверительные отношения автоматически создаются и между корневыми доменами деревьев в одном лесу.

2) Доверие к внешнему домену.

Данный тип доверительных отношений не является транзитивным, то есть доверительные отношения существуют лишь между двумя выбранными доменами и не распространяются на другие.

3) Доверие к сокращению.

Данный тип является способом создания прямых доверительных отношений между двумя доменами, которые уже могут быть связаны цепочкой транзитивных доверий, но которым нужно оперативнее реагировать на запросы друг друга.

4) Доверие к сфере.

Данный тип доверия служит для подключения домена Windows Server к сфере Kerberos, которая не поддерживает Windows и использует протокол защиты Kerberos V5. Доверие к сфере может быть транзитивным или не транзитивным, одно или двусторонним.

5) Доверие к лесу.

Данный тип упрощает управление несколькими лесами и обеспечивает более эффективное защищенное взаимодействие между ними. Этот тип доверия позволяет обращаться к ресурсам в другом лесу по той же идентификации пользователя, что и в его собственном лесу.

За построение связи между компонентами логической структуры и топологией корпоративной сети отвечает физическая структура Active Directory, основными компонентами которой являются подсети, сайты и контроллеры домена.

Подсеть (Subnet) - объект, позволяющий определить принадлежность компьютеров к тому или иному сайту. Подсети обладают заданной областью IP-адресов и сетевой маской. Имена подсетей указываются в формате сеть/битовая маска, например 192.168.1.0/24. Подсеть описывает отдельную IP-сеть и связывает ее с сайтом Active Directory. При регистрации в домене происходит фиксация принадлежности компьютера к определенному сайту. Это позволяет обслуживать пользователей компьютера ближайшему контроллеру домена.

Сайт (Site) - это группа тесно связанных между собой компьютеров и контроллеров домена, образованная в рамках одной или нескольких подсетей, используемая для планирования физической структуры или топологии сети. Следует отметить, что планирование сайта происходит независимо от логической структуры домена. Active Directory позволяет создавать множество сайтов в одном домене или один сайт, охватывающий множество доменов. Сайт является базовой единицей репликации и создается

для более эффективной передачи данных каталога по сети. Процедура репликация между контроллерами домена, находящимися в границах одного сайта, по умолчанию выполняется значительно чаще, нежели между контроллерами, находящимися в разных сайтах.

Контроллер домена (Domain controller) - это сервер, обеспечивающий работу Active Directory. И хотя для функционирования AD достаточно одного контроллера домена, следует учесть, что при выходе его из строя работа AD будет полностью парализована. Поэтому в полноценной структуре рекомендуется использовать не менее двух контроллеров. Каждый контроллер домена содержит собственную копию каталога Active Directory.

Данные каталога предоставляются пользователям и компьютерам посредством хранилища данных (data stores) и глобальных каталогов (global catalogs). Хотя большинство функций Active Directory и задействуются через хранилище данных, глобальные каталоги важны не меньше, поскольку используются для авторизации в системе и поиска информации. Обычные пользователи не смогут войти в домен при недоступности глобального каталога.

Доступность и распространение данных Active Directory обеспечиваются посредством протоколов доступа к каталогу (directory access protocols) и репликации (replication). Репликация необходима для распространения обновленных данных на контроллеры домена. Основным методом распространения обновлений является репликация с несколькими хозяевами, но часть изменений обрабатываются только специализированными контроллерами, так называемыми хозяевами операций (operations masters).

Хранилище данных содержит сведения о важнейших объектах службы каталогов Active Directory, таких как учетные записи, общие ресурсы, ОП и групповые политики. Зачастую хранилище данных называют просто каталогом (directory), хранящимся на контроллере домена в файле NTDS.DIT, расположение которого определяется при установке Active Directory (это обязательно должен быть диск с файловой системой NTFS). В то же время часть данных каталога можно хранить и отдельно от основного хранилища, например, групповые политики, сценарии и другую информацию, записанную в общем системном ресурсе SYSVOL. Предоставление информации каталога в совместное пользование называют публикацией (publish).

Глобальный каталог является своего рода индексом базы данных Active Directory, хранящий частичную копию ее содержимого. В частности в нем содержатся ссылки на все имеющиеся в AD объекты, что обеспечивает возможность пользователям осуществлять поиск объектов, находящихся в других доменах леса. В глобальный каталог реплицируются только наиболее часто используемые в операциях поиска атрибуты объекта. Если кэширование членства в универсальных группах локально не производится,

вход в сеть осуществляется на основе предоставленной ГК информации о членстве в универсальной группе.

В каталоге хранятся сведения следующих типов: данные домена, данные схемы и данные конфигурации. Данные домена реплицируются на все контроллеры домена. Так как все контроллеры домена равноправны, все вносимые изменения с любого контроллера домена будут реплицированы на все остальные контроллеры домена. Схема и данные конфигурации реплицируются на все домены дерева или леса. Кроме того, все объекты индивидуального домена и часть свойств объектов леса реплицируются в ГК. Это означает, что контроллер домена хранит и реплицирует схему для дерева или леса, информацию о конфигурации для всех доменов дерева или леса, а также все объекты каталога и свойства для собственного домена.

Контроллер домена, на котором хранится ГК, содержит и реплицирует информацию схемы для леса, информацию о конфигурации для всех доменов леса и ограниченный набор свойств для всех объектов каталога в лесу (он реплицируется только между серверами ГК), а также все объекты каталога и свойства для своего домена.

Упрощенный протокол доступа к каталогам (Lightweight Directory Access Protocol, LDAP) является открытым и кроссплатформенным протоколом соединений в сетях TCP/IP, спроектированным специально для доступа к службам каталогов с минимальными издержками. В LDAP также определены операции, используемые для запроса и изменения информации каталога.

Клиенты Active Directory применяют LDAP для связи с компьютерами, на которых работает Active Directory, при каждом входе в сеть или поиске общих ресурсов. LDAP упрощает взаимосвязь каталогов и переход на Active Directory с других служб каталогов.

1.2 Требования к безопасности Active Directory

Так как Active Directory является системой управления всей IT-инфраструктурой организации, обеспечение безопасности служб каталогов становится ключевым моментом, поскольку степень защищенности последней определяет уровень безопасности всей организации.

Проектируя Active Directory, следует помнить, что безопасность последней напрямую зависит от системы информационной безопасности в целом. Еще в 2000 году за авторством Скотта Калпа вышла статья "Десять непреложных законов управления безопасностью". [1] И хотя с тех пор прошло уже двадцать лет, актуальность приведенных ниже правил не подвергается сомнению.

1. "Никто не верит, что может произойти что-то плохое до тех пор, пока это не случится".

К сожалению, огромное количество сотрудников компаний зачастую пренебрегают требованиями безопасности в своей повседневной работе с сетью. Это вовсе не означает, что они осознанно подвергают угрозам сеть, а просто-напросто, будучи сконцентрированными на своей деятельности, не

задумываются над вопросами компьютерной безопасности. Ведь не так велика вероятность, что им отправят вредоносное письмо по электронной почте, или попытаются взломать их пароль. Но очень часто злоумышленнику достаточно обнаружить маленькую щель в обороне вашей сети для проникновения и последующего обрушения этой самой обороны. Соответственно полагаться на добровольные меры обеспечения безопасности нельзя. Должна быть разработана комплексная политика безопасности по определению ценности информации в вашей сети с последующим внедрением мер по обеспечению ее защиты.

2. "Безопасность работает только в том случае, если безопасный путь является еще и легким".

Для обеспечения безопасности сети IT-специалистам должны быть предоставлены полномочия, но в то же время не стоит превращать сеть в полицейское государство, иначе наверняка поднимется восстание. Если меры по обеспечению безопасности препятствуют бизнес-процессам компании, пользователи могут и будут их игнорировать. Иными словами, разработанная политика должна обеспечивать разумный компромисс между безопасностью и производительностью.

3. "Если вы не успеваете исправлять уязвимости, ваша сеть недолго будет вашей".

Программное обеспечение содержит ошибки, в том числе связанные с безопасностью. И есть огромное количество людей, стремящихся обнаружить эти ошибки, чтобы использовать их впоследствии. И как бы не была безопасна ваша сеть сегодня, всё может измениться в одночасье, если будет обнаружена критическая уязвимость. Не менее, а зачастую даже более критической может быть совокупность менее серьезных уязвимостей. Нужно всегда "держать руку на пульсе" новостей мира информационной безопасности, для того чтобы быть готовым затыкать бреши в обороне по мере их появления.

4. "Нет смысла исправлять уязвимости на компьютере, который с самого начала не был защищен".

Какой смысл в исправляющих критические уязвимости обновлениях на контроллере домена, если у вас слабый административный пароль? Или если диск вашего веб- сервера предоставлен всему миру? Или если у вас включен гостевой доступ к общему ресурсу, на котором хранится конфиденциальная информация? Оборона должна быть комплексной.

5. "Вечная бдительность - цена безопасности".

Внимательно прочитали пункты 3 и 4? Казалось бы, ваша сеть теперь безопасна и можно успокоиться. Не стоит. Не смотря на всё предпринятое, ваша сеть всё еще подвержена атакам злоумышленника. Можно нарушить работу сервера, отправляя ему в огромном количестве вполне себе легитимные запросы. Или осуществлять попытки подбора пароля методом brute-force. Ни патчи безопасности, ни развернутая политика не помогут, потому что подобные действия при всей своей вредоносности не являются

незаконными в широком смысле этого слова. Как раз на этот случай существуют журналы событий, позволяющие получать информацию о том, кто использует системные ресурсы, что они делают, была ли операция успешной или нет. Регулярное отслеживание этих процессов позволяет предпринимать соответствующие меры: блокировать запросы с определенных IP-адресов, отключать учетные записи, находящиеся в зоне риска, устанавливать ловушки и т.д. Таким образом, журнал событий позволяет оценить работоспособность ваших систем и определить правильный курс для обеспечения их безопасности. Но следует с умом подходить к настройке журналов событий - не следует разворачивать аудит до такого состояния, когда он начинает превышать ваши возможности по анализу данных. Следует тщательно планировать, какие события следует регистрировать. Наконец возможно наступление момента, когда придется задуматься о приобретении стороннего инструмента интеллектуального анализа данных журнала событий.

6. "Кто-то постоянно пытается подобрать ваши пароли".

Пароли представляют необычайную ценность. Независимо от других правил безопасности, если злоумышленник получит пароль только лишь одного пользователя, он сможет получить доступ к вашей сети и соответственно идеальную позицию для проведения дополнительных атак.

Пароли являются так называемыми "низко висящими фруктами". Большинство пользователей выбирают слабый пароль и не задумываются об его изменении. Если заставить подобного пользователя использовать более стойкий пароль, он наверняка его запишет, что также является уязвимостью. Не нужно быть технически грамотным специалистом для взлома учетной записи, если известен пароль.

Информационная система не может считаться безопасной, если не настроена политика применения надежных паролей. Можно настроить минимальную длину пароля, сложность и срок действия. Подобные меры могут быть частью групповой политики ОС Windows. Кроме того следует задействовать систему блокировки учетных записей и проводить аудит неудачных попыток входа в систему. Также необходимо убедиться, что пользователи понимают, почему нельзя записывать свои пароли.

В дополнение к паролям стоит рассмотреть возможность использования других способов аутентификации. Примерами могут служить использование смарт-карт или биометрическая аутентификация.

Иными словами, процесс аутентификации должен обеспечивать уровень безопасности, соизмеримый с остальными мерами безопасности сети.

7. "Только хорошо управляемая сеть является безопасной".

Успех большинства проводимых атак основывается не на недостатках программного обеспечения. Как правило, проникновения организуются за счет неверных параметров конфигурации системы: разрешения, повышенные на период устранения неполадок и оставленные в таком состоянии; учетная

запись временного сотрудника, не отключенная впоследствии; прямое подключение к Интернету, настроенное без одобрения и т.д. При отсутствии порядка в соблюдении определенных процедур будет трудно и даже невозможно отслеживать подобные детали, и в результате ваша система будет подвергнута опасности.

Наличие определенных документированных процедур является абсолютной необходимостью. Все начинается с корпоративной политики безопасности, которая должна быть изложена на широком уровне, определяя уровень ответственности за каждый сегмент сети и общую философию управления, развертывания и эксплуатации сети. Но не стоит останавливаться только на политике высокого уровня. Каждая группа должна разработать операционные процедуры в своей сфере деятельности. Чем конкретнее эти процедуры, тем лучше. И они должны быть задокументированы. Процедуры, существующие в устной форме, не работают.

8. "Чем сложнее сеть, тем труднее обеспечить ее безопасность".

Более сложные сети значительно труднее администрировать. Но это правило выходит за рамки простого администрирования. Важнейшим аспектом является сама архитектура.

а) как выглядят доверительные отношения между доменами в вашей сети? Они просты и понятны? Если не так, существует большая вероятность того, что кто-то попытается злоупотребить ими в целях получения привилегий, которыми не стоило их наделять;

б) известны ли вам все точки доступа к вашей сети? Если одна из групп в вашей компании настроила, к примеру, общедоступный FTP или веб - сервер, это может подорвать безопасность вашей сети в целом;

в) к вашей сети обеспечен доступ сотрудников другой компании, связанной партнерскими отношениями? В таком случае степень безопасности вашей сети приравнивается к партнерской;

Невозможно обеспечить безопасность сети при отсутствии ее понимания, и если вы не в состоянии ее контролировать.

9. "Невозможно избежать всех рисков, необходимо управлять этими рисками".

Самым безопасным компьютером является тот, который отключен от сети, обесточен и до кучи залит бетоном. К сожалению, такой подход не поможет в деятельности вашей компании. Следует помнить, что безопасность любой сети никогда не будет идеальной, и это должно быть учтено при планировании. Ваша цель не должна заключаться в стремлении избежать всех рисков - это просто нереально. Вместо этого следует принять две неоспоримые истины:

а) обязательно наступят времена, когда корпоративная деятельность вступит в конфликт с корпоративной безопасностью. Безопасность - это вспомогательный механизм для компании, а не сама цель. Необходимо взвешенно оценить риски, смягчив их в максимально возможной степени;

б) безопасность вашей сети будет нарушена. Это может быть незначительный сбой или настоящая катастрофа. Будет связано с нападением человека или стихийным бедствием, но рано или поздно ваша сеть будет каким-то образом скомпрометирована. Следует составить план действий в чрезвычайных ситуациях для обнаружения, расследования и восстановления после компрометации.

Решение этих проблем состоит в разработке политики безопасности, которая предусматривает наихудшие сценарии и устанавливает рекомендации по исправлению последствий.

10. "Технология не панацея".

Для обеспечения безопасности недостаточно только лишь технологии. Безопасность сети определяется как технологиями, так и политиками использования этих технологий. Необходимо четко понимать, что требуются защищать, и какие действия для этого следует предпринять. Следует разработать планы действий при чрезвычайных ситуациях. Тщательное планирование совместно с надежной технологией обеспечивают высокий уровень корпоративной безопасности.

На что следует обратить внимание при проектировании и последующей поддержке Active Directory? Для ответа на этот вопрос следует воспользоваться базовыми рекомендациями, которые содержатся в документе Best Practices for Securing Active Directory. Ниже перечислен список мер, которые значительно снижают вероятность совершения несанкционированных действий с базой данных AD [4].

1) Своевременное обновление ОС и ПО позволяет уменьшить вероятность компрометации системы и осуществления несанкционированной злонамеренной деятельности внутри ИТ-инфраструктуры организации. Проводимое на регулярной основе обновление серверов и рабочих станций организации является обязательным требованием для повышения уровня безопасности службы каталога.

2) Эффективная антивирусная защита и защита от вредоносного ПО позволяет существенно повысить защищенность ИТ-инфраструктуры организации в целом.

3) Регулярное резервное копирование AD обеспечивает возможность оперативно восстановить базу данных службы каталогов и удаленные в результате ошибочных действий администраторов объекты AD, а также службу каталога в ситуации катастрофического сбоя. Также не стоит забывать о правильном хранении резервных копий.

4) Эффективная стратегия именования объектов позволяет администраторам службы AD эффективно идентифицировать объекты и управлять данными, хранящимися в AD, сведя к минимуму возможность некорректного назначения прав доступа, делегирования полномочий и назначения политик.

5) Безопасность контроллеров доменов (DC) обеспечивают серверы, хранящие реплику БД службы каталога AD, которые выполняют функции

управления данными AD. Если доступ к контроллеру домена получает злоумышленник, то его деструктивные действия могут вывести из строя или скомпрометировать всю организацию. Обеспечение безопасности контроллеров домена – одна из наиболее важных задач службы информационной безопасности.

6) Защита учетных записей привилегированных пользователей. Учетные записи администраторов сервисов и администраторов данных представляют интерес для взломщика, т.к. дают доступ к ключевым функциям системы и к объектам службы каталога. Необходимо обеспечить их безопасность и мониторинг. Ошибочное включение пользователей в группы с высокими привилегиями может привести к краху системы как из-за отсутствия достаточных знаний и навыков, так и в результате злонамеренных действий.

7) Использование дополнительных возможностей ОС по обеспечению безопасности. Зачастую IT-администраторы отключают ряд систем защиты ОС или ее отдельные службы для упрощения выполнения повседневных рутинных задач. Характерные примеры – User Account Control и Windows Firewall. Не обеспечив использование более совершенных средств защиты, администратор отказывается от имеющихся под рукой и централизованно управляемых встроенных средств ОС, понижая общий уровень безопасности.

8) Использование принципа наименьших привилегий позволит существенно повысить уровень безопасности, уменьшая для злоумышленника область атаки.

9) Блокировка возможности развертывания и выполнения неавторизованных приложений и сервисов повышает безопасность системы.

10) Наличие доступа к Интернету значительно снижает безопасность всей инфраструктуры. Обеспечение безопасного доступа в Интернет и доступа из Интернета к ресурсам организации является одной из важнейших задач по повышению общего уровня безопасности системы.

11) Изменение настроек безопасности по умолчанию. AD предоставляет стандартные параметры безопасности при установке. Необходимо привести их к требованиям корпоративной политики.

12) Следует удалять или блокировать недействительные учетные записи пользователей и компьютеры [4].

2 Практическая часть

2.1 Доменная структура. Описание предприятия

Для начала разберемся в структурной схеме предприятия. Структурная схема предприятия представлена на рисунке 1.

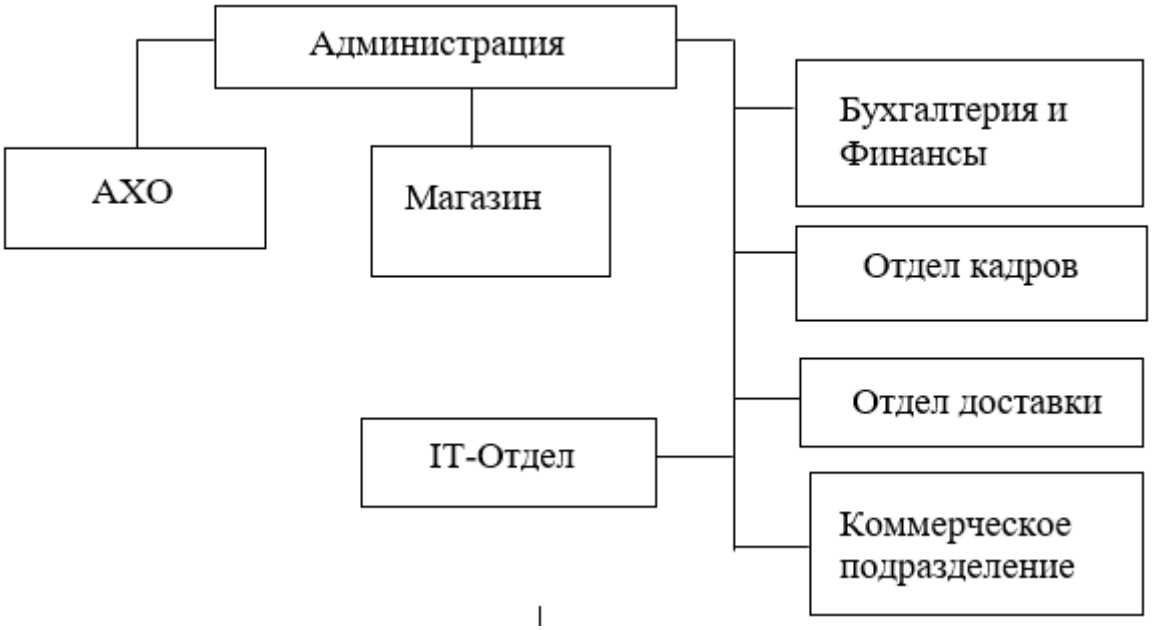


Рисунок 1 – Структурная схема предприятия

Здание А. Одно этажное здание с площадью М1. В помещений происходит прием клиентов. В помещений нужно организовать выход в интернет и телефонную связь. Так же необходимо организовать сеть с зданиями Б и В через интернет и маршрутизаторы.

Здание Б. Имеет три этажа на первом этаже располагаются подразделения Департамент бухгалтерии и финансов, отдел кадров и IT-отдел.

На втором этаже располагается Отдел доставки, коммерческий отдел и администрация компании. В здании находится шесть помещений. В этих помещениях необходимо организовать локальную сеть с общим ресурсом также необходима беспроводная сеть.

Здание В. Одно этажное здание. В нем располагается административно– хозяйственное подразделение, которое занимается хозяйственной деятельностью на предприятии. В помещений нужно

организовать выход в интернет и телефонную связь. Так же необходимо организовать сеть с зданиями А и Б через интернет и маршрутизаторы.

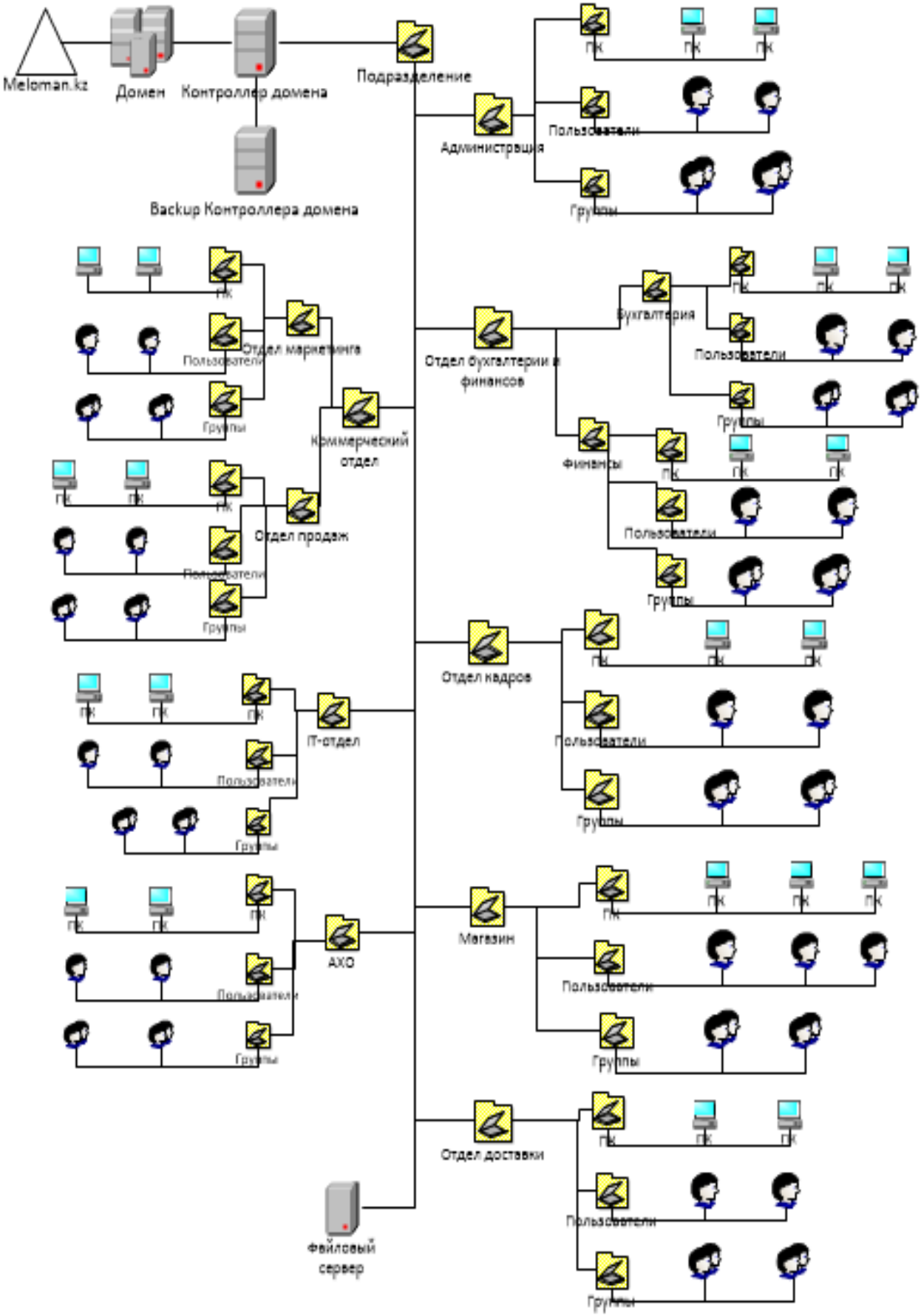


Рисунок 2 - Доменная структура

2.2 Создание групповой политики для RDP-порта

RDP — протокол удалённого рабочего стола. Чаще всего для удаленного подключения используют стандартные порты, такие порты всем известны и всегда открыты. Для уменьшения риска несанкционированного подключения через удаленный рабочий стол была создана групповая политика для изменения RDP-порта.

Значение RDP-порта находится в реестре по адресу HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp, его и нужно изменить.

Групповая политика представляет собой файл с расширением *.adm. Внутри файла находится набор правил групповой политики в виде кода. Создадим файл TEST.adm, внутри которого будет код по изменению значения RDP-порта в реестре. Данный скрипт представлен в приложении А.

Далее нам необходимо добавить файл TEST.adm в шаблоны групповых политик, для этого заходим в редактор локальной групповой политики (смотреть рисунок 3), выбираем «удаление или добавление шаблонов» и добавляем созданный файл TEST.adm (смотреть рисунок 4).

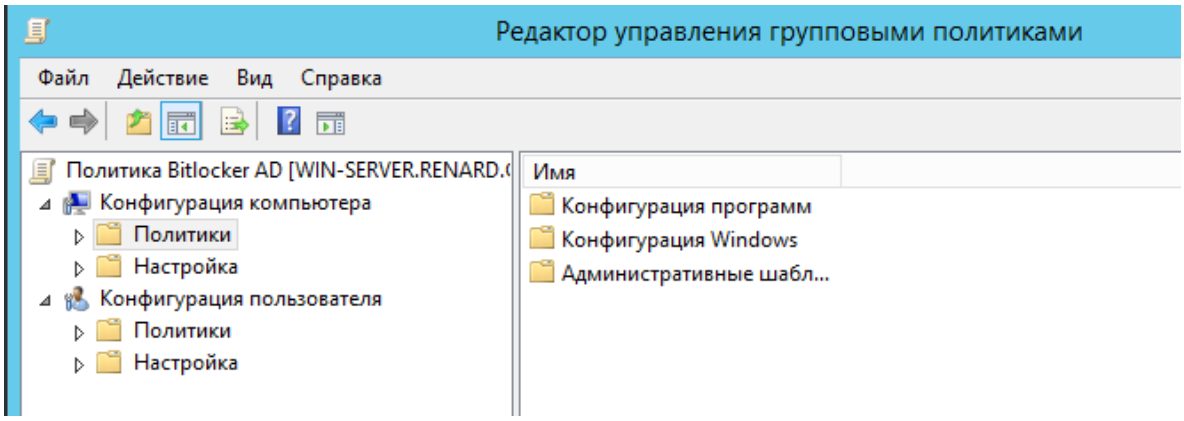


Рисунок 3 – Редактор локальной групповой политики

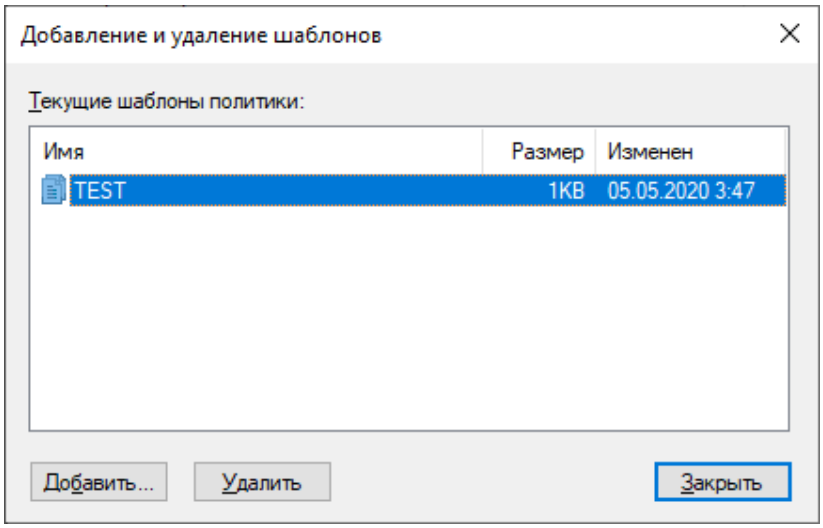


Рисунок 4 – Добавление файла в шаблоны групповых политик

Групповая политика находится по адресу Конфигурация компьютера\Административные шаблоны\SYSTEM\CorrentControlSet\RDP. Далее с контекстном меню выбираем «Изменить» и настраиваем групповую политику. Изменим значение порта на значение 3397, что представлено на рисунке 5.

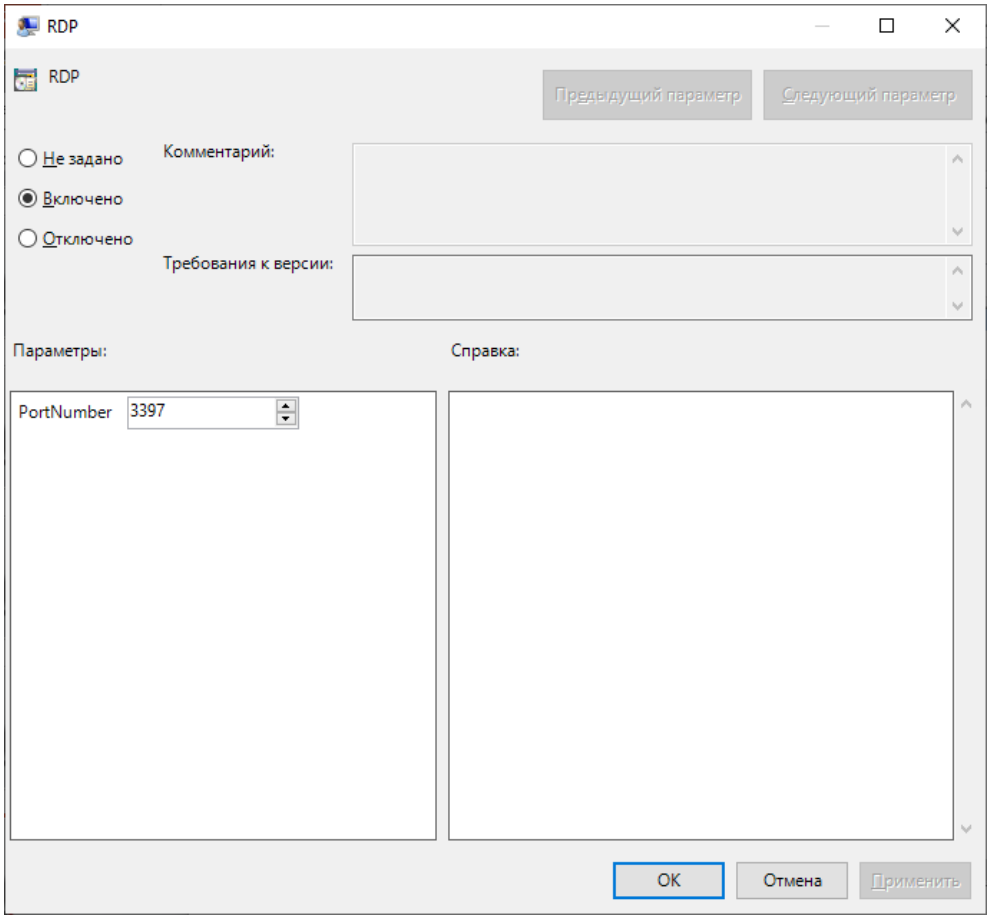


Рисунок 5 – Изменение значения RDP-порта

Для проверки выполнения групповой политики переходим в редактор реестра по адресу HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\ WinStations\RDP-Tcp. Как видно на рисунке 6, групповая политика отработала и изменила значение RDP-порта на значение 3397.

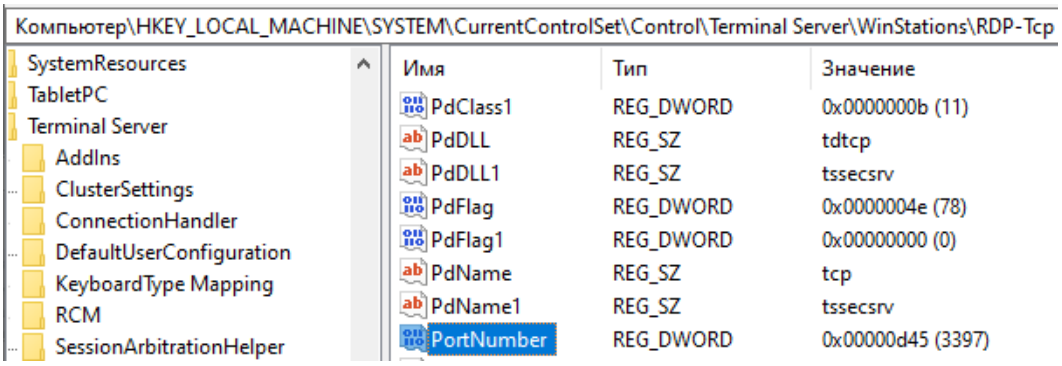


Рисунок 6 – Значение RDP-порта

Проверим IP-адрес клиента и попробуем подключиться через удаленный рабочий стол, что представлено на рисунках 7 и 8.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : Dlink
   Локальный IPv6-адрес канала . . . : fe80::593d:1a20:450e:80ac%4
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.10
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.1.1
```

Рисунок 7 – IP-адрес сервера

Как видно из рисунка 8 подключиться по стандартному порту, теперь для подключения через удаленный рабочий стол необходимо указать порт, на котором находится необходимый вам клиент, это выглядит так: 192.168.1.10:3397

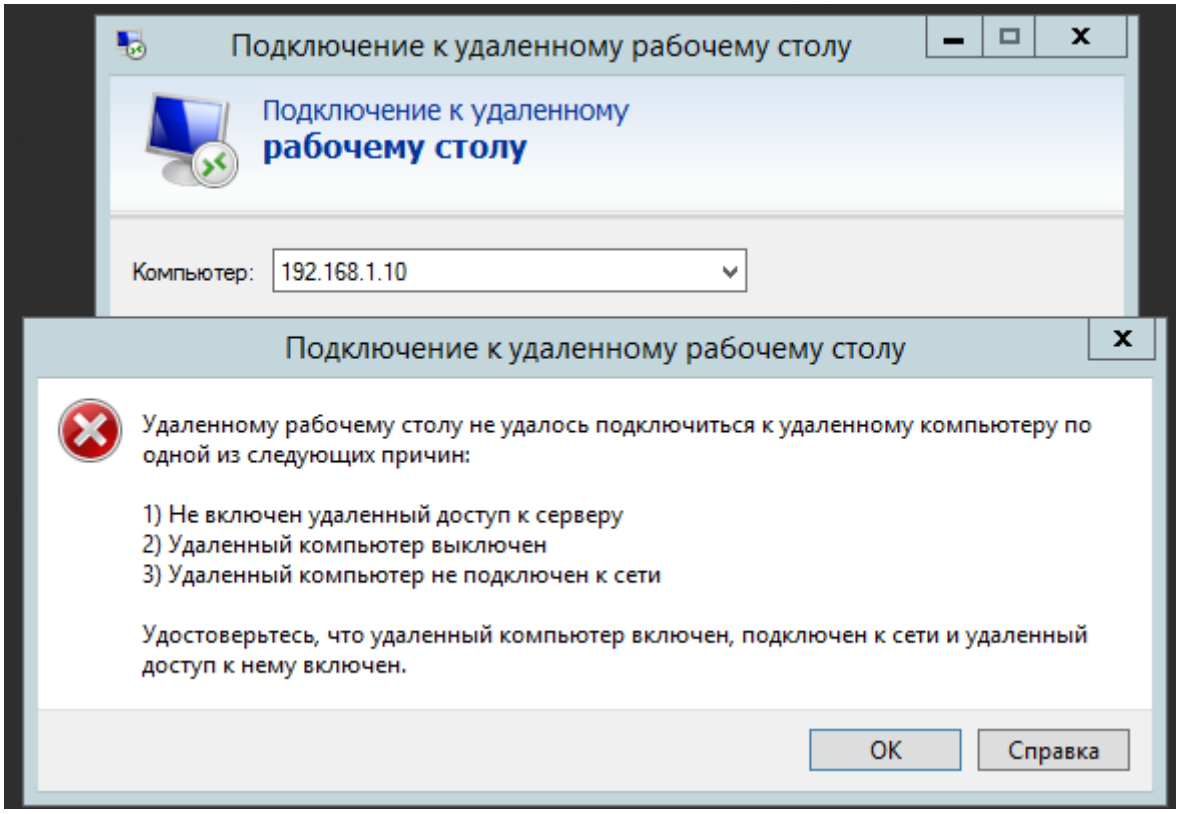


Рисунок 8 – Попытка подключение к клиенту

Так как никому кроме системного администратора домена не известны значения измененных RDP-портов, вероятность несанкционированного подключения значительно уменьшается.

2.3 Автоматизация процессов AD

В Active Directory достаточно много процессов которые можно автоматизировать. К примеру, в компании имеется политика хранения

документов, согласно которой документы, хранящиеся в памяти больше 3 месяце необходимо заносить в архив либо удалять. Искать вручную все документы, не соответствующие данной политике, очень сложный и долгий процесс. Для этого можно создать скрипт, который будет находить все документы по заданным параметрам и заносить все в отдельный документ. Данный скрипт представлен в приложении Б.

Для демонстрации работы скрипта выполним поиск документов в директории C:\supp0rt\, хранящихся в памяти больше 30 дней. Данный скрипт представлен на рисунке 9.

```
7
8   $path = "C:\supp0rt\"
9           $limit = (Get-Date).AddDays(-31)
10          Get-ChildItem $path -Recurse -Force | Where-Object { !$_.PSIsContainer -and $_.ModificationTime -lt $limit } |
11          Out-File c:\date.txt
```

Рисунок 9 – Пример скрипта

Далее на рисунке 10 представлена отработка скрипта. Так можно видеть, что скрипт не выдал никаких ошибок и записал результат в файл C:\date.txt, который представлен на рисунке 11.

```
PS C:\Users\Администратор\Desktop\scripts> $path = "C:\supp0rt\"
        $limit = (Get-Date).AddDays(-31)
        Get-ChildItem $path -Recurse -Force | Where-Object { !$_.PSIsContainer -and $_.ModificationTime -lt $limit } |
        Out-File c:\date.txt

PS C:\Users\Администратор\Desktop\scripts>
```

Рисунок 10 – Отработка скрипта

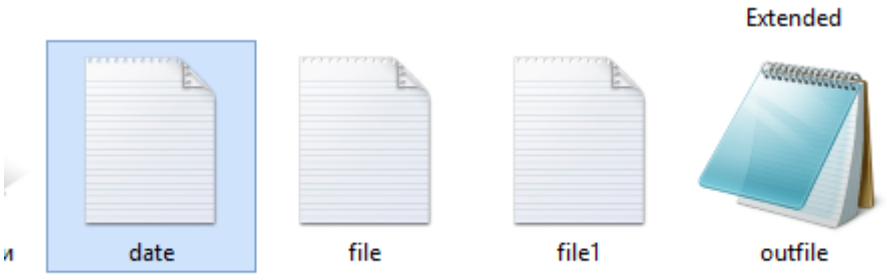


Рисунок 11 - Записанный файл с результатом

Как мы можем видеть на рисунке 12, скрипт нашел один документ sum.rtf, который был создан 05.05.20, т.е. больше 31 день назад. Скрипт работает без ошибок и отображает данные по документам правильно.

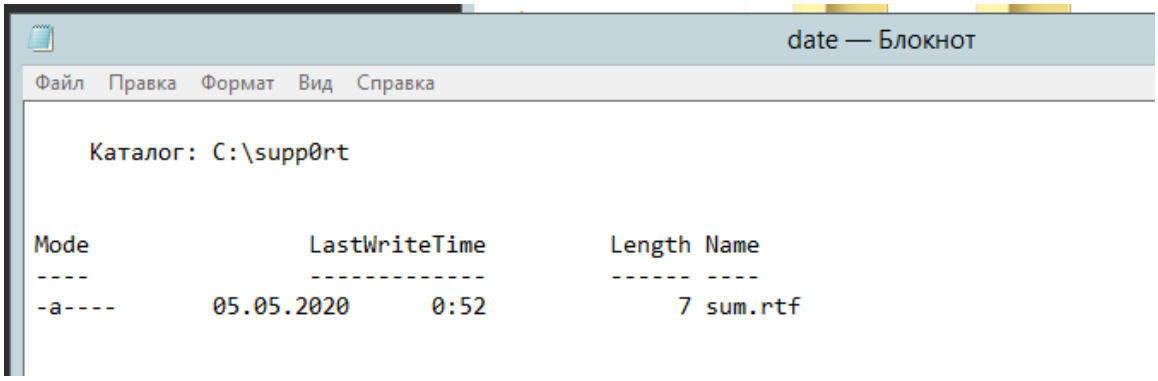


Рисунок 12 – Результат проверки

Бывают ситуации, в которых системному администратуру необходимо посмотреть информацию о пользователях в домене. Для автоматизации этого процесса был создан скрипт, который собиравает всю инфорацию о учетных записях пользователей домена и заносит их в файл (для удобства чтения результатов был выбран файл с расширением *.html). Пример отработки скрипта представлен на рисунке 13. Данный скрипт полностью представлен в приложении В.

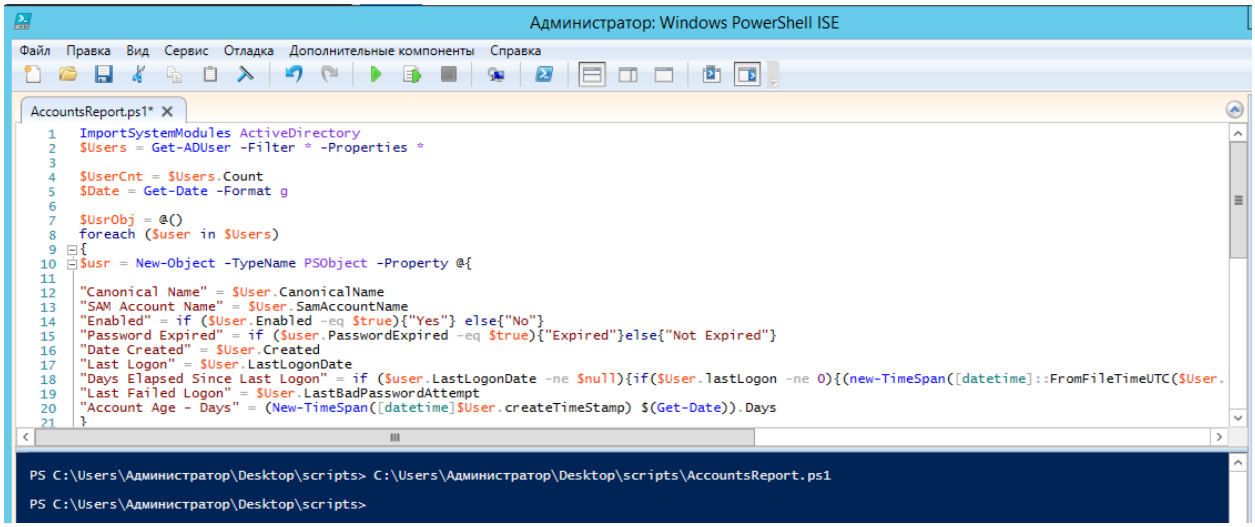


Рисунок 13 – Пример отработки скрипта

Данный скрипт собирает инфорацию по пользователям и зановит результаты в файл предствленный на рисунке 14.

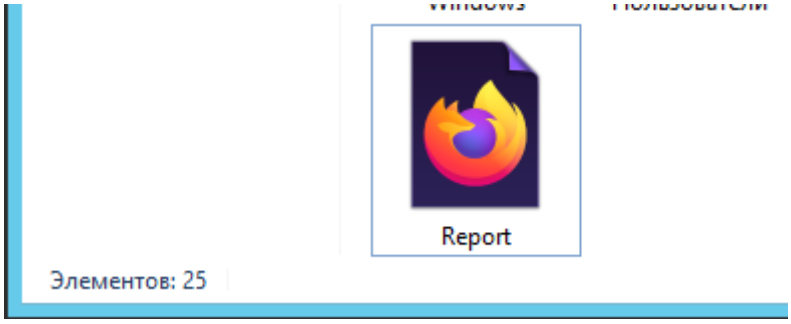
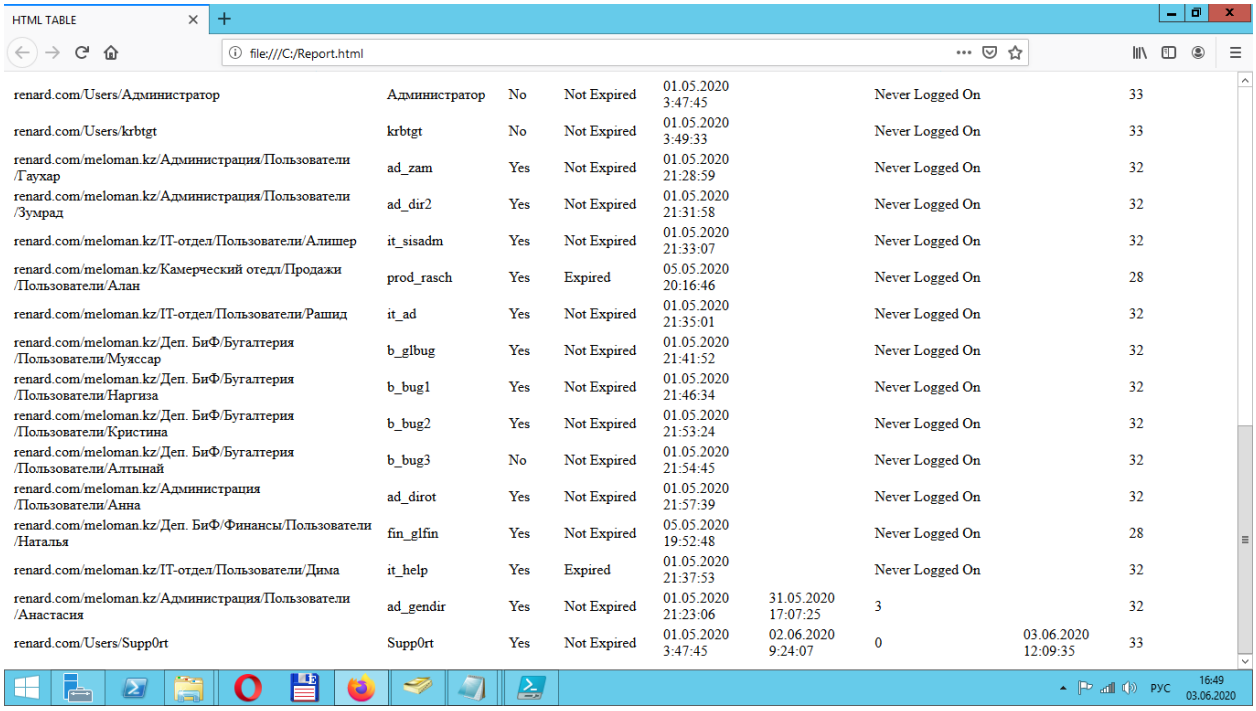


Рисунок 14 – Созданный файл

Как видно из рисунка 15, скрипт нашел: адрес хранения учетной записи, имя учетной записи, дату создания учетной записи, последние время входа и выхода учетной записи.



renard.com/Users/Администратор	Администратор	No	Not Expired	01.05.2020 3:47:45		Never Logged On	33
renard.com/Users/krbtgt	krbtgt	No	Not Expired	01.05.2020 3:49:33		Never Logged On	33
renard.com/meloman.kz/Администрация/Пользователи /Гаухар	ad_zam	Yes	Not Expired	01.05.2020 21:28:59		Never Logged On	32
renard.com/meloman.kz/Администрация/Пользователи /Зумрад	ad_dir2	Yes	Not Expired	01.05.2020 21:31:58		Never Logged On	32
renard.com/meloman.kz/IT-отдел/Пользователи/Алишер	it_sisadm	Yes	Not Expired	01.05.2020 21:33:07		Never Logged On	32
renard.com/meloman.kz/Камерческий отедл/Продажи /Пользователи/Алан	prod_rasch	Yes	Expired	05.05.2020 20:16:46		Never Logged On	28
renard.com/meloman.kz/IT-отдел/Пользователи/Рашид	it_ad	Yes	Not Expired	01.05.2020 21:35:01		Never Logged On	32
renard.com/meloman.kz/Деп. БиФ/Бугалтерия /Пользователи/Муясcар	b_glbug	Yes	Not Expired	01.05.2020 21:41:52		Never Logged On	32
renard.com/meloman.kz/Деп. БиФ/Бугалтерия /Пользователи/Наргиза	b_bug1	Yes	Not Expired	01.05.2020 21:46:34		Never Logged On	32
renard.com/meloman.kz/Деп. БиФ/Бугалтерия /Пользователи/Кристина	b_bug2	Yes	Not Expired	01.05.2020 21:53:24		Never Logged On	32
renard.com/meloman.kz/Деп. БиФ/Бугалтерия /Пользователи/Алтынай	b_bug3	No	Not Expired	01.05.2020 21:54:45		Never Logged On	32
renard.com/meloman.kz/Администрация /Пользователи/Анна	ad_dirot	Yes	Not Expired	01.05.2020 21:57:39		Never Logged On	32
renard.com/meloman.kz/Деп. БиФ/Финансы/Пользователи /Наталья	fin_glfin	Yes	Not Expired	05.05.2020 19:52:48		Never Logged On	28
renard.com/meloman.kz/IT-отдел/Пользователи/Дима	it_help	Yes	Expired	01.05.2020 21:37:53		Never Logged On	32
renard.com/meloman.kz/Администрация/Пользователи /Анастасия	ad_gendir	Yes	Not Expired	01.05.2020 21:23:06	31.05.2020 17:07:25	3	32
renard.com/Users/Supp0rt	Supp0rt	Yes	Not Expired	01.05.2020 3:47:45	02.06.2020 9:24:07	0	03.06.2020 12:09:35 33

Рисунок 15 – Результат отработки скрипта

С точки зрения безопасности в домене для учетных записей не должен назначаться вечный пароль. Для проверкиимеющихся пользователей с вечным паролем был создан скрипт, который ищет учетные записи по парамметрам пароля. Данный скрипт представлен в приложении Г. Пример отработки скрипта представлен на рисунке 16.

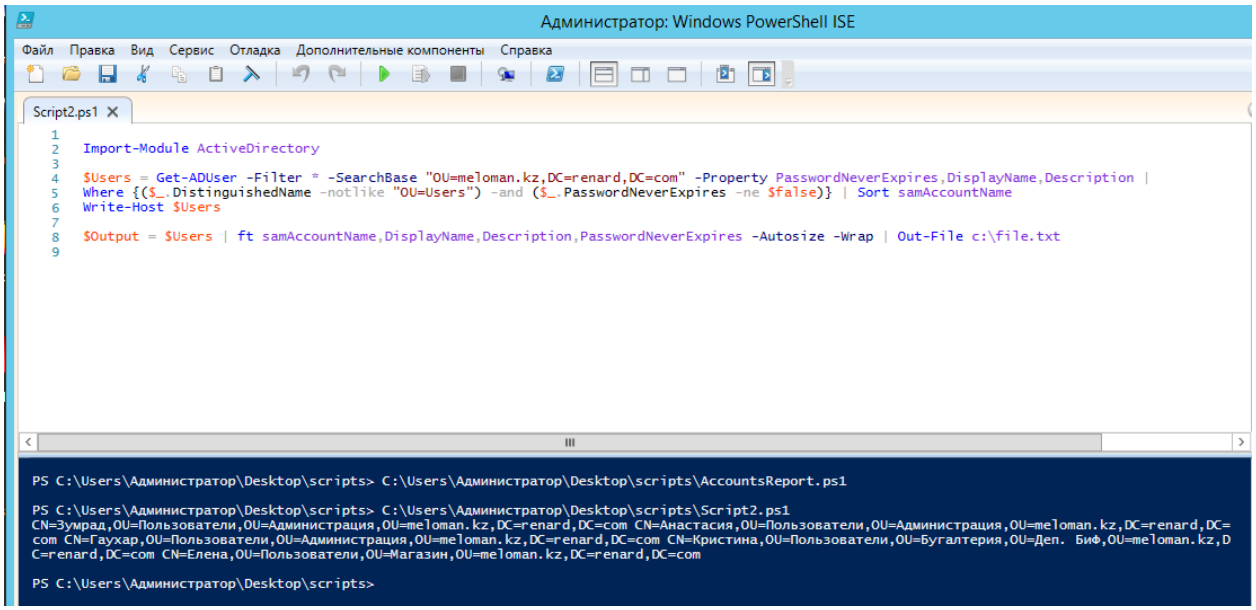


Рисунок 16 – Отработка скрипта

Как видно скрипт не выдал никаких ошибок, и записал результаты поиска в файл file.txt, представленный на рисунке 17.

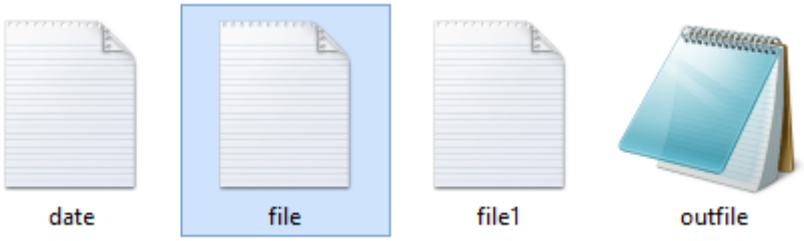


Рисунок 17 – Созданный файл

Как можно видеть на рисунке 18, скрипт нашел 5 пользователей имеющих вечный пароль.

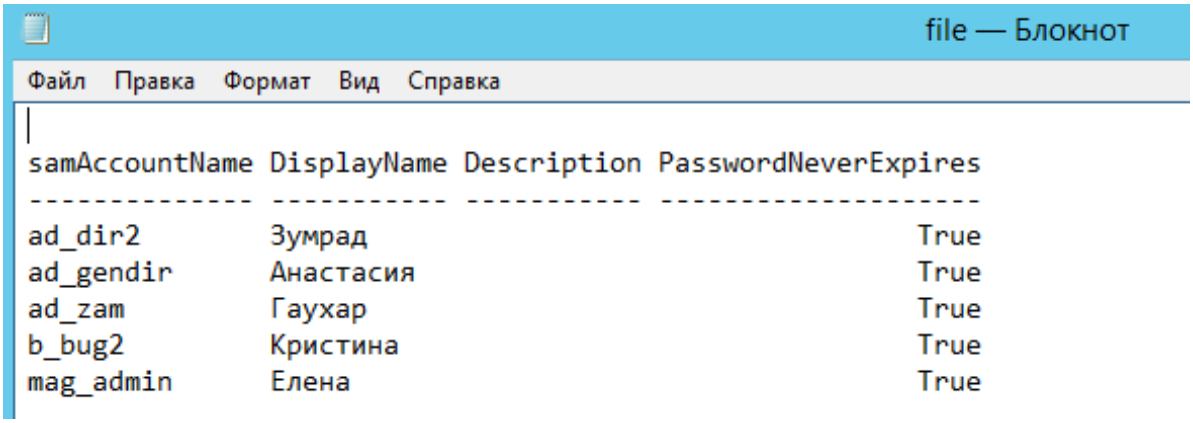


Рисунок 18 – Результат отработки скрипта

2.4 Проверка паролей домена

Уже не для кого не секрет, что парольная политика длины и сложности задаваемых паролей учетных записей пользователей не гарантирует создание серьезных затруднений злоумышленника для их подбора.

Нередко пользователи задают пароль по форме «Наименование организации + год» или «Наименование организации + год +месяц» или «Инициалы +специальный символ +год», в итоге получаем Gazprom2020, Lukoil052020, или RAD-2019.

С целью запрета использования таких паролей, рассмотрим утилиту Lithnet Password Protection for Active Directory (LPP) и настроить его с нуля.

Возможности решения предлагают использование базы хэшей скомпрометированных паролей haveibeenpwned.com.

Также в работе представлено создание собственного словаря.

На выбранном сервере DC AD установили утилиту LPP. При установке выбираем все компоненты, как можно видеть на рисунке 19 установщик содержит модуль PowerShell и шаблон групповой политики (ADMX).

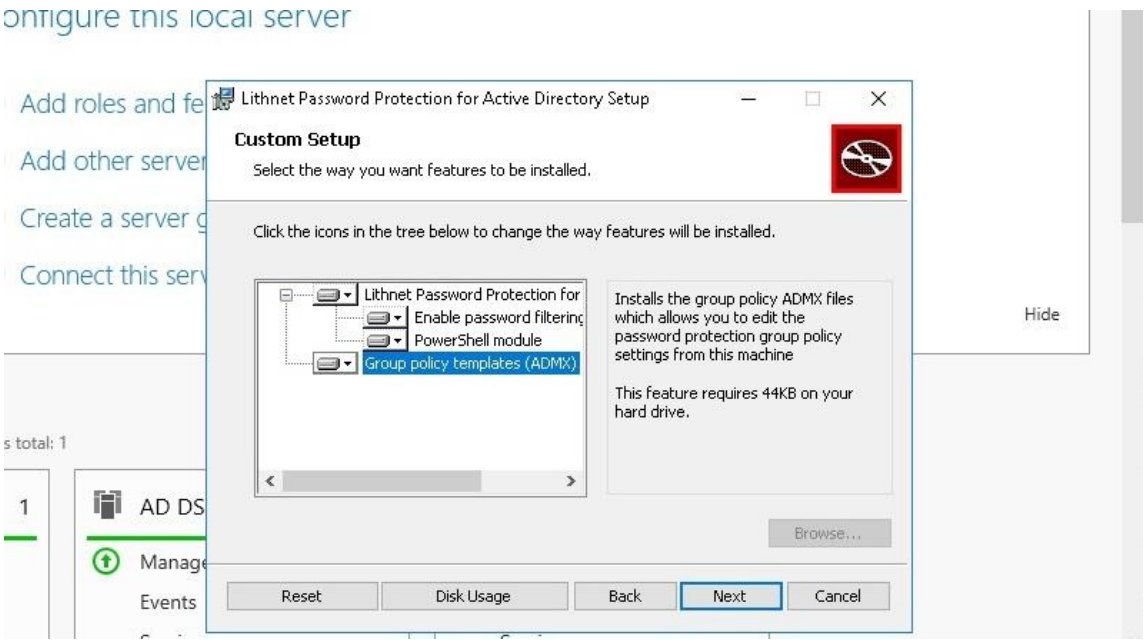


Рисунок 19 – Установка программы

Выбираем путь к папке где будет храниться базы скомпрометированных паролей или паролей по словарю, как представлено на рисунке 20.

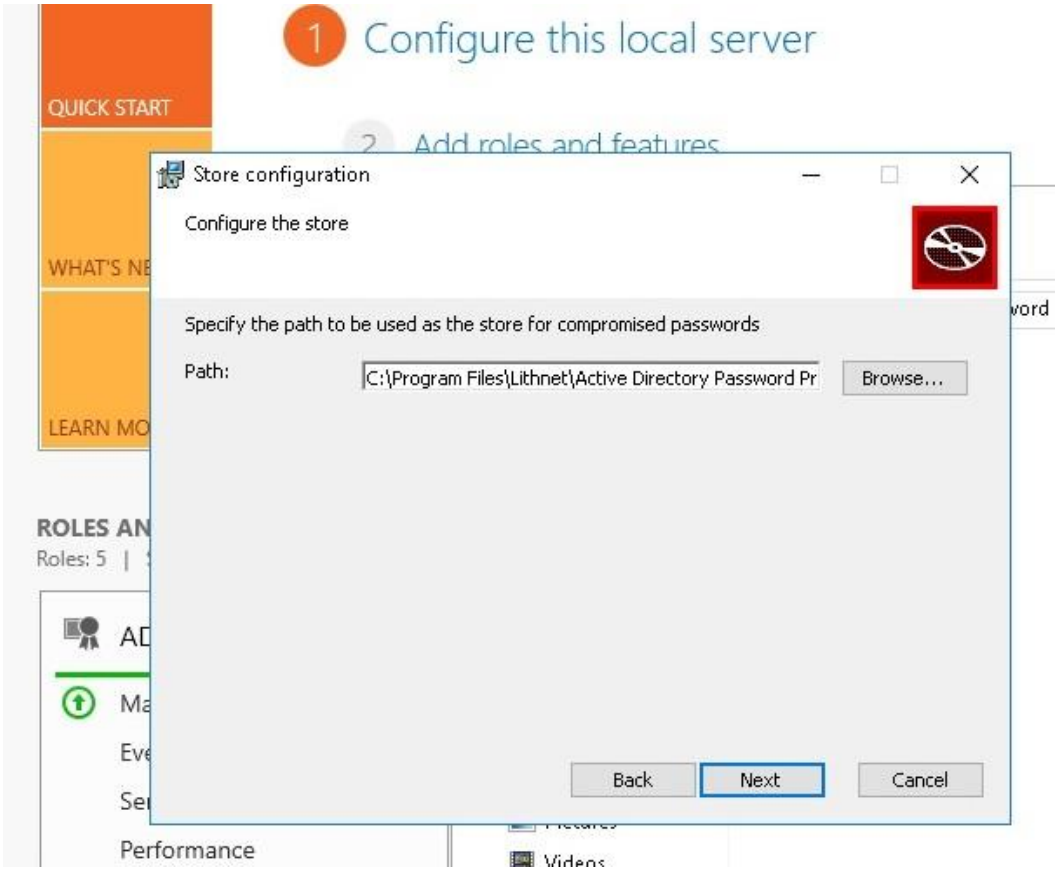


Рисунок 20 – путь к папке

На рисунке 21 представлена папка, в которой будут хранится база скомпрометированных паролей и созданный словарь паролей.

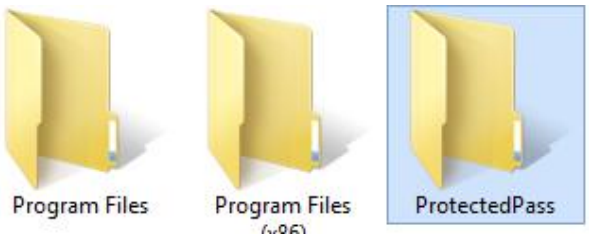


Рисунок 21 – папка с паролями

На рисунке 22 представлен файл скомпрометированных паролей. Размер файла 18 ГБ. Содержимое файла представлено на рисунке 23. Для демонстрации работы данной методики был создан свой словарь запрещенных паролей, что представлено на рисунке 24.

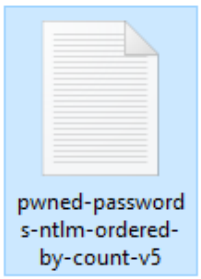


Рисунок 22 – файл с паролями

```
32ED87BDB5FDC5E9CBA88547376818D4:23547453
C22B315C040AE6E0EFEE3518D830362B:7799814
2D20D252A479F485CDF5E171D93985BF:3912816
8846F7EAEE8FB117AD06BDD830B7586C:3730471
2D7F1A5A61D3A96FB5159B5EEF17ADC6:3120735
259745CB123A52AA2E693AAACCA2DB52:2938594
F9E37E83B83C47A93C2F09F66408631B:2855057
328727B81CA05805A68EF26ACB252039:2512537
5835048CE94AD0564E29A924A03510EF:2413945
7A21990FCD3D759941E45C490F143D5F:2380800
8AF326AA4850225B75C592D4CE19CCF5:2250015
579110C49145015C47ECD267657D3174:2230508
3FA45A060BD2693AE4C05B601D05CA0C:1957995
B963C57010F218EDC2CC3C229B5E4D0F:1608627
7CE21F17C0AEE7FB9CEBA532D0546AD6:1289385
3E24DCEAD23468CE597D6883C576F657:1198045
0D757AD173D2FC249CE19364FD64C8EC:1098172
3DBDE697D71690A769204BEB12283678:1038635
F2477A144DFF4F216AB81F2AC3E3207D:987676
F7EB9C06FAFAA23C4BCF22BA6781C1E2:977231
69CBE3ACBC48A3A289E8CDB000C2B7A8:974581
4057B60B514C5402DDE3D29A1845C366:944954
AF27EFB60C7B238910EFE2A7E0676A39:925818
E8CD0E4A9E89EAB931DC5338FCBEC54A:888171
F67F5E3F66EFD7298BE6ACD32EEEB27C:772589
6920C58D0DF184D829189C44FAFB7ECE:740190
7CA5BEBEBE1CBC9298F508D5B4FE90CE:737102
E01A82730005ECA51033F231F14EE106:727480
AD70819C5BC807280974D80F45982011:723683
```

Рисунок 23 – Содержимое файла

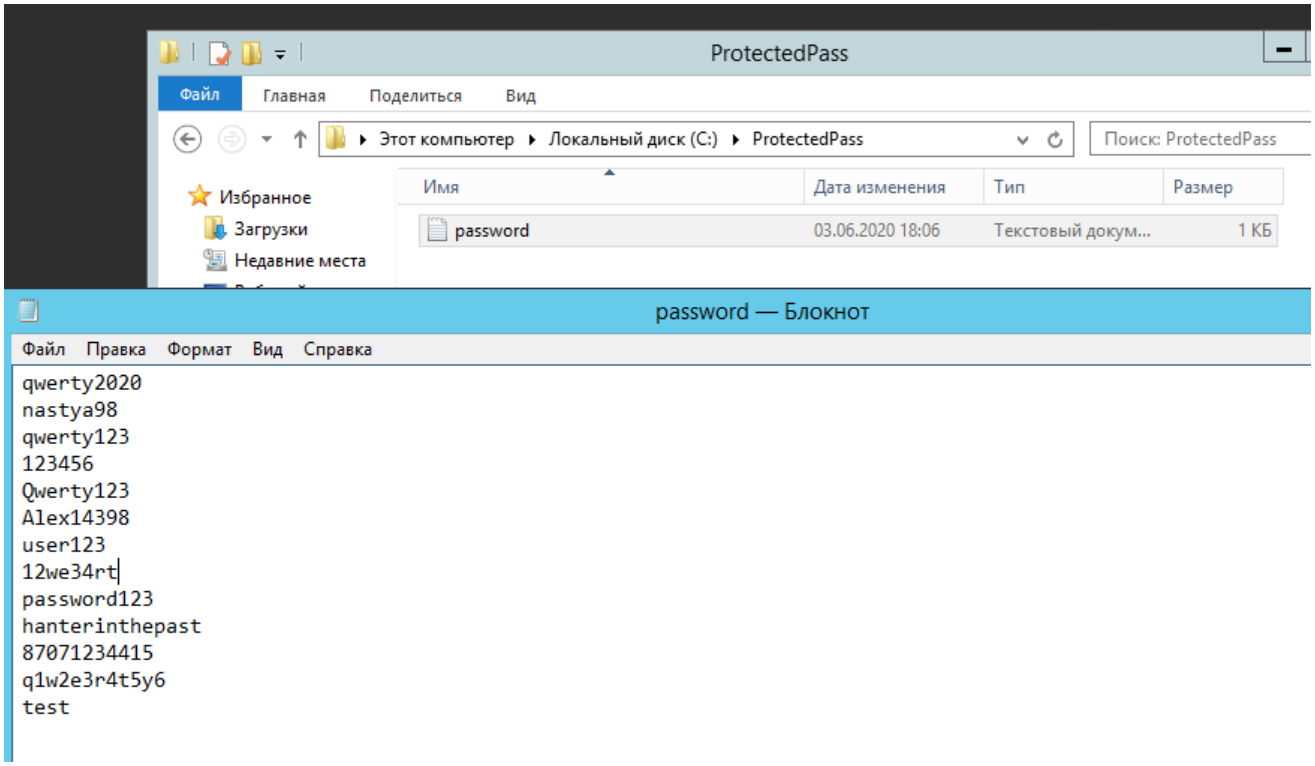


Рисунок 24 – файл с паролями

Далее с помощью PowerShell выполнен скрипт для занесения созданного словаря в базу утилиты LPP, что представлено на рисунке 25.

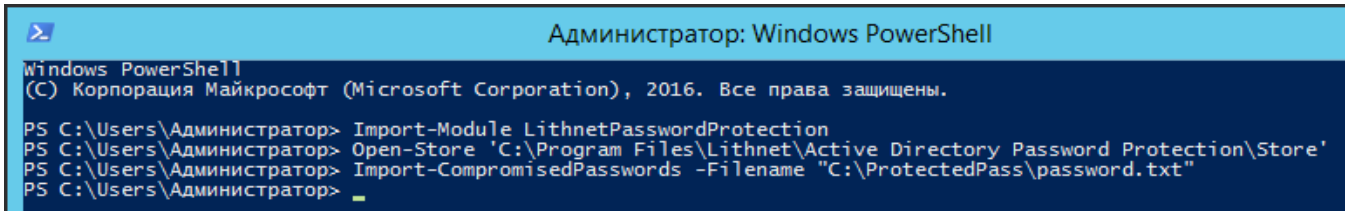


Рисунок 25 – Запуск скрипта

Для занесения в утилиту базы скомпрометированных паролей скрипт будет выглядеть следующим образом.

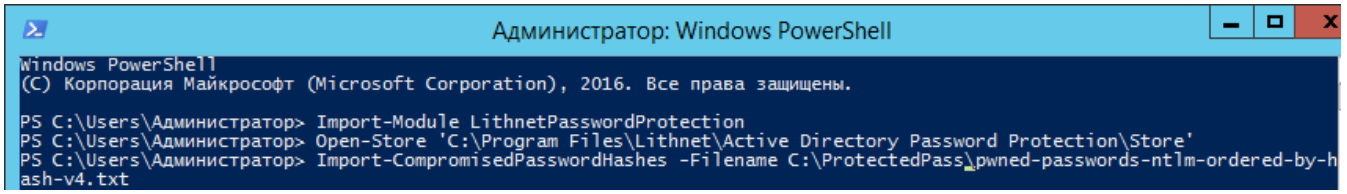


Рисунок 26 – Добавление скомпрометированных паролей

Далее была настроена политика группы, чтобы агент мог проверить пароли по базе конвертируемой базе хэшей.

Через оснастку MMC управления политикой группы и создано новое GPO и связанно с OU, в который находится ваш сервер. Задано имя политики pass, что представлено на рисунке 27.

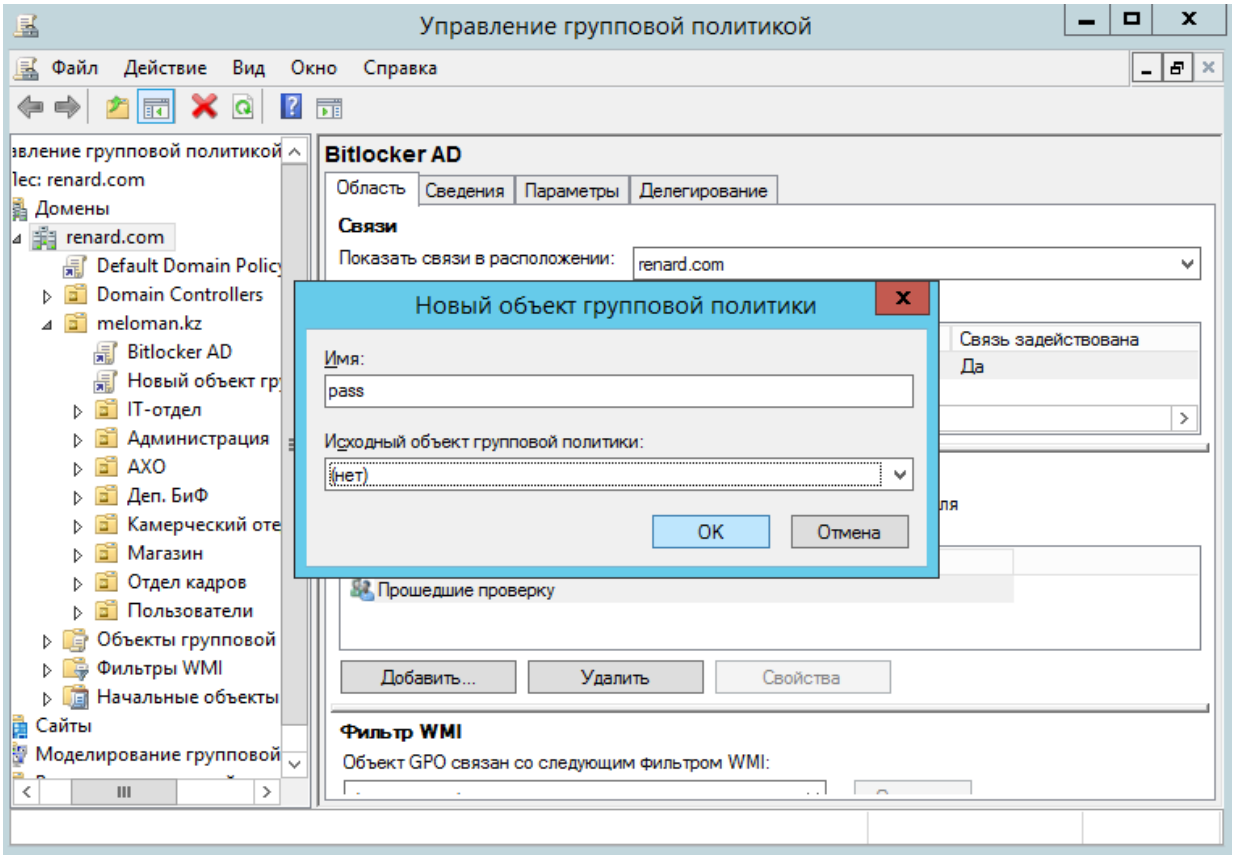


Рисунок 27 – Создание групповой политики

Необходимая политика хранится по адресу: Computer Configuration\Administrative Templates\Lithnet\Password Protection for Active Directory\Default Policy. Необходимая политика *Reject passwords found in the compromised password store, запущена*, а также настроены флажки на параметрах enable password set и password change operation, что представлено на рисунке 28.

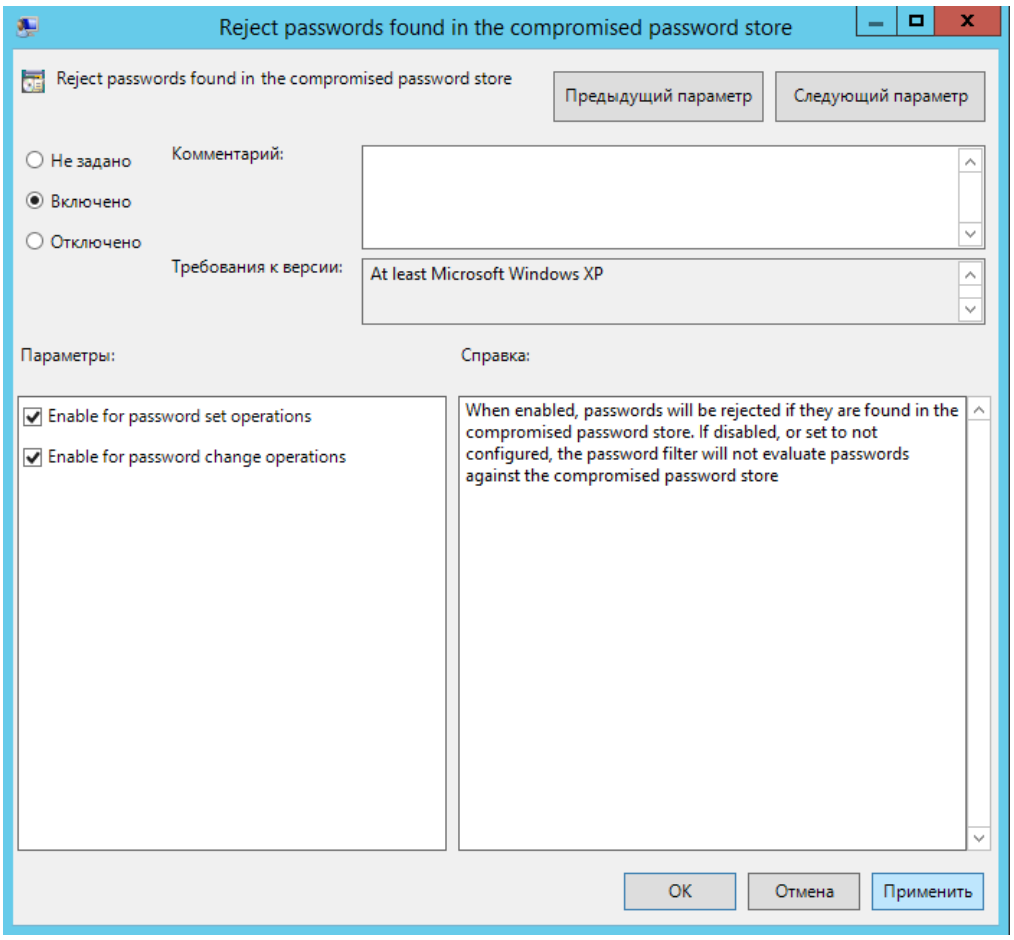


Рисунок 28 – Запуск групповой политики

Форсируется применение групповой политики в командной строке выполнив gpudpate /force (смотреть рисунок 29).

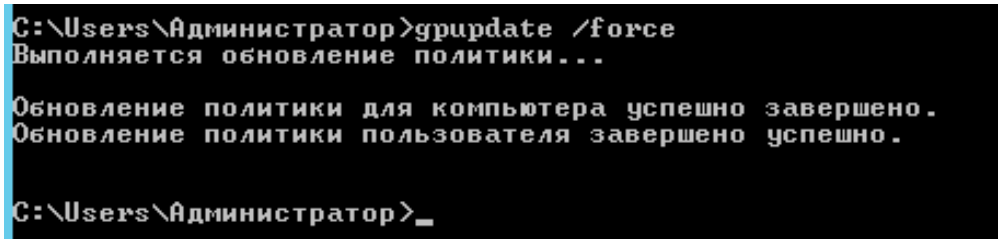


Рисунок 29 – Обновление ГП

Теперь политика активна. Для проверки работы групповой политики был выбран пользователей домена Вадим и проведена попытка смены пароля пользователя на Password123. Данные действия представлены на рисунке 30.

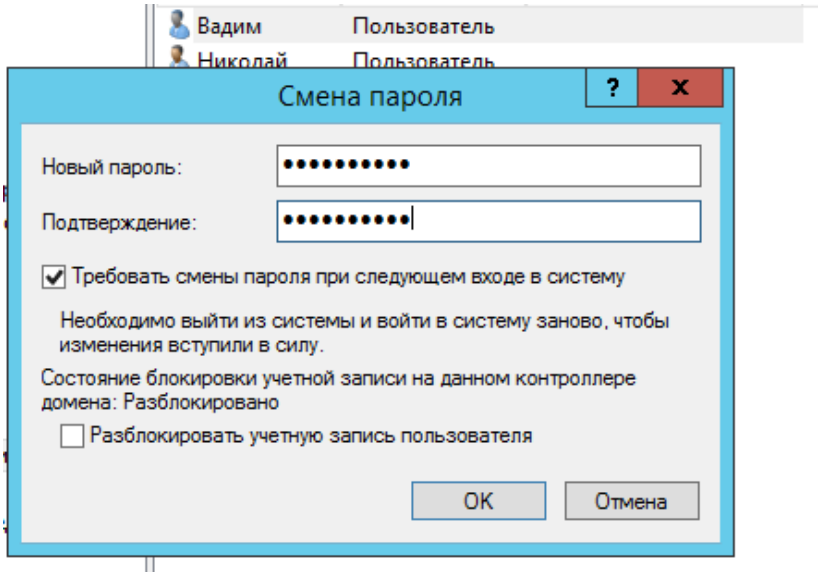


Рисунок 30 – задаем пароль пользователю

На рисунке 31 видно, что данный пароль не установился, от сюда следует что все настройки было произведены верно.

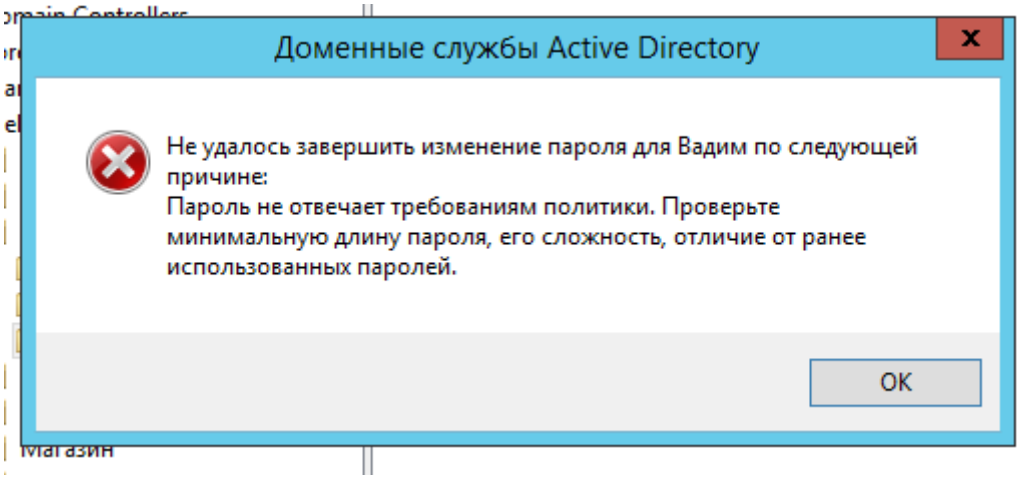


Рисунок 31 – Отработка настроек

2.5 Атаки направленные на получение хэшей паролей пользователей в AD

Первое, что должен сделать любой злоумышленник после того, как он закрепится в домене Active Directory - попытаться повысить уровень своего доступа. Удивительно как легко провести рекогносцировку домена с помощью PowerShell, и зачастую без каких-либо повышенных привилегий. В данном разделе представлено несколько различных способов использования PowerShell злоумышленниками для определения вашей среды и выбора целей.

Целью любого злоумышленника является компрометация члена администратора домена или администратора предприятия. На рисунке 32 представлен способ поиска администраторов.

Рисунок 32 – Команда поиска администраторов

После того, как злоумышленник установил точку опоры внутри вашего домена, его основная цель - как можно быстрее скомпрометировать свою цель без обнаружения. Злоумышленник может получить хэши паролей пользователей несколькими способами:

– украсть файл Ntds.dit;

– украсть хэши из дампа памяти Windows;

Файл Ntds.dit представляет собой базу данных, в которой хранятся данные Active Directory, включая информацию об объектах пользователя, группах и членстве в группах. Он включает хеши паролей для всех пользователей в домене.

Извлекая эти хэши, можно использовать такие инструменты, как Mimikatz, для выполнения атак с использованием хэша. После того как злоумышленник извлечет эти хэши, он сможет действовать как любой пользователь домена, включая администраторов домена.

Чтобы получить хеши паролей из Ntds.dit, первым шагом является получение копии файла. Это не так просто, как кажется, так как этот файл постоянно используется AD и заблокирован. Если вы попытаетесь просто скопировать файл, вы увидите сообщение об ошибке, представленной на рисунке 33.

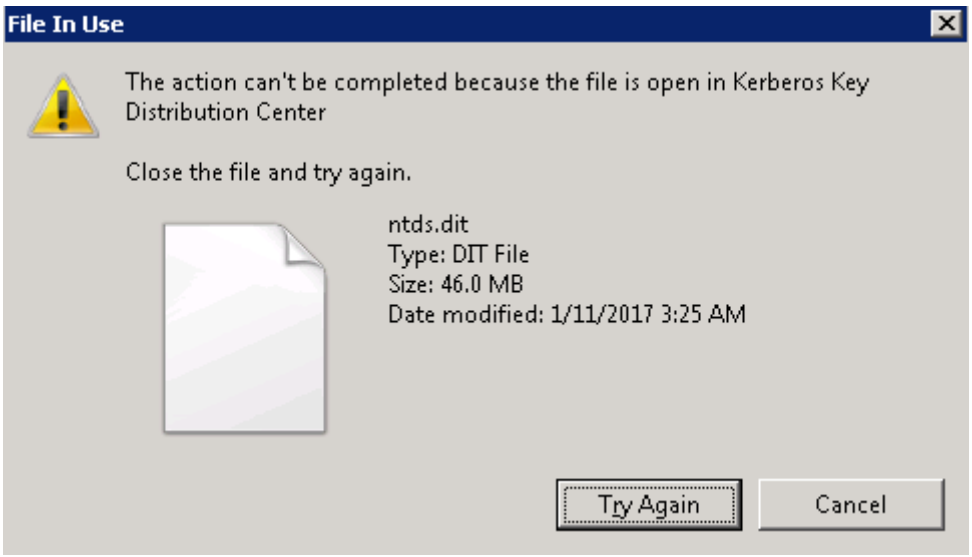


Рисунок 33 – Ошибка копирования файла

Есть несколько способов обойти это, используя возможности, встроенные в Windows, или с библиотеками PowerShell. Эти подходы включают в себя:

Использовать теневые копии томов с помощью команды VSSAdmin, данные действия представлены на рисунках 34-38.

Рисунок 34 – Создание теневого тома

Рисунок 35 - Получение файла Ntds.dit из теневой копии

Рисунок 36 - Перенос файла SYSTEM в реестр

Рисунок 37 - Копирование файла SYSTEM из реестра

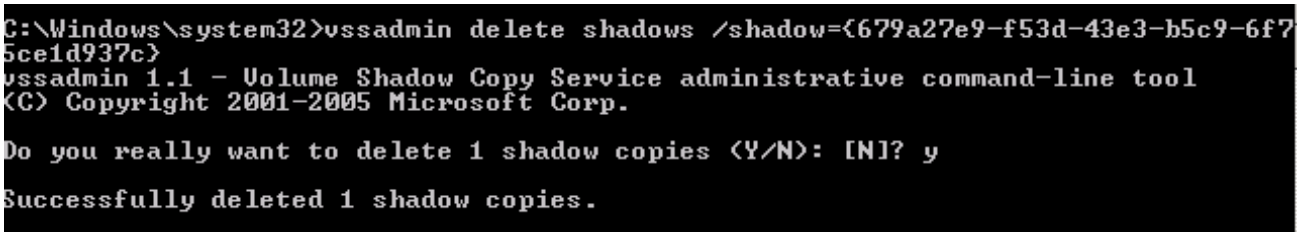


Рисунок 38 - Удаление треков из памяти

Далее на рисунке 39 можно видеть, что теперь можно запустить сеанс PSExec через Mimikatz и перечислить содержимое каталога NTDS контроллера домена, используя метод Pass-the-Hash.

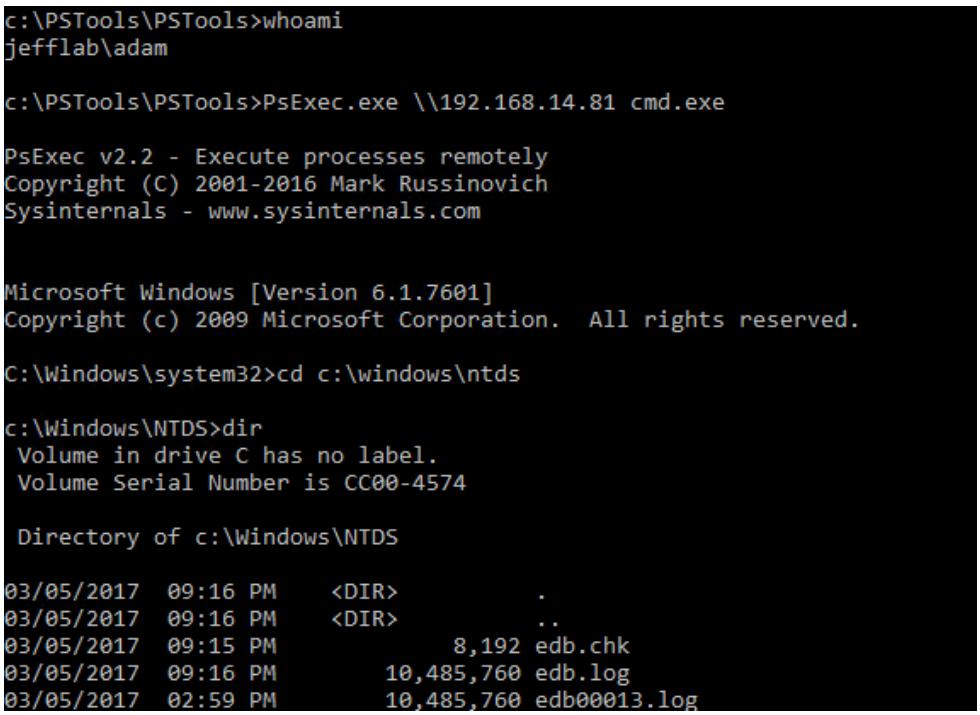


Рисунок 39 – Расшифровка файла Ntds.dit

Благодаря расшифровке файла Ntds.dit хэш пароля каждого пользователя находится под контролем, злоумышленник так же легко может выполнять действия от имени любого пользователя.

На рисунках 40-41 представлен способ извлечения хэшей паролей из дампа памяти Windows.

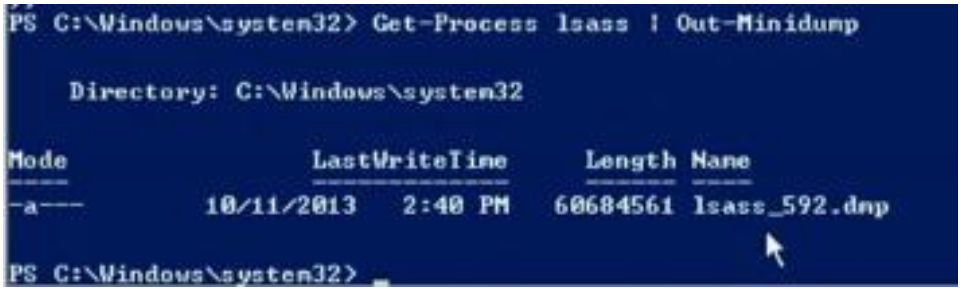


Рисунок 40 - Получившийся дамп памяти

Получившийся дамп памяти, это lsass_592.dmp, по умолчанию он сохраняется в каталоге %windir\system32%, необходимо скопировать его на другой компьютер, в которой имеется утилита mimikatz и выполнить команды представленные на рисунке 41.

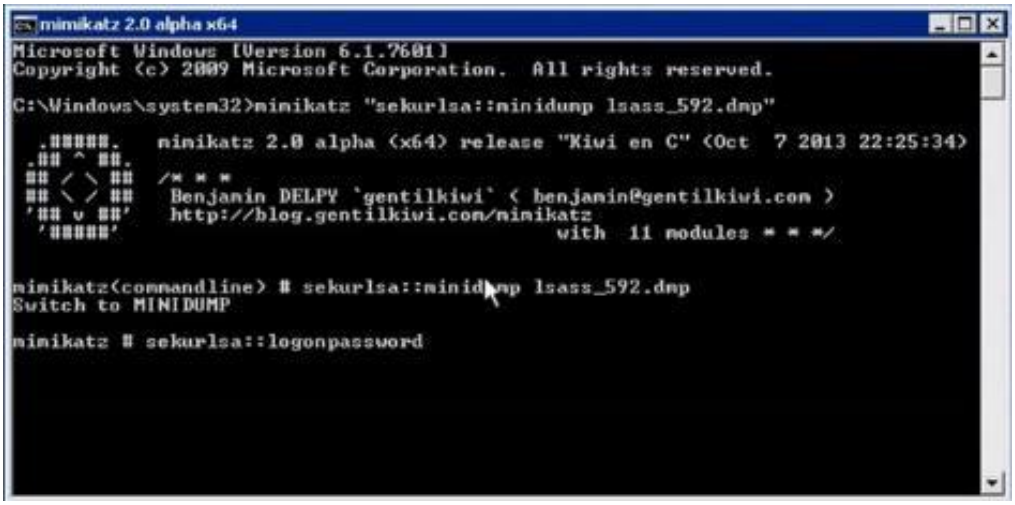


Рисунок 41 - Получение из сохранённого дампа памяти список пользователей, работающих в системе и их пароли

2.6 Защита на уровне сети

По умолчанию в Active Directory трафик по протоколу LDAP между контроллерами домена и клиентами не шифруется, т.е. данные по сети передаются в открытом виде. Потенциально это означает, что злоумышленник может прочитать эти данные как было описано в предыдущей главе.

Защитить данные, передаваемых по протоколу LDAP между клиентом и контроллером домена можно с помощью SSL версии протокола LDAP – LDAPS, который работает по порту 636. Для этого на контроллере домена необходимо установить специальный SSL сертификат.

Для этого для начала была установлена роль «Службы сертификатов Active Directory» на контроллере домена (смотреть рисунок 42).

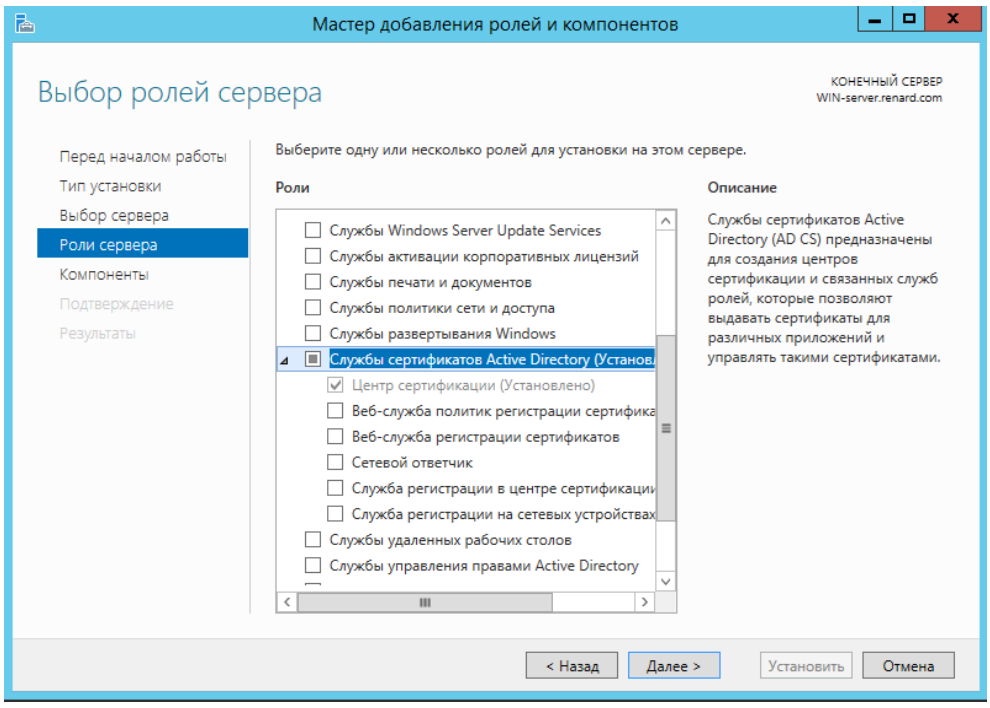


Рисунок 42 – Установка служб

Через консоль Certification Authority Management Console, необходимо выберать раздел шаблонов сертификатов и в контекстном меню выбрать Управление (смотреть рисунок 43).

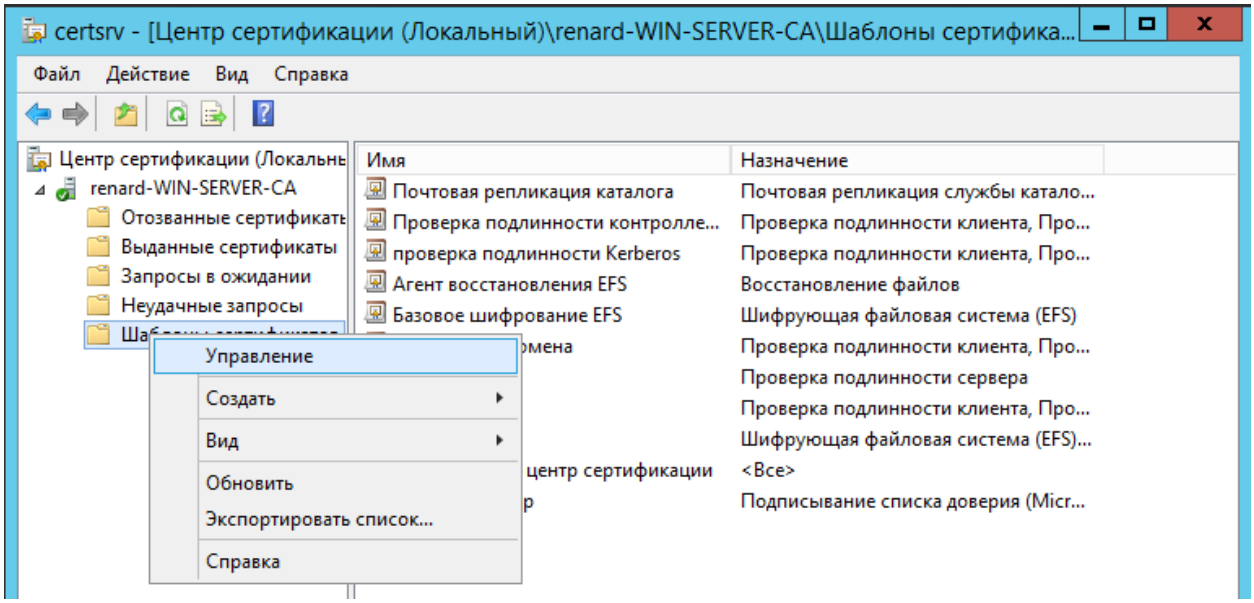


Рисунок 43 – Управление шаблонами сертификатов

На рисунке 44 представлен шаблон «проверка подлинности Kerberos» и создается его копия, выбрав в меню «Скопировать шаблон».

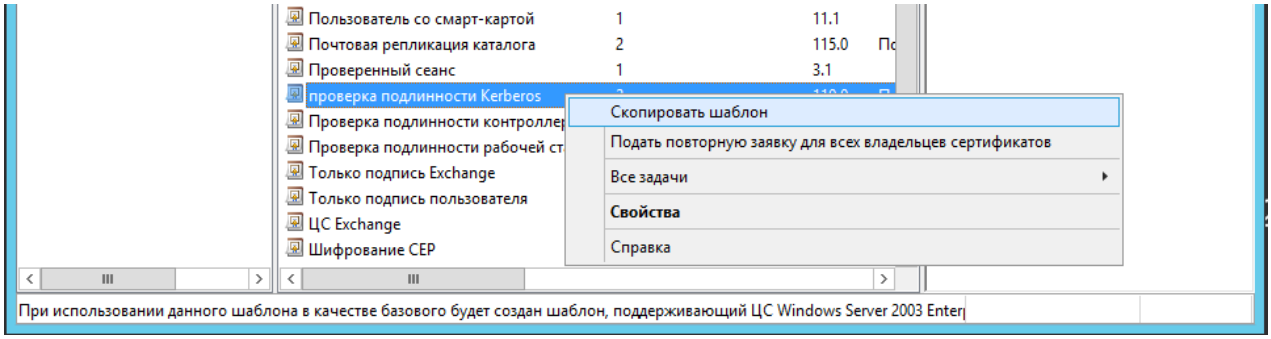


Рисунок 44 – Создание шаблона

На рисунке 45 видно, как во вкладке «Общие» переименовывается шаблон сертификата в LDAPoverSSL, указывается период его действия и его публикация в AD.

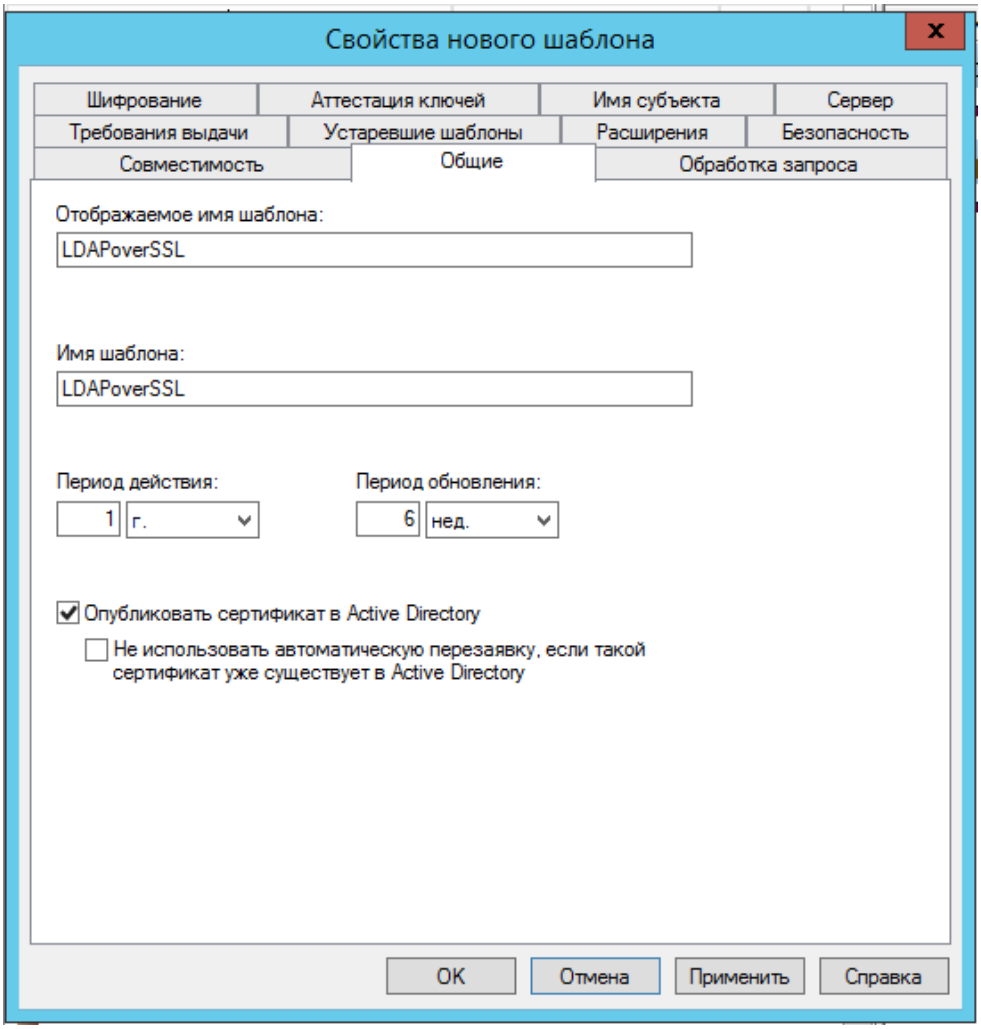


Рисунок 45 – Настройка шаблона

На рисунке 46 во вкладке «Обработка запроса» отмечается чекбокс у пункта «Разрешить экспортировать закрытый ключ» и сохраняется шаблон.

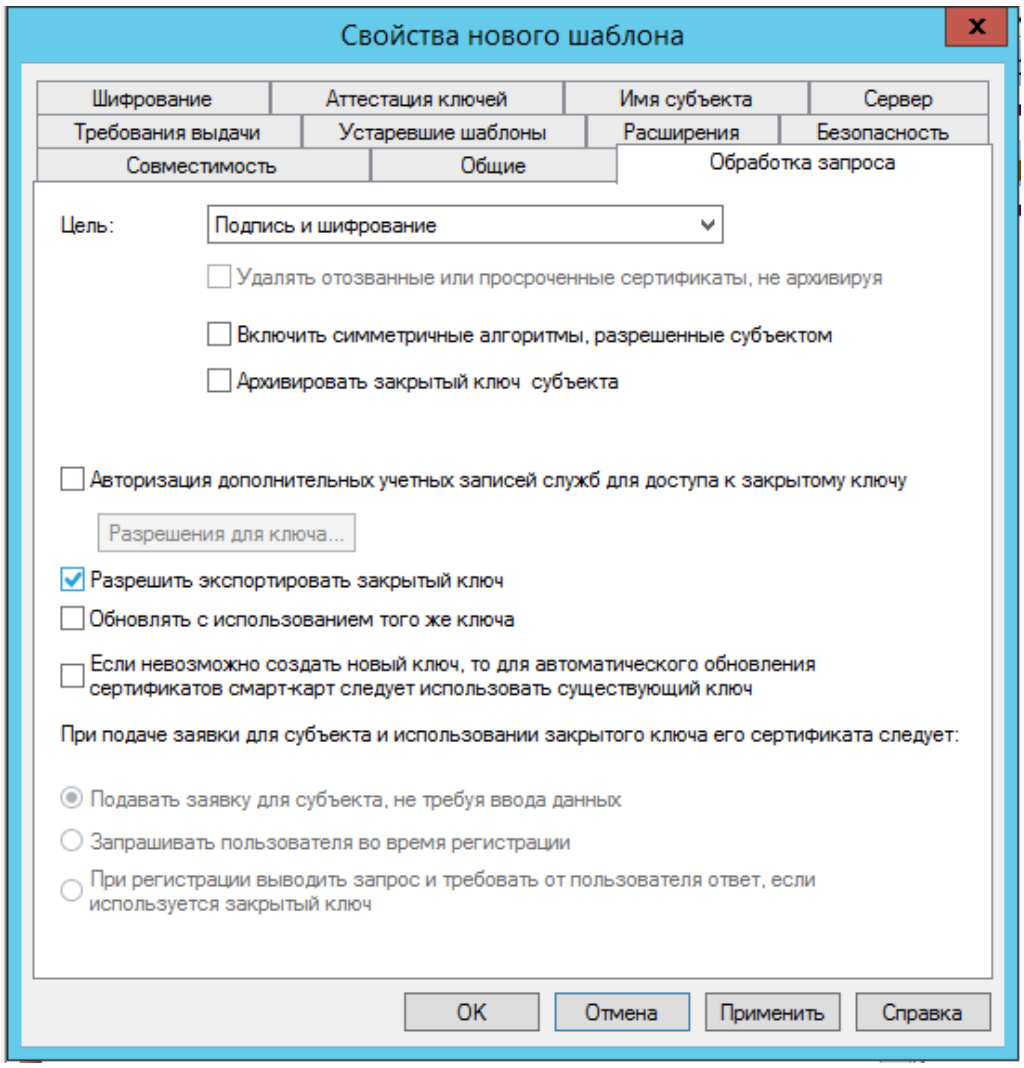


Рисунок 46 – Настройка обработки шаблона

На базе созданного шаблона, публикуется новый тип сертификата. Для этого, в контекстном меню раздела Шаблоны сертификата выбирается пункт Создать – Выдаваемый шаблон сертификата (смотреть рисунок 47).

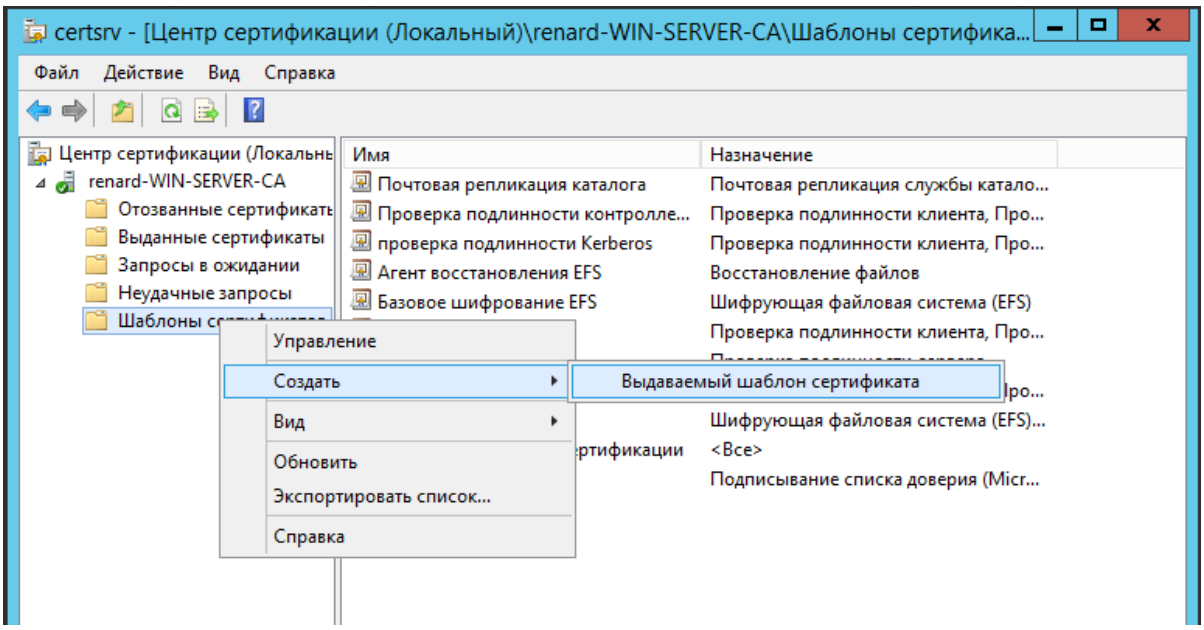


Рисунок 47 – Публикация нового сертификата

Из списка доступных шаблонов выбирается LDAPoverSSL (смотреть рисунок 48).

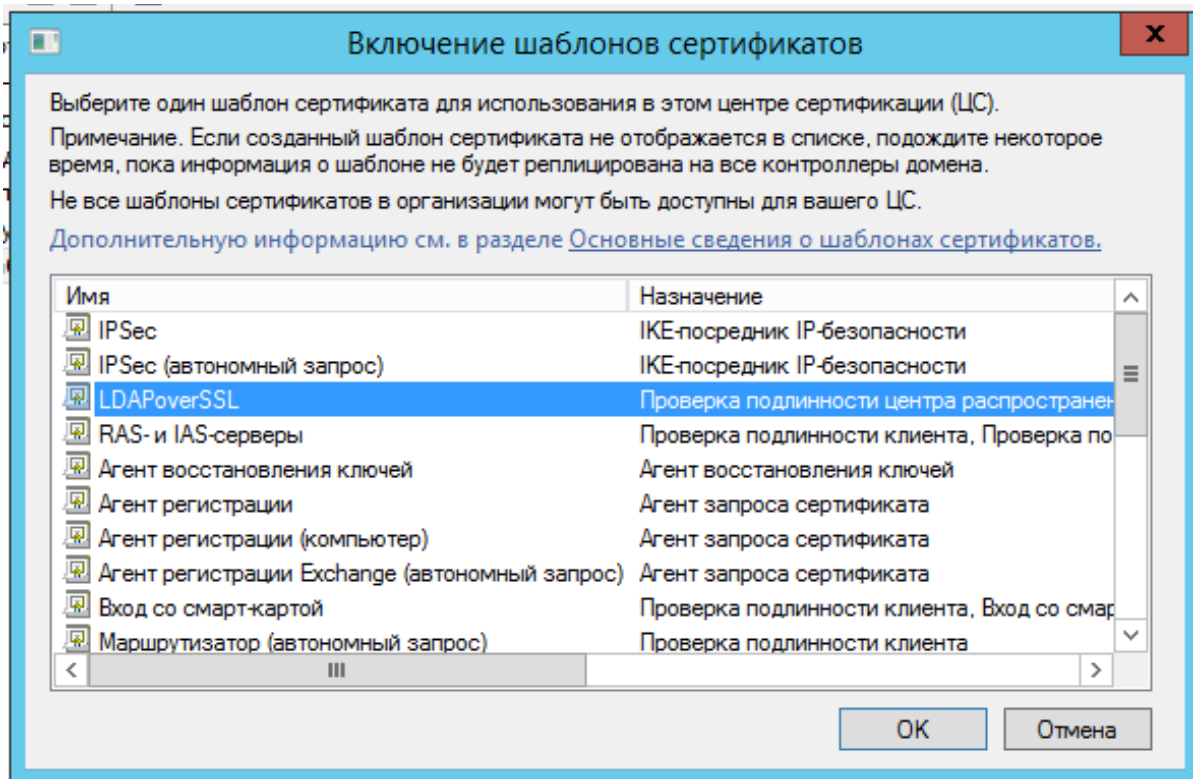


Рисунок 48 – Выбор созданного шаблона

На контроллере домена, для которого планируется задействовать LDAPS, открывается оснастка управления сертификатами и в хранилище сертификатов «Личные» запрашивается новый сертификат (Сертификаты- Все задачи- Запросить новый сертификат). В списке доступных сертификатов

выбирается сертификат LDAPoverSSL. Данные действия представлены на рисунках 49-52.

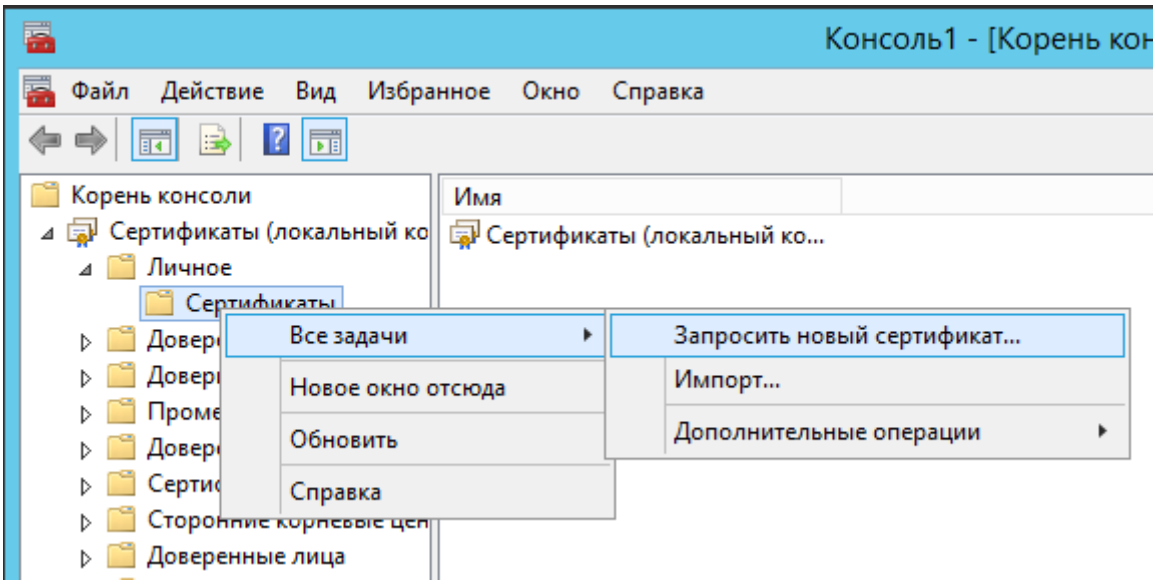


Рисунок 49 – Запрос нового сертификата

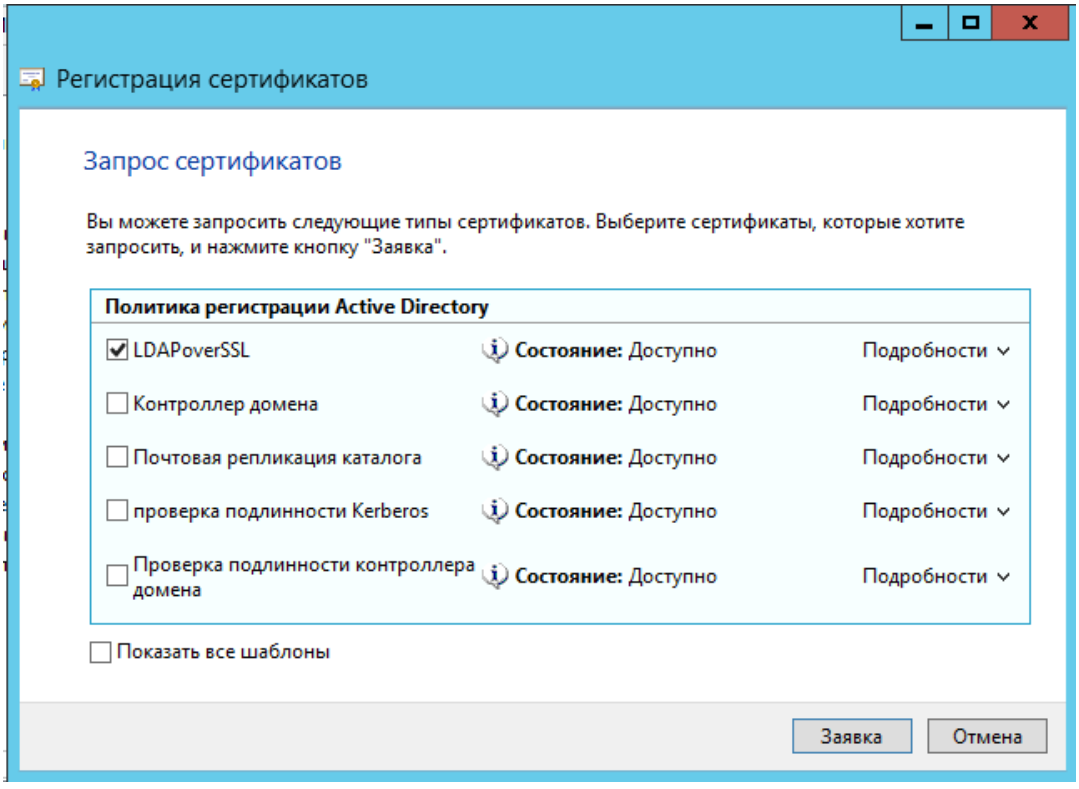


Рисунок 50 – Выбор сертификата LDAPoverSSL

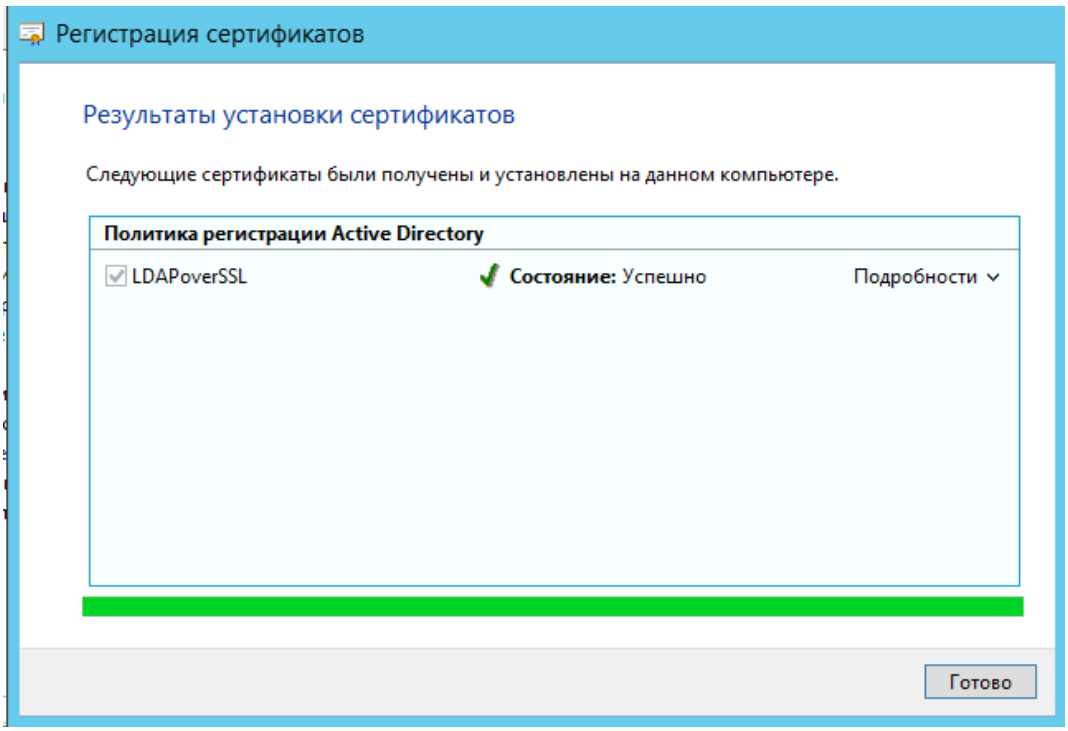


Рисунок 51 – Завершение установки сертификата

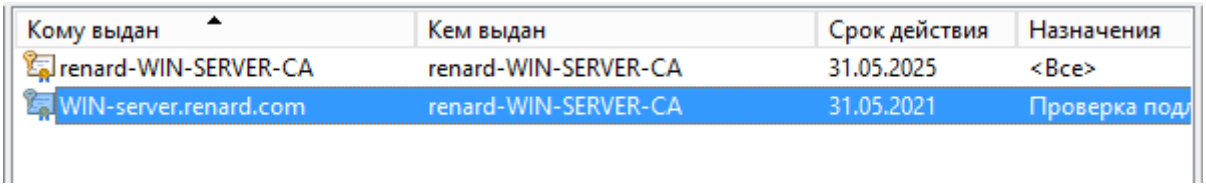


Рисунок 52 – Созданный сертификат

Следующее требование – необходимо, чтобы контроллер домена и клиенты, которые будут взаимодействовать через LDAPS доверяли удостоверяющему центру (CA), который выдал сертификат для контроллера домена. Для этого на контроллере домена выполняем команду, представленную на рисунке 53.

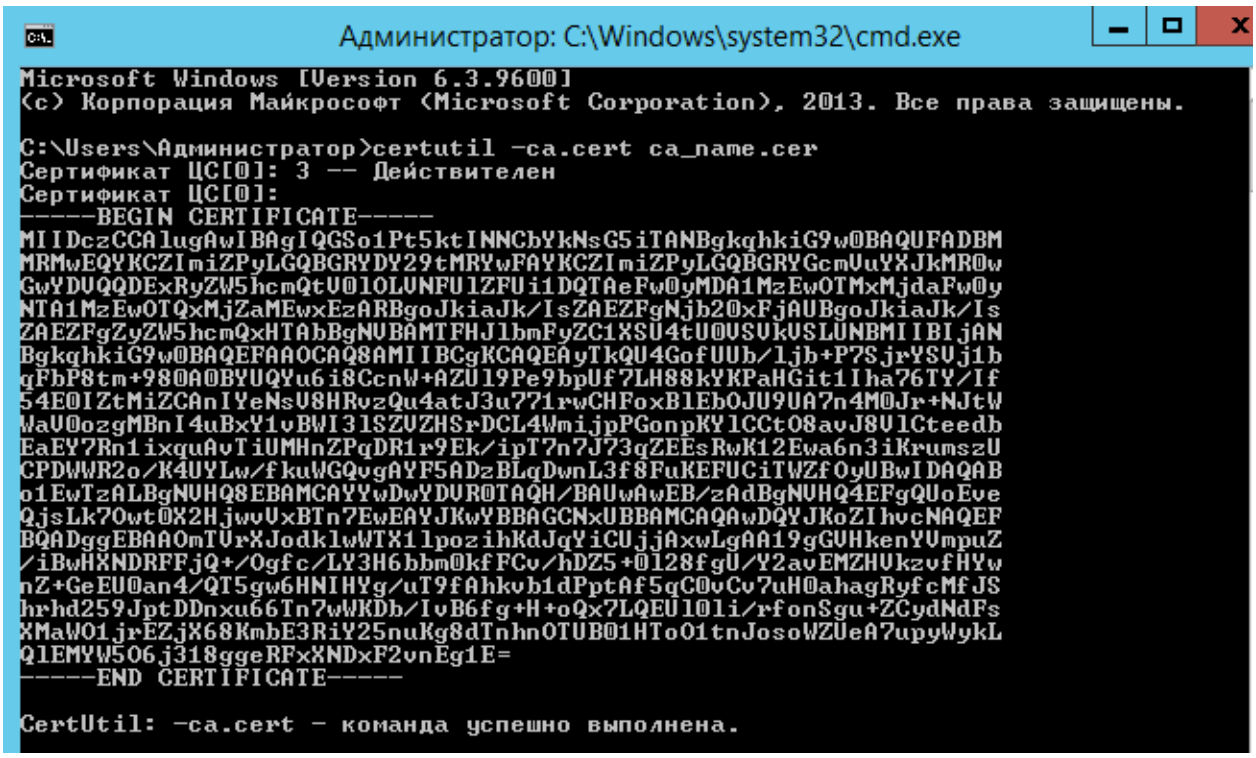


Рисунок 53 - Экспорт корневого сертификата удостоверяющего центра в файл

А затем экспортированный сертификат добавляется в хранилища сертификатов «Доверенные корневые центры сертификации» и «Доверенные издатели» на клиенте и контроллере домена. Данные действия представлены на рисунках 54-58.

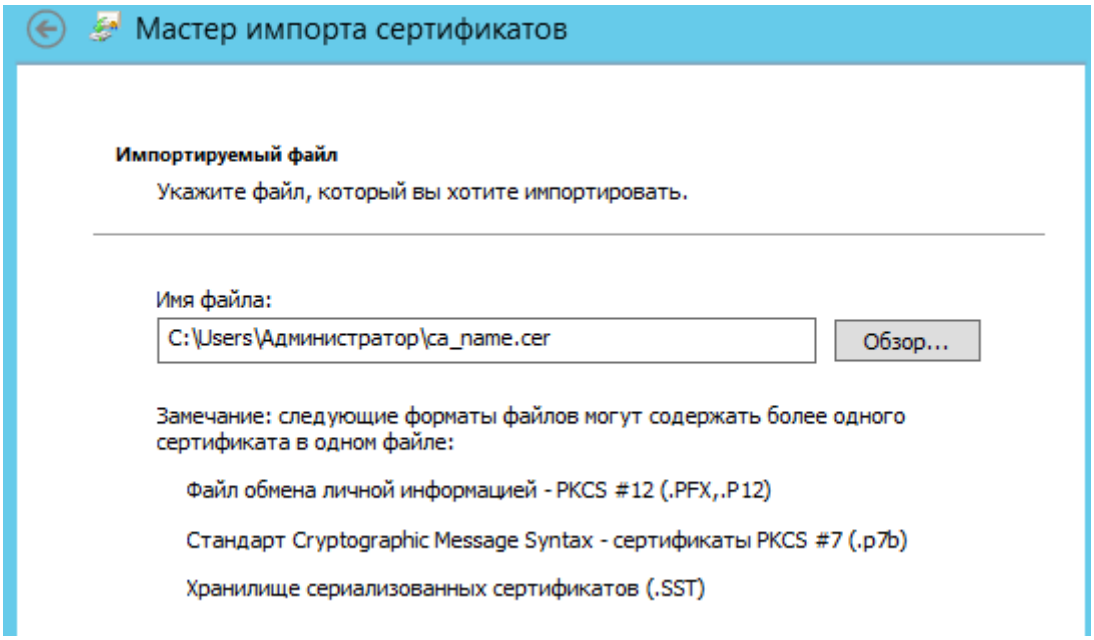


Рисунок 54 –Выбор сертификата

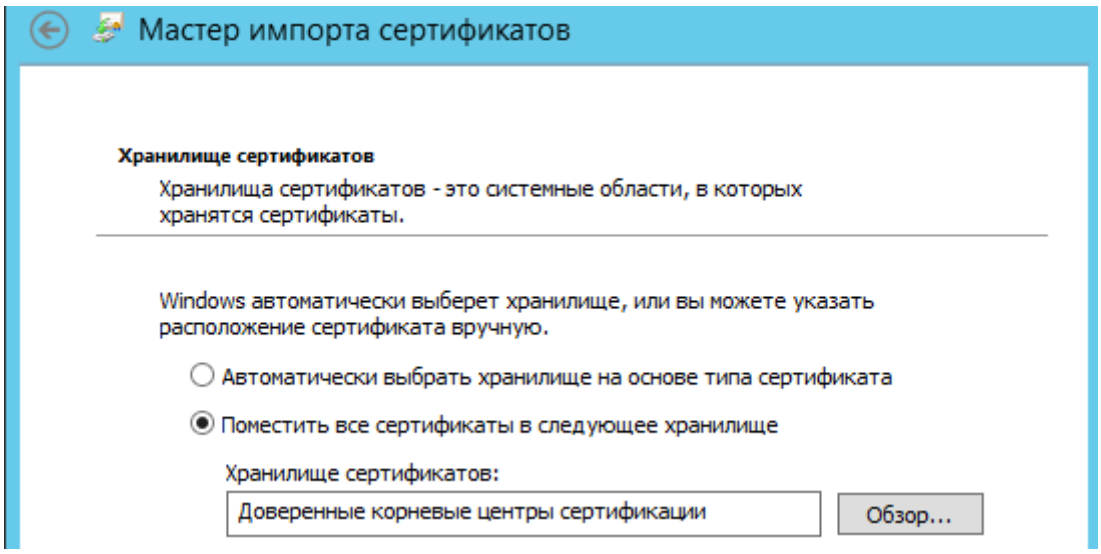


Рисунок 55 – Выбор хранилища

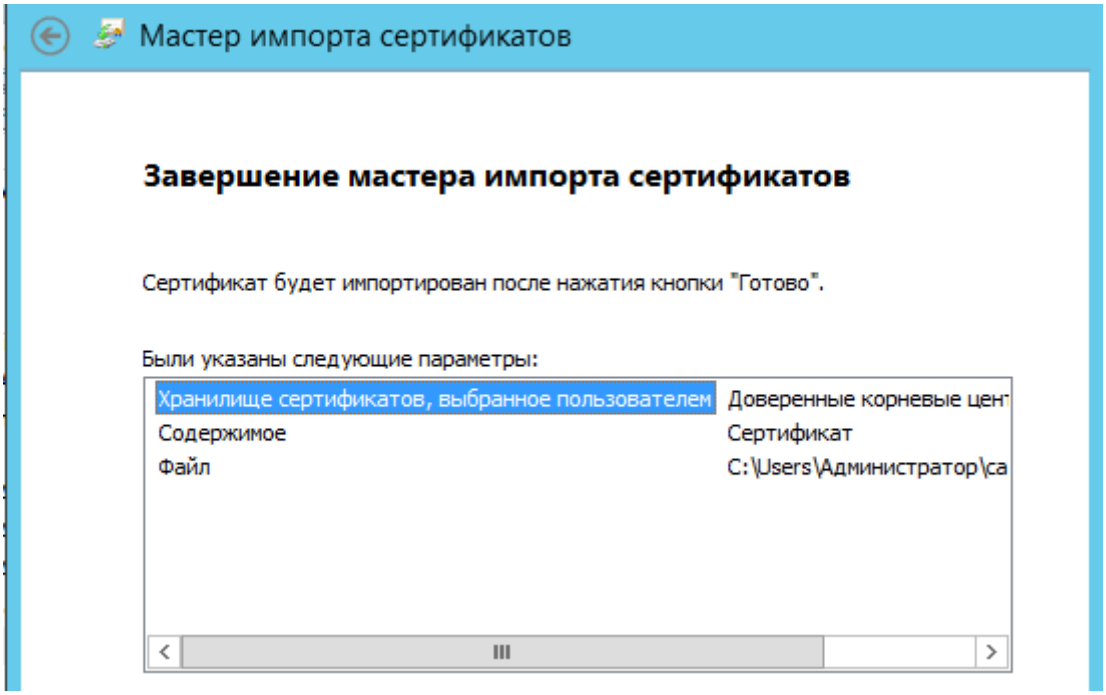


Рисунок 56 – Сохранение сертификата в хранилище

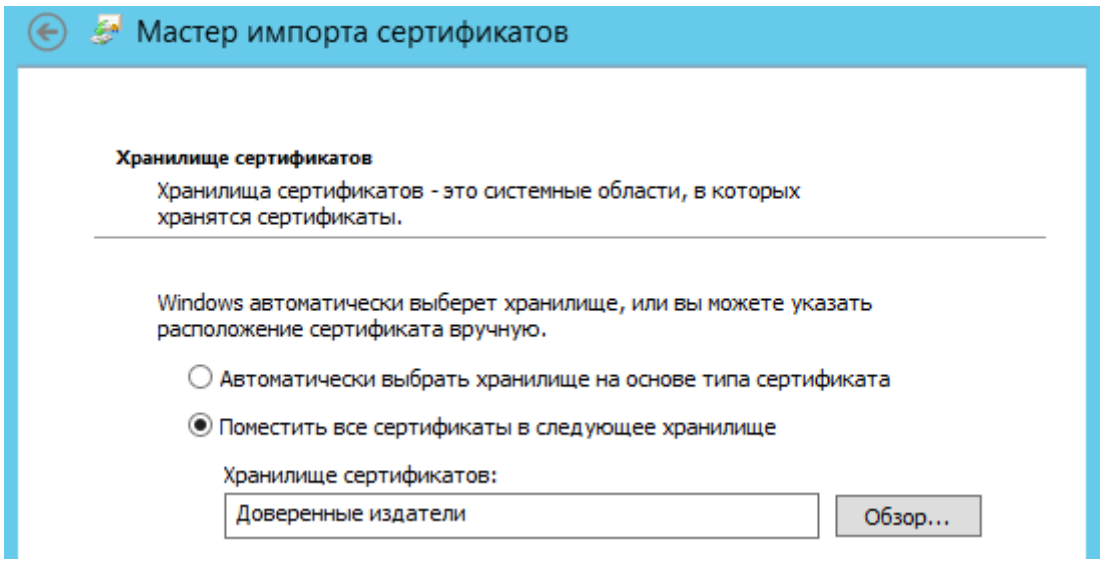


Рисунок 57 – Выбор второго хранилища

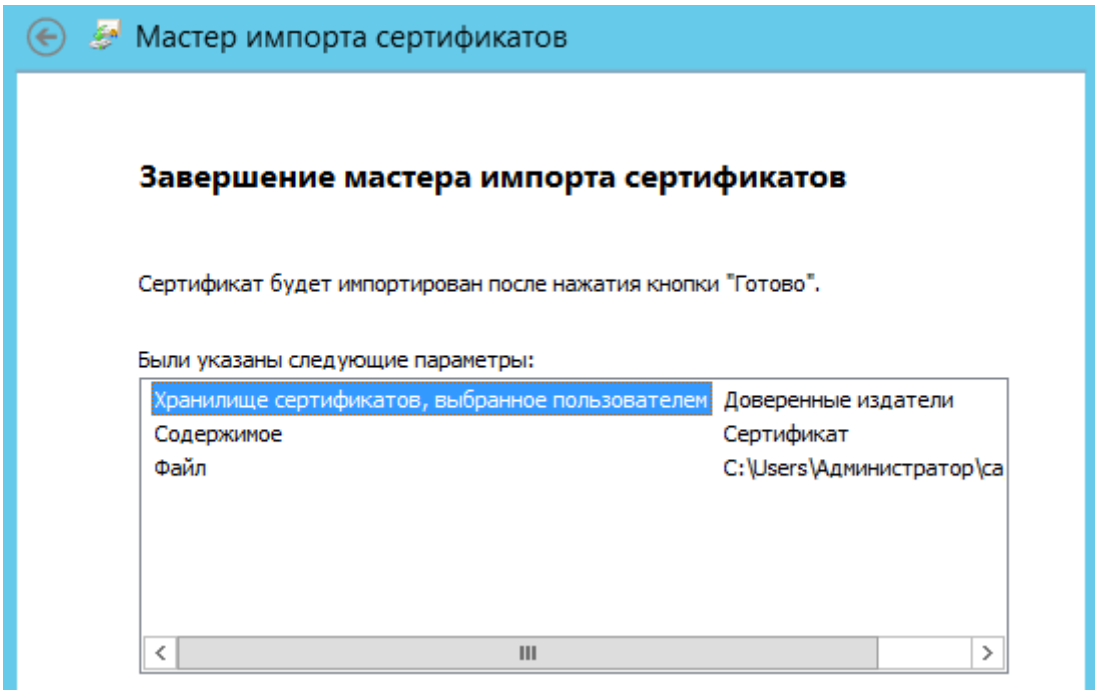


Рисунок 58 – Сохранение сертификата во второе хранилище

Осталось протестировать работу по LDAPS. Для этого на клиенте запускается утилита ldp.exe и в меню выбирается Подключение – Подключить- Указывается полное имя контроллера домена, выбирается порт 636 и отмечается SSL (смотреть рисунок 59). Как видно из рисунка 60 все сделано правильно, подключение было установлено.

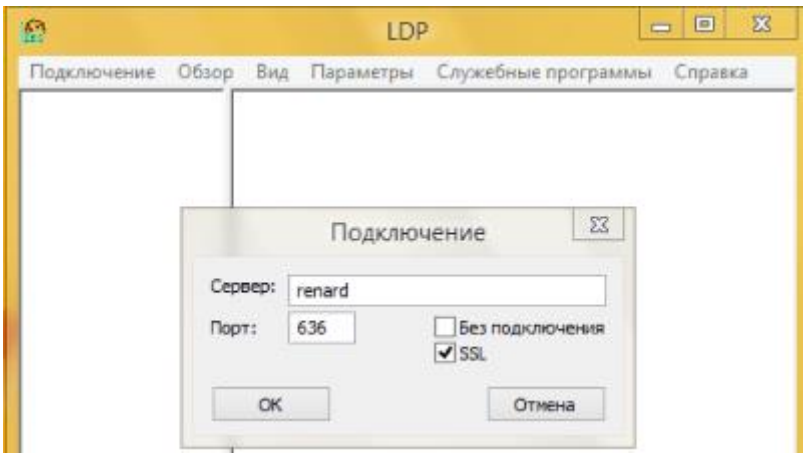


Рисунок 59 – Подключение порта SSL

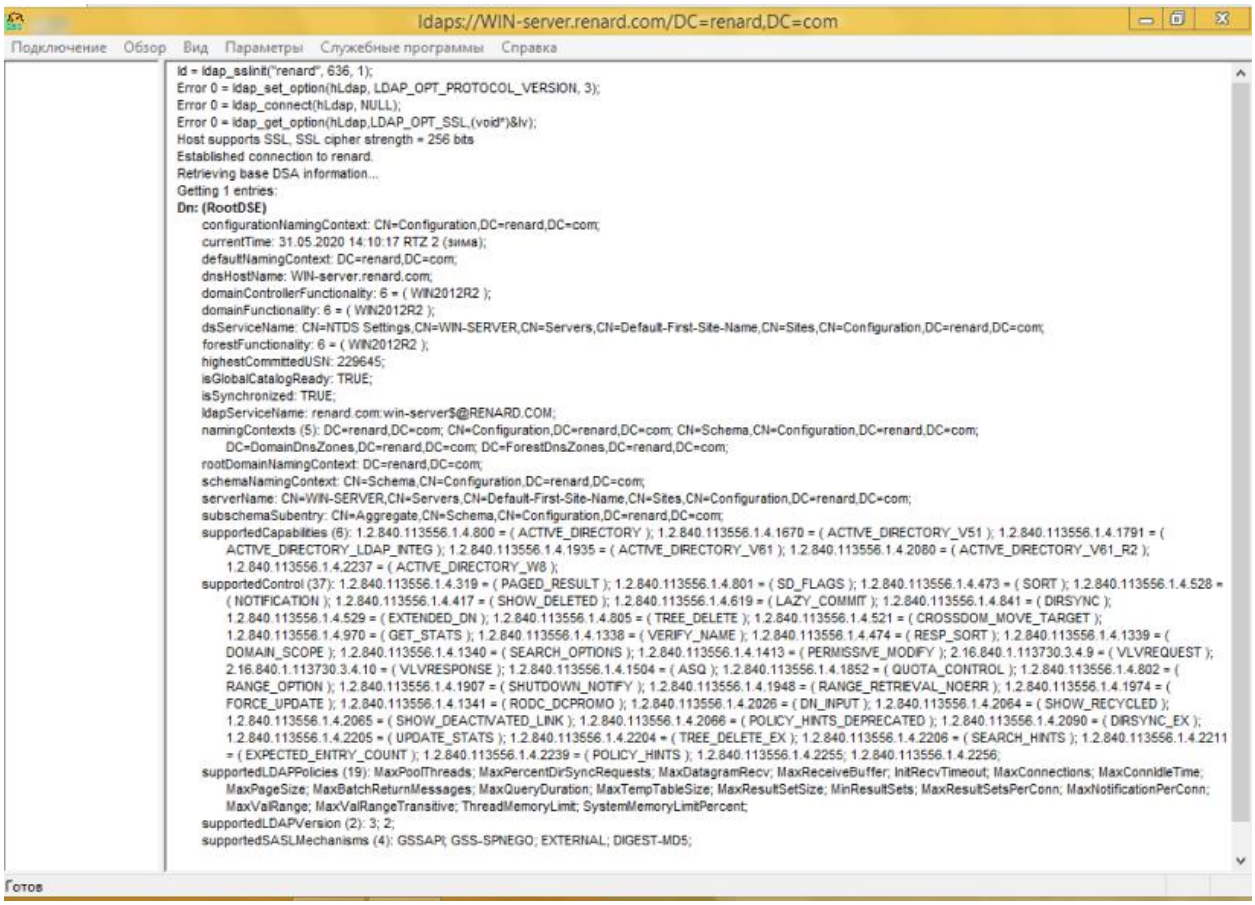


Рисунок 60 – Результат установки сертификации

Далее необходимо настроить отслеживания запросов по LDAP. Это можно сделать через оснастку контроллера домена «Системный монитор». Открыть Производительность - Группы сборщиков данных - Сеансы отслеживания событий. В контекстном меню выбрать Создать - Группа сборщиков данных (смотреть рисунок 61).

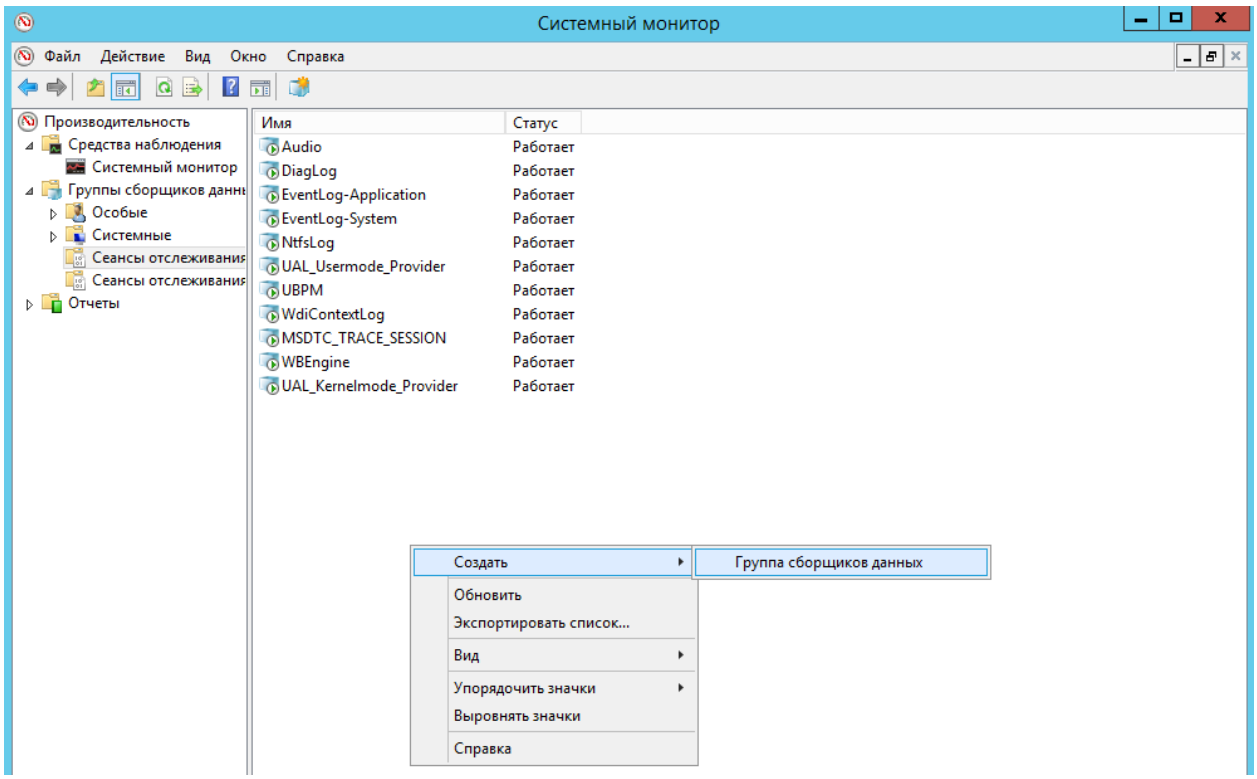


Рисунок 61 – Создание новой группы сборщиков данных

Вводится имя новой группы, выбирается пункт «Создать вручную (для опытных)». Данные действия представлены на рисунке 62.

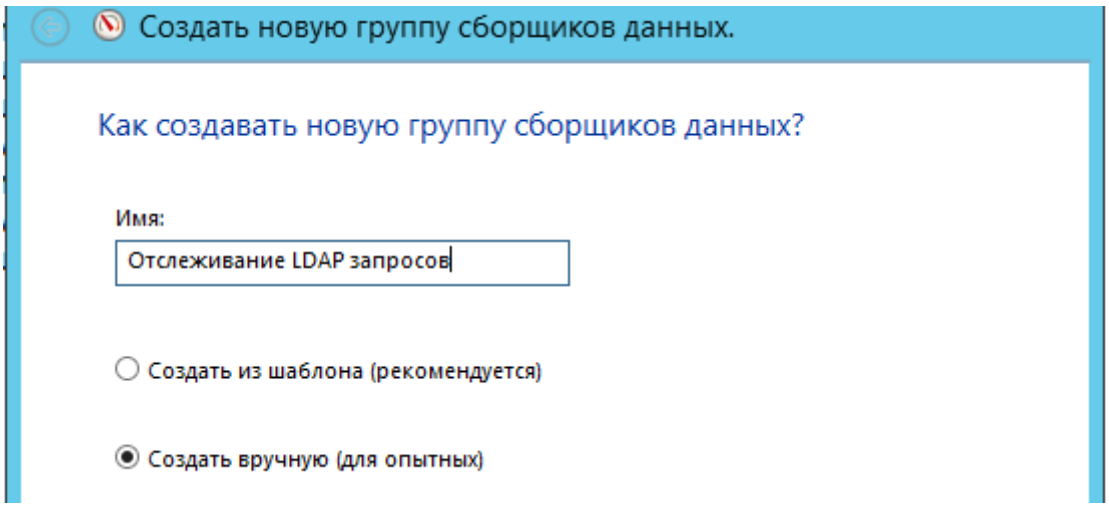


Рисунок 62 – Настройка новой группы сборщиков данных

На рисунке 63 выбирается поставщик данных. На рисунке 64 выбирается папка для сохранения отчетов мониторинга и на этом настройка новой группы сборщиков данных завершается остается ее только запустить. Для проверки мониторинга необходима остановить мониторинг службы, перейти в папку хранения отчетов и импортировать отчет в читаемый формат, что представлено на рисунках 65-67.

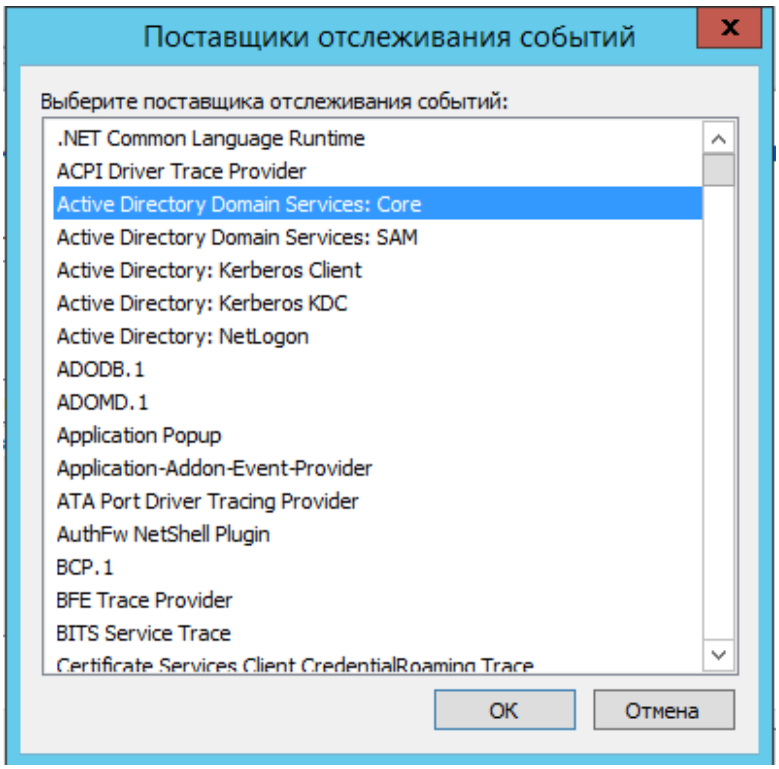


Рисунок 63 – Выбор поставщика данных

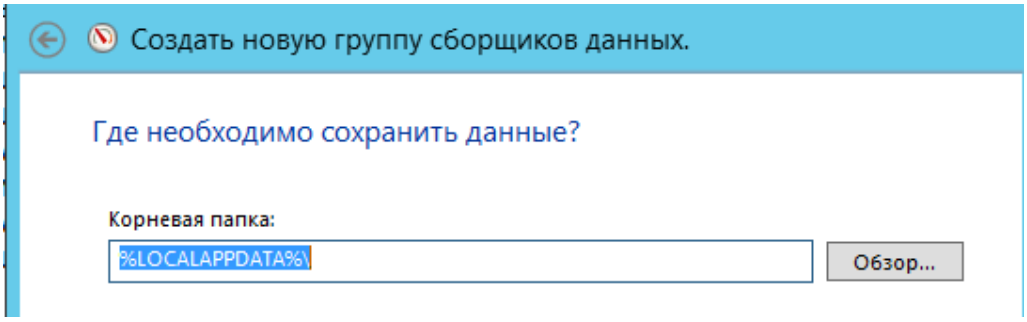


Рисунок 64 – Выбор папки хранения отчетов мониторинга

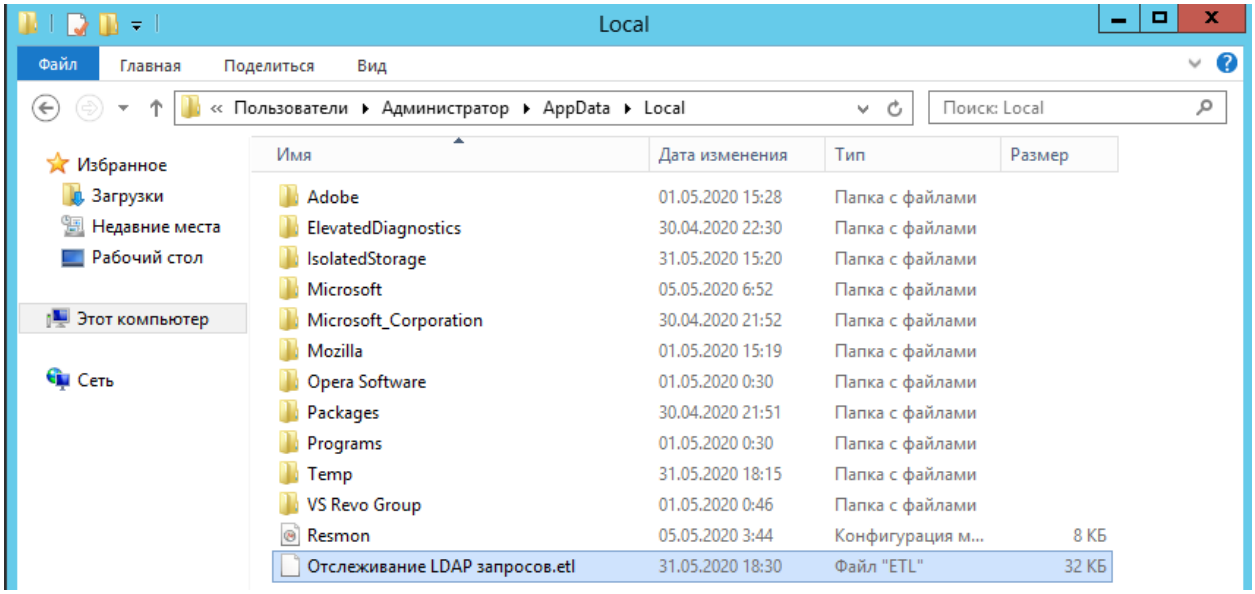


Рисунок 65 – Созданные отчеты по мониторингу

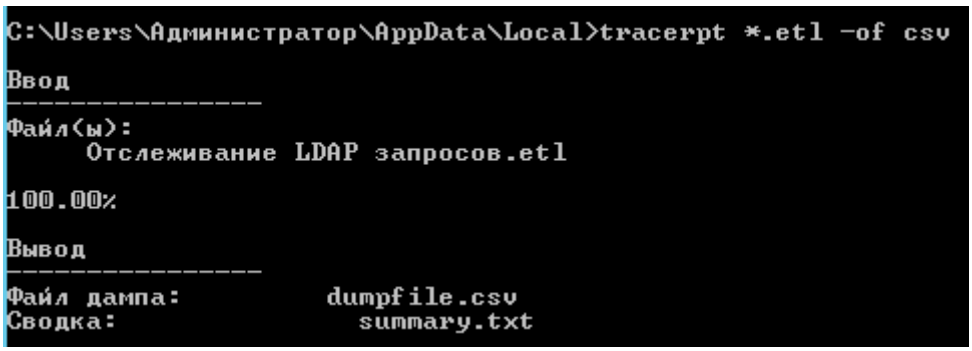


Рисунок 66 – Конвертация файла в читаемый формат

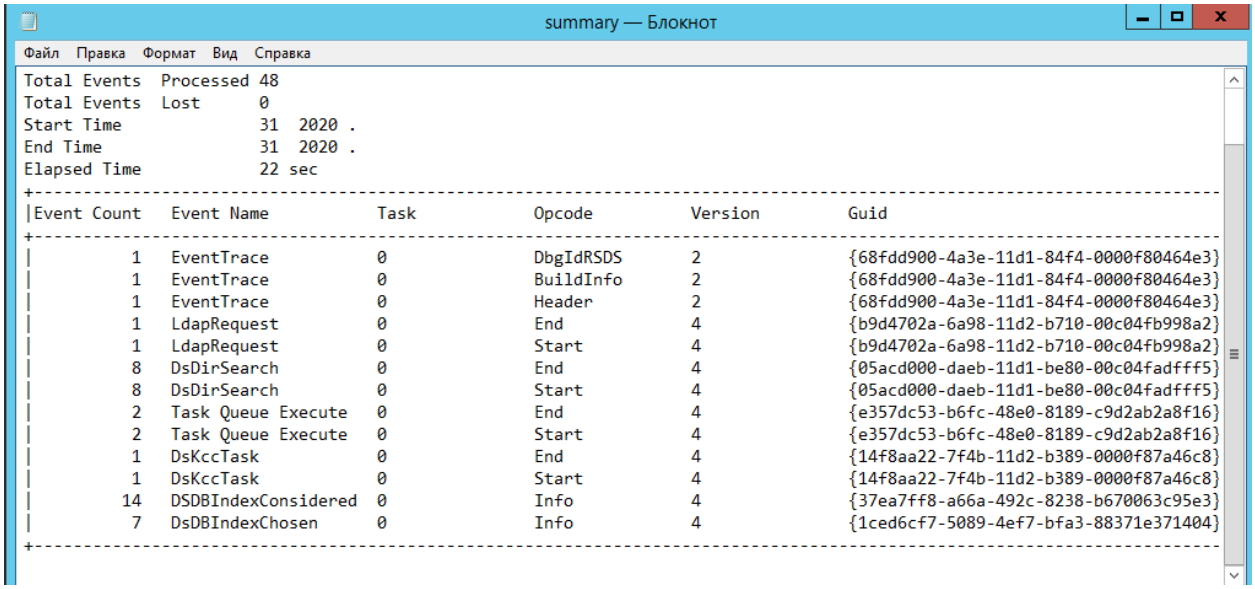


Рисунок 67 – Результат мониторинга

2.7 Защита от кражи кэша паролей

В этом разделе представлена комплексная методика защиты Windows от атак посредством утилиты Mimikatz. Стандартные средства Windows предлагают защищаться от этой утилиты с помощью запрета получения прав debug. Но этот метод считается неактуальным, так как злоумышленники давно нашли способ его обойти.

Для надежной защиты от Mimikatz для начала настроем безопасность памяти LSA. В Windows 8.1 и Windows Server 2012 R2 появилась возможность включения защиты LSA, обеспечивающей защиту памяти LSA и предотвращаю возможность подключения к ней из незащищённых процессов.

Для включения этой защиты, необходимо в ветке реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA с оздать параметр RunAsPPL со значением 1. Данное действие представлено на рисунке 68.

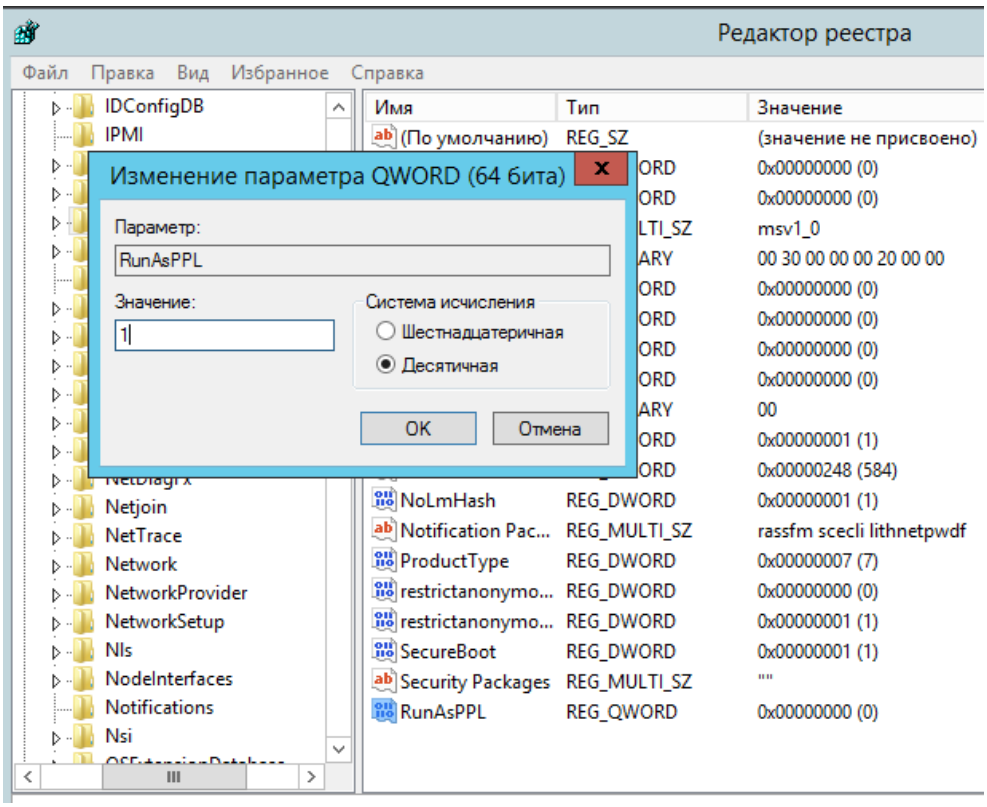


Рисунок 68 – Создание параметра безопасности LSA

После применения этого параметра атакующий не сможет получить доступ к памяти LSA, а mimikatz на команду securlsa::logonpassword, выдаст ошибку: ERROR kuhl_m_securlsa_acquireLSA : Handle on memory (0x00000005), представленную на рисунке 69.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # _
```

Рисунок 69 – Ошибка использования команды Mimikatz

Далее для защиты необходимо применить политику к компьютерам домена, запрещающую сохранять кэши учетных записей пользователей. Для этого включаем групповую политику Интерактивный вход в систему: количество предыдущих входов в кэш (если контроллер домена недоступен) а разделе Конфигурация компьютера - Настройки Windows - Локальная политика - Параметры безопасности, представленную на рисунке 70.

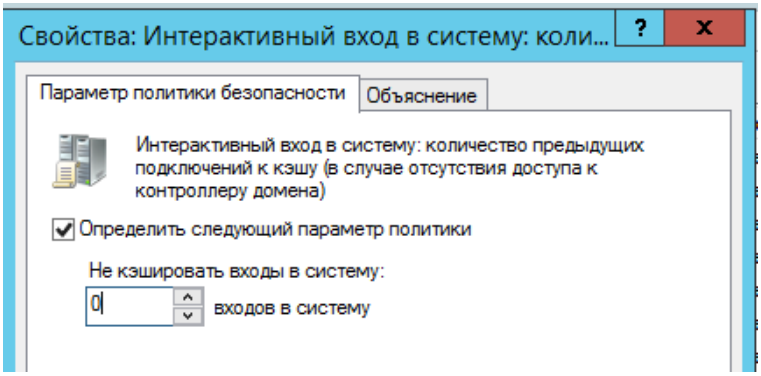


Рисунок 70 – Настройка групповой политики

Далее необходимо запретить пользователям домена сохранять свои пароли для доступа к сетевым ресурсам. Для этого необходимо включить групповуб политику Доступ к сети: не разрешать хранение паролей и учетных данных для сетевой аутентификации в разделе Конфигурация компьютера - Параметры Windows - Параметры безопасности - Локальные политики -Параметры безопасности и отключить сохранение паролей. Данные действия представленны на рисунках 71 и 72.

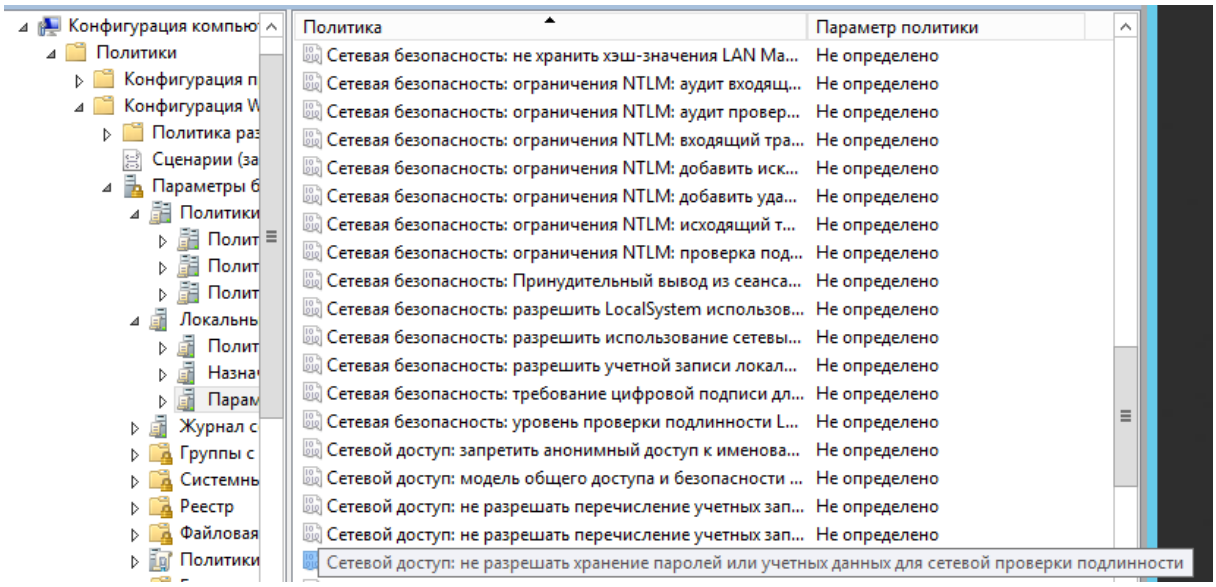


Рисунок 71 – Групповая политика

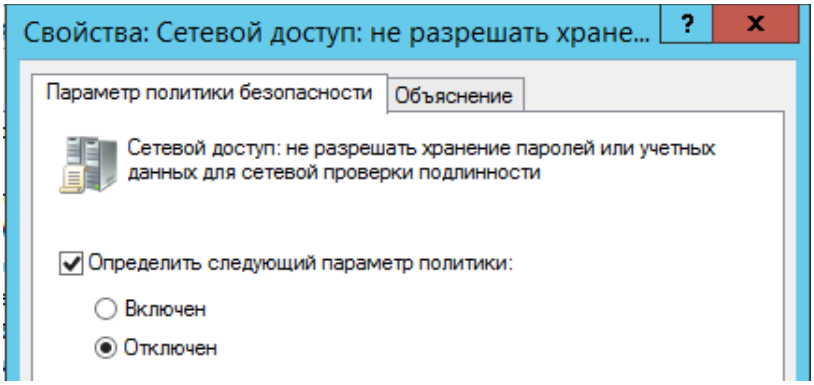


Рисунок 72 – Настройка групповой политики

2.8 Аудит членства групп пользователей

Так же утилиту Mimikatz можно использовать чтоб повысить свои привилегии в домене. Если же злоумышленнику все же получиться обойти защиту, выстроенную ранее необходимо настроить аудит для проверки членства в группах пользователей домена. Для этого был создан скрипт настроенный на аудит членства групп пользователей. Для скрипта были настроены время проверки и параметры проверки. Части скриптов представлены на рисунках 74,75 и 76. Весь скрипт представлен в приложении Д.

GroupScript.ps1

```
$script:monitorServer = 'WIN-server'

function New-AdGroupMembershipMonitor {
    [OutputType('pscustomobject')]
    [CmdletBinding(SupportsShouldProcess)]
    param
    (
        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$GroupName,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [scriptblock]$Action,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [pscustomobject]$Schedule,

        [Parameter()]
        [ValidateNotNullOrEmpty()]
        [string]$Name = ("AD Group $GroupName Monitor" -replace ' ', '_')
    )

    $ErrorActionPreference = 'Stop'
```

Рисунок 73 – Часть скрипта, указывающая на параметры проверки

GroupScript.ps1

```
function New-RecurringScheduledTask {
    [OutputType([void])]
    [CmdletBinding()]
    param
    (
        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$ComputerName,

        [Parameter(Mandatory)]
        [string]$Name,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [scriptblock]$Scriptblock,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [ValidateSet('Daily', 'Weekly')] ## This can be other intervals
        [string]$Interval,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$Time,
```

Рисунок 74 – Часть скрипта, указывающая на время работы проверки

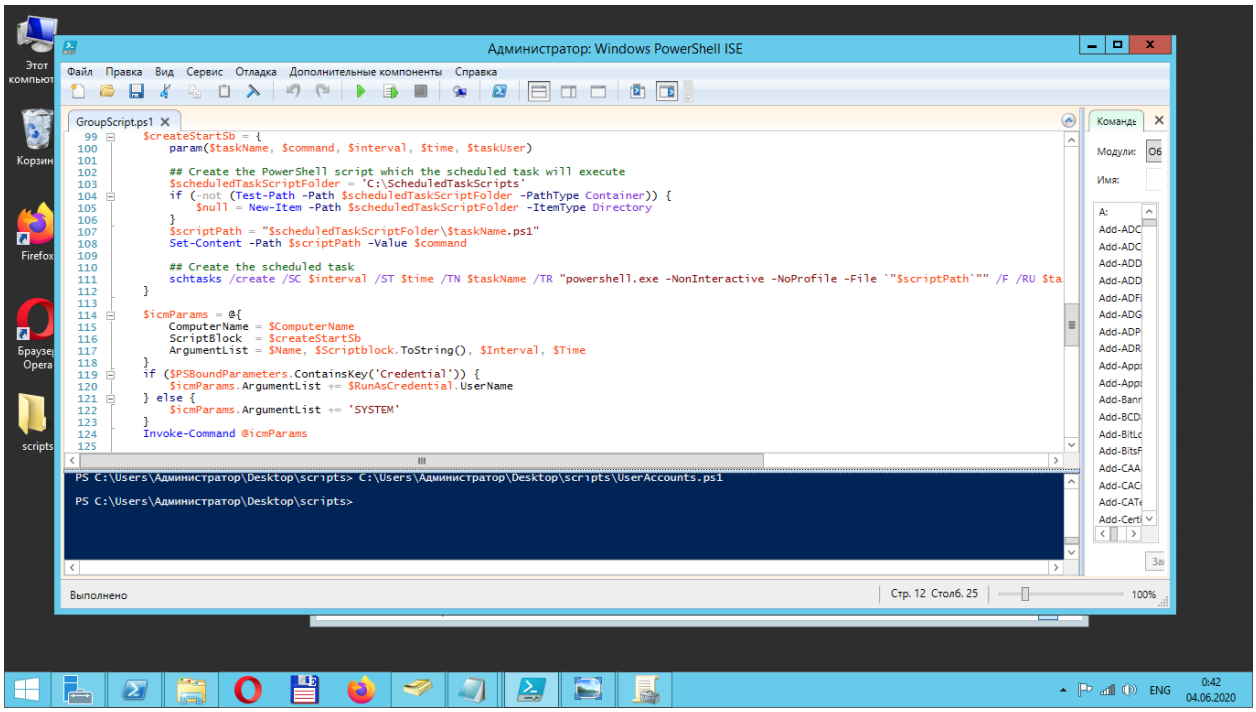


Рисунок 75 – Пример отработки скрипта

Из рисунка 76 видно что скрипт не выдал никаких ошибок. Теперь скрипт запущен и проводит проверки групп пользователей семь раз в неделю в соответствии с указаными параментрами. Результаты проверки будут записываться в файл C:\ ScheduledTaskScripts\ GroupAudit.csv

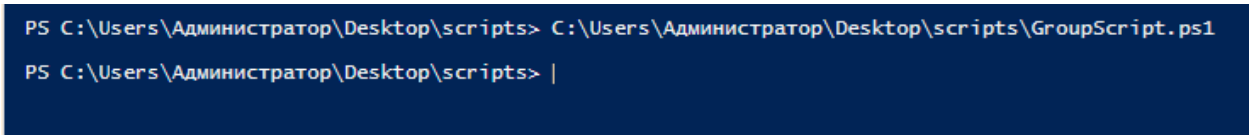


Рисунок 76 – Результат запуска скрипта

2.9 Проверка учетных записей пользователя

Часто в системе находятся учетные записи, не использующиеся пользователями. Подобные учетные записи могут быть целью злоумышленников, поэтому подобные учебные записи лучше блокировать либо вовсе удалять из домена. Для этого был создан скрипт который ищет учетные записи по нескольким критериям:

– учетная запись отключена;
– срок действия пароля истек;
– аккаунт никогда не использовался;
– аккаунт не использовался в течение 60 дней;

Заносит данные в документ и удаляет их из домена. На рисунке 77 представлен пример отработки скрипта. Весь скрипт представлен в приложении Ж.

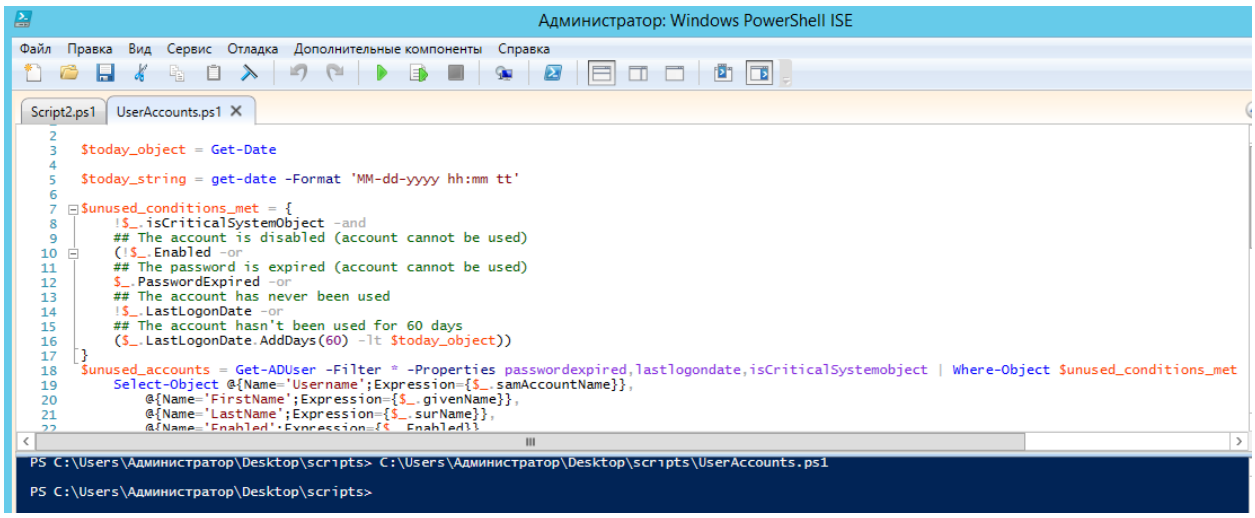


Рисунок 77 – Пример отработки скрипта

Как можно видеть, скрипт не выдал никаких ошибок и записал результат в файл file1.txt, представленный на рисунке 78.

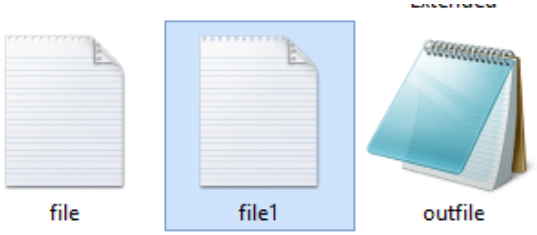


Рисунок 78 – Созданный файл

На рисунке 79 видно, что скрипт нашел трех пользователей подходящих под заданные параметры. Попробуем зайти под учетной записью найденной скритом. Результаты отработки скрипта представленны на рисунках 80 и 81.

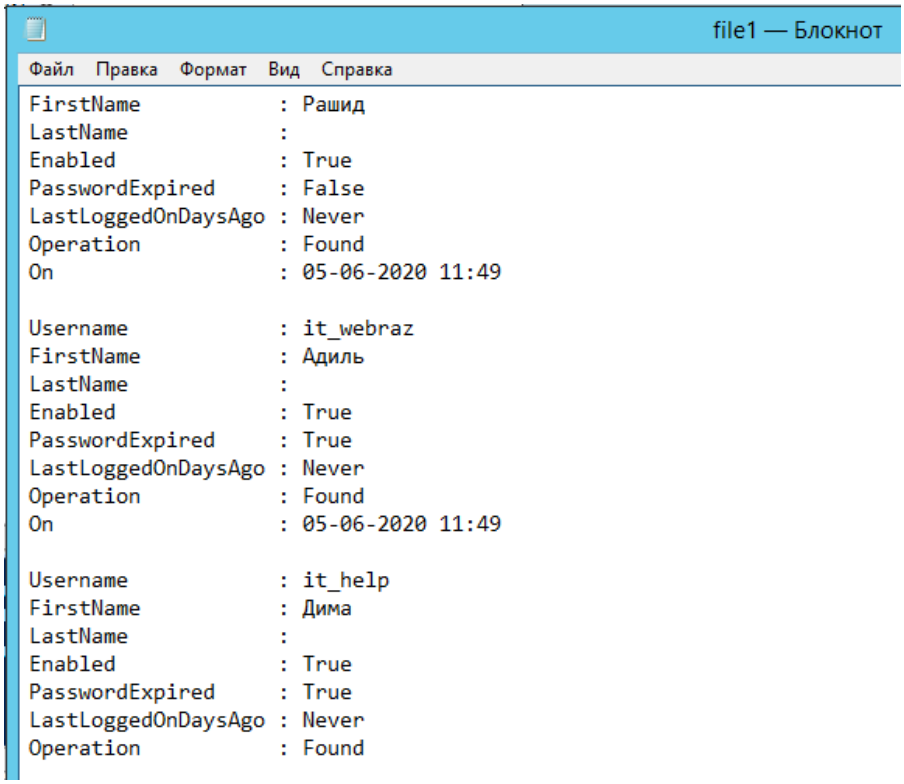


Рисунок 79 – Результат отработки скрипта

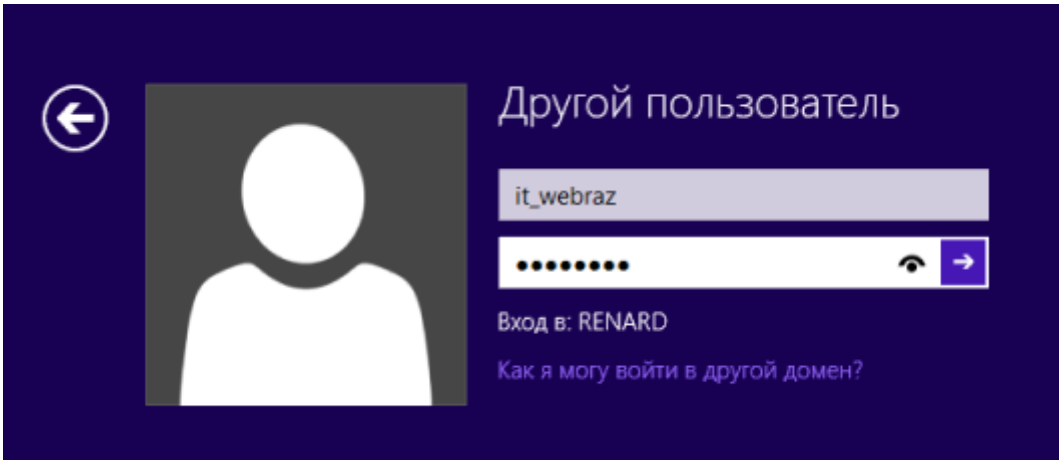


Рисунок 80 – попытка входа через удаленную учетную запись

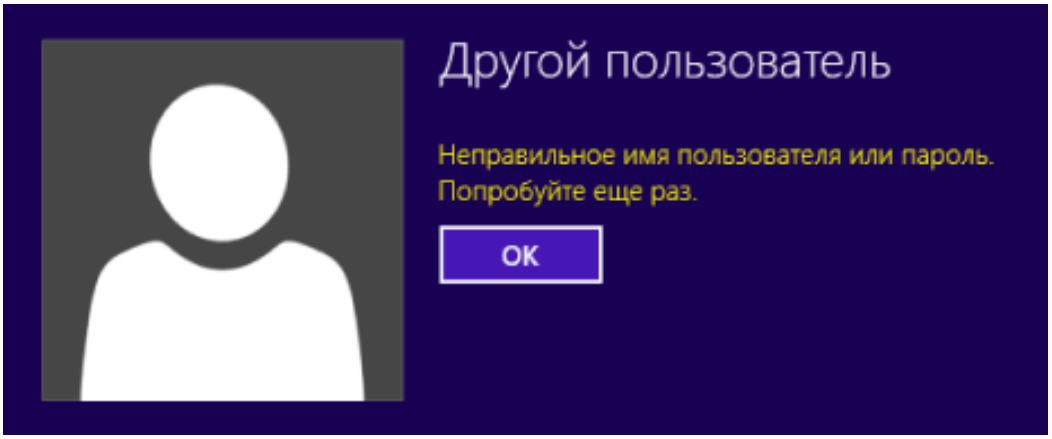


Рисунок 81 – подтверждение удаления учетной записи

3 Анализ рисков информационной безопасности

В первую очередь для расчета рисков информационной безопасности были определены защищаемые активы: сам Active Directory, данные пользователей (учетные записи, пароли, права доступа), сетевая инфраструктура и сервер (сервер, на котором находится AD).

Риски информационной безопасности были рассчитаны с учетом особенностей темы работы. Были рассчитаны риски для вышеперечисленных активов (незащищенных).

Основным методом при оценке рисков, являлся качественный метод с помощью которого были определен максимальный уровень риска. Качественная оценка риска определяет риск с точки зрения степени его воздействия и вероятности его возникновения. Уровни воздействия и вероятности могут быть объединены в матрицу риска для получения оценки уровня серьезности риска. Оценки точности низкого, среднего и высокого уровня могут быть присвоены оценке риска, чтобы показать его достоверность.

В отличие от количественного анализа риска, который применяет числовые значения и использует проверяемые данные, качественный анализ риска работает в более обобщенном, «большом» пространстве. Количественный анализ риска использует данные для получения значения для измерения приемлемости результата события риска.

После этого в качестве мер обработки данных рисков были указаны меры защиты, рассмотренные в данной работе. Расчет остаточных рисков был произведен с учетом данных защитных мер.

Для анализа рисков был выбран алгоритм из стандарта ISO-27005. Расчет по первому алгоритму (по двум шкалам) производится на основе приложения Е стандарта ISO-27005.

Таблица 1 – Ценность активов, уровни угроз и уязвимостей

Степень вероятности возникновения угрозы	Низкая			Средняя			Высокая		
Простота использования	Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	1	2	1	2	3	2	3	4
	1	2	3	2	3	4	3	4	5
	2	3	4	3	4	5	4	5	6
	3	4	5	4	5	6	5	6	7
	4	5	6	5ы	6	7	6	7	8

Простой общий рейтинг рисков:

- низкий риск: 0-2;
- средний риск: 3-5;
- высокий риск: 6-8.

Остаточный риск – это риск, который остается после мер по контролю над рисками. Расчет остаточного риска осуществляется по формуле, представленной на рисунке 82.

Остаточный риск = Первичный риск – Влияние мероприятий по контролю над рисками

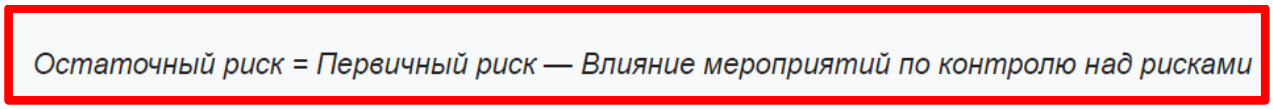


Рисунок 82 – Формула расчета остаточного риска

Далее описаны основные угрозы и уязвимости, касающиеся активы Компании:

1. Некорректно составленная система привилегий – данный тип уязвимости может привести к тому, что пользователи могут получить доступ к информации, которая была для них не предназначена, что может повлиять на конфиденциальность целостность и доступность актива.
2. Удаленный доступ по незащищенным портам – при подключении пользователей необходимо организовать защищенный канал связи, для того чтобы избежать потерю конфиденциальной информации, также необходимо ознакомить сотрудников с памяткой при удаленной работе.
3. Данные системы хранятся в незашифрованном виде – для защиты данных системы и бэкапов, необходимо использовать методы шифрования для избежание потери или же компрометации информации, хранящиеся на съёмных носителях.
4. Соединение с базой данных по незащищенному соединению – для того, чтобы сервер получал информацию с БД необходимо организовать защищённый туннель, по которому будут передаваться бэкап данные БД.
5. Сетевые атаки по типу «человек посередине» – данный тип атаки довольно распространённый и при осуществлении такого типа атаки можно потерять всю конфиденциальную информацию, находящаяся в сети работника или же Компании.
6. Успешно сгенерированный пароль с помощью «брутфорс» – для предотвращения такой угрозы, необходимо чтобы все сотрудники компании были ознакомлены с политикой безопасности компании.
7. Пользователи являются участниками всех групп пользователей – при администрировании AD, необходимо учитывать, группы доступ, к которым разрешен определенным пользователям, в противном случае пользователи может получить доступ к информации, которая не предназначалась для него, либо повысить себе привилегии, с помощью аудита можно отследить действия отдельных пользователей и администраторов сети, что положительно влияет на защищенность корпоративных данных.
8. Включенная гостевая учетная запись – необходимо отключить гостевую учетную запись, доступ к которой злоумышленник может

получить, и при работе в данной учетной записи злоумышленник может украсть отчетность отделов связанные с финансами.

9. Некорректная настройка сервера – специалист по администрированию сервер, должен быть высококвалифицированным так как при неправильном ремонте или же его настройке может привести к потере или утрате важной информации.

10. Атаки на приложения работающее на сервере – приложения, которые работают на сервере должны иметь защищенное внешнее соединение, журналировать все события, а также мониториться программами корректировки, так как если будет совершена атака на приложения, информация, хранящаяся на сервере может быть полностью утрачена или атаки, могут привести к неисправности сервера в целом.

Таблица 2 – Анализ рисков информационной безопасности

№	Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Комментарии, ресурсы, ответственный
Актив 1. Active Directory						
1	Несанкционированный доступ к данным нелегитимных пользователей	Непродуманная система предоставления привилегий	7	Аккуратное и продуманное предоставление прав пользователям. Аудит: отслеживание несанкционированных действий	2	Администратор домена
2	Получение доступа через удаленный рабочий стол	Использование стандартных RDP-портов для подключения к удаленному рабочему столу	7	Создание и настройка групповых политик для смены портов	2	Сетевой администратор
3	Получен доступ к файлам. Как следствие,	Отсутствие шифрования на жестком диске	7	Настройка шифрования диска с помощью Bitlocker	2	Администратор домена

	возможность копирования конфиденциальных данных					

Продолжение таблицы 2

Актив 2. Сетевая инфраструктура						
4	Атака на порт ssh. Следствие: перехват передаваемых на бэкап-сервер копий БД	Отсутствие контроля сетевого доступа	6	Использование ACL-списков пакета dbms_network_acl_admin	2	Администратор домена
5	Осуществление атаки "Человек посередине". Перехват трафика	Недостаточная защита передаваемого трафика	7	Шифрование трафика между сервером и клиентами. Oracle Network Encryption	1	Сетевой администратор
Актив 3. Данные пользователей						
6	Повышение привилегий. Брут форс логинов и паролей пользователей.	Отсутствие политик пользователей	8	Политики паролей и использования ресурсов. Настройка профилей пользователей	3	Администратор домена
7	Повышение привилегий через группы пользовател	Отсутствие аудита групп пользователей	6	Создание и запуск скрипта на аудит изменений в группах	3	Администратор домена

	ей			пользователей		
8	Модификация данных. Злоумышленник может, используя гостевую учетную запись, получить доступ к отчетности и модифицировать или удалить данные	Отсутствие мониторинга пользователей, Отсутствие проверки политики хранения документов	6	Создание и запуск скриптов на сбор данных по пользователям. Проверка хранимых документов	2	Администратор домена

Продолжение таблицы 2

Актив 4. Серверы: сервер и бэкап-сервер						
9	Испорчен жесткий диск сервера, информация с него восстановлена не в	Неправильный и неаккуратный ремонт аппаратуры сервера	6	Резервное копирование хранящейся на диске информации	1	Администратор домена

	полной мере					
10	Сетевые атаки на приложения (работающие с сервером) из внешних или кооперативных сетей, использующие уязвимости приложении с целью нарушения КЦД информации	уязвимости приложении, работающих с сервером	7	Настройка соответствующих групповых политик, запрет на использование приложений	3	Администратор домена

Данная таблица наглядно показывает степень влияния рисков возникшие в результате возникновения угроз. С помощью данных полученные в результате расчёта, можно увидеть, что высокую степень риска имеют угрозы, связанные с физическим доступом к серверу с AD, а также атаки, направленные на повышение привилегий. Степень риска колеблется от 7-8, что значит данные угрозы имеют высокий уровень риска. После того, как были проведены расчеты, для снижения уровня риска выставлены защитные меры с помощью, которых степень риска данных угроз сократились в 2 раза, и тем самым Компания может в дальнейшем уменьшить степень влияниях данных рисков, что позволяет увеличить бюджет для улучшения мер защиты.

Далее представлены различные диаграммы взаимосвязей компонентов анализа рисков (на базе вышеуказанной таблицы анализа рисков), реализованные в программе CORAS.

На рисунке 83 представлена диаграмма защищаемых активов. Они разделены на категории: «Оборудование» и «Информационные ресурсы». К примеру, актив «Сервер» входит в категорию «Оборудование», актив «Active Directory» - в категорию «Информационные ресурсы».

На рисунке 84 представлена диаграмма модели угроз. Данная диаграмма графически показывает угрозы и уязвимости, которые могут возникнуть с активами Компании. Элементы диаграммы слева направо: источники угроз, уязвимости, этапы реализации угроз, последствия реализации угроз (инциденты), понесшие от реализации угрозы ущерб

активы. К примеру, источник угроз «Прочий персонал», используя уязвимость «Отсутствие аудита изменений групп пользователей», осуществляет «Повышение привилегий в домене» и получает доступ к конфиденциальной информации. Возможные последствия реализации угрозы: «Копирование файлов», «Удаление файлов», «Модификация файлов». Актив, на который направлена угроза – «Данные пользователей», «Active Directory».

На рисунке 85 представлена диаграмма модели угроз с учетом вероятности возникновения инцидента. Ее следует читать также, как и диаграмму, представленную на рисунке 3, только добавлен параметр вероятности возникновения инцидентов (высокая, средняя, низкая). К примеру, инцидент «Повышение привилегий в домене» имеет высокую вероятность возникновения, а инцидент «Атака человека по середине» имеет среднюю вероятность возникновения.

На рисунке 86 представлена диаграмма рисков с характеристиками влияния угроз. Элементы диаграммы слева направо: источники угроз, уязвимости, способы реализации угроз, степень влияния реализации угроз, понесшие от реализации угрозы ущерб активы. К примеру, «Злоумышленник», используя уязвимость «Отсутствие политик паролей», осуществляет угрозу «Брут форс логинов и паролей пользователей», что сильно повлияло на атакуемые активы – Active Directory и данные пользователей.

На рисунке 87 представлена диаграмма модели угроз с учетом защитных мер. Ее следует читать так же, как и диаграмму, представленную на рисунке 3, с единственным отличием: между уязвимостями и способами реализации угроз добавлены защитные меры для уменьшения рисков. К примеру, для уязвимости «Отсутствие шифрования» внедрена защитная мера «Шифрование данных при помощи BitLocker».

На рисунке 88 представлена диаграмма недопустимых рисков. Она построена на базе диаграммы, представленной на рисунке 5, однако на данной диаграмме показаны только те риски, которые имеют высокую степень влияния угроз.

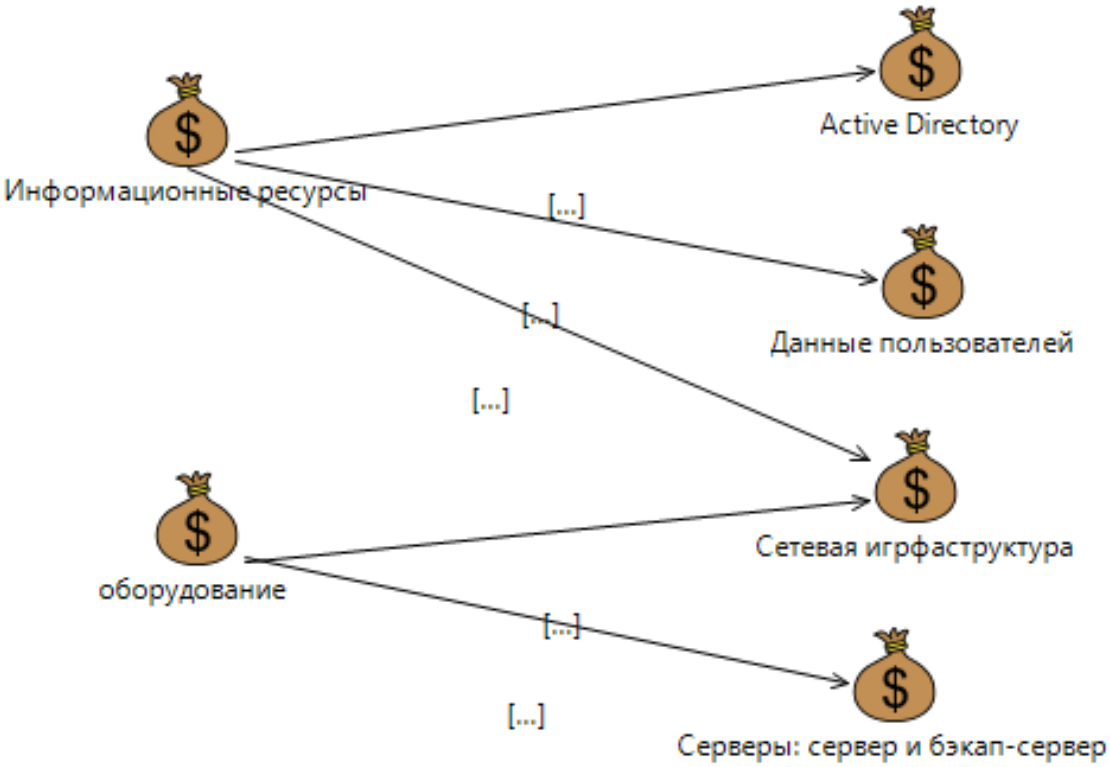


Рисунок 83 – Перечень активов

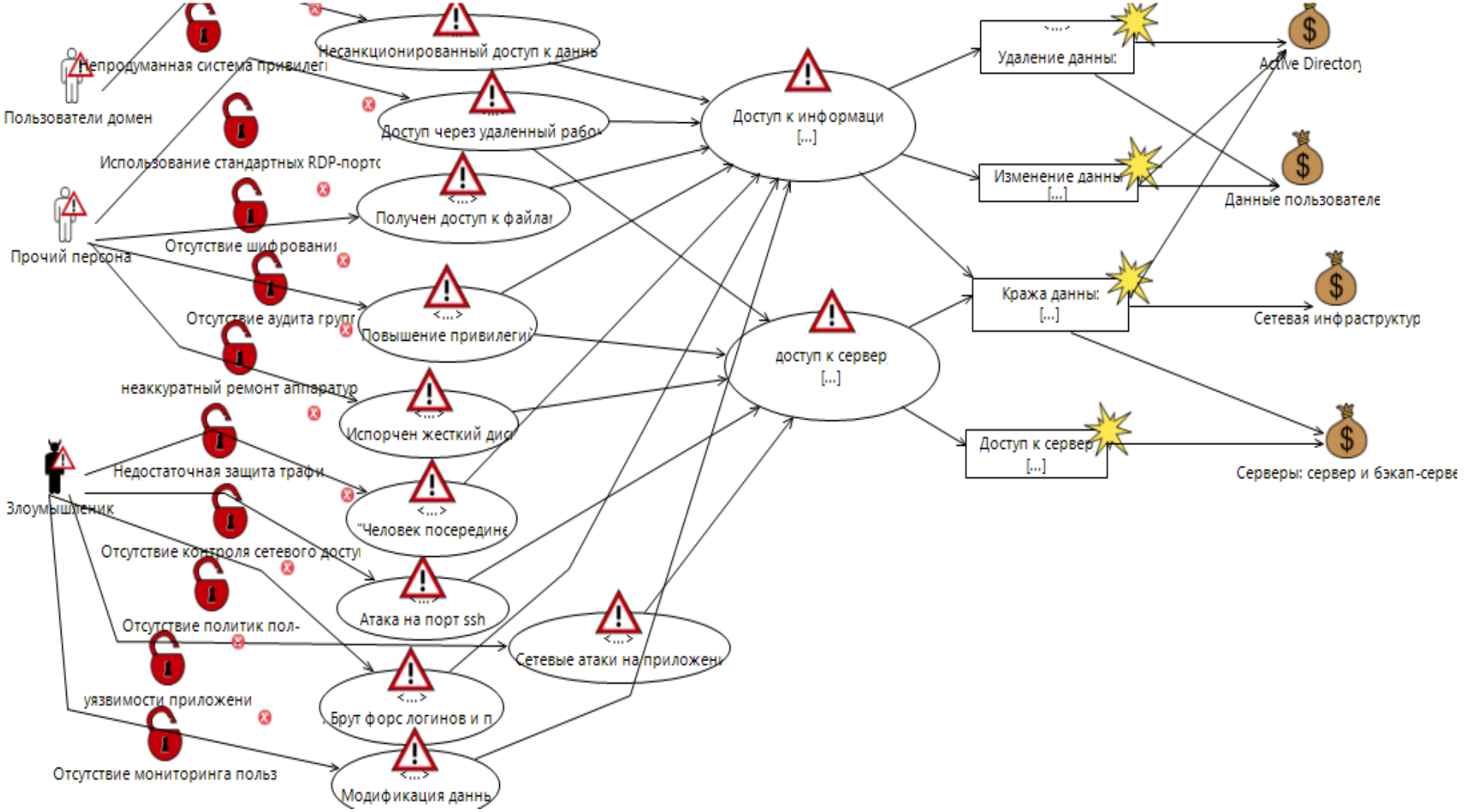


Рисунок 84 – Модель угроз

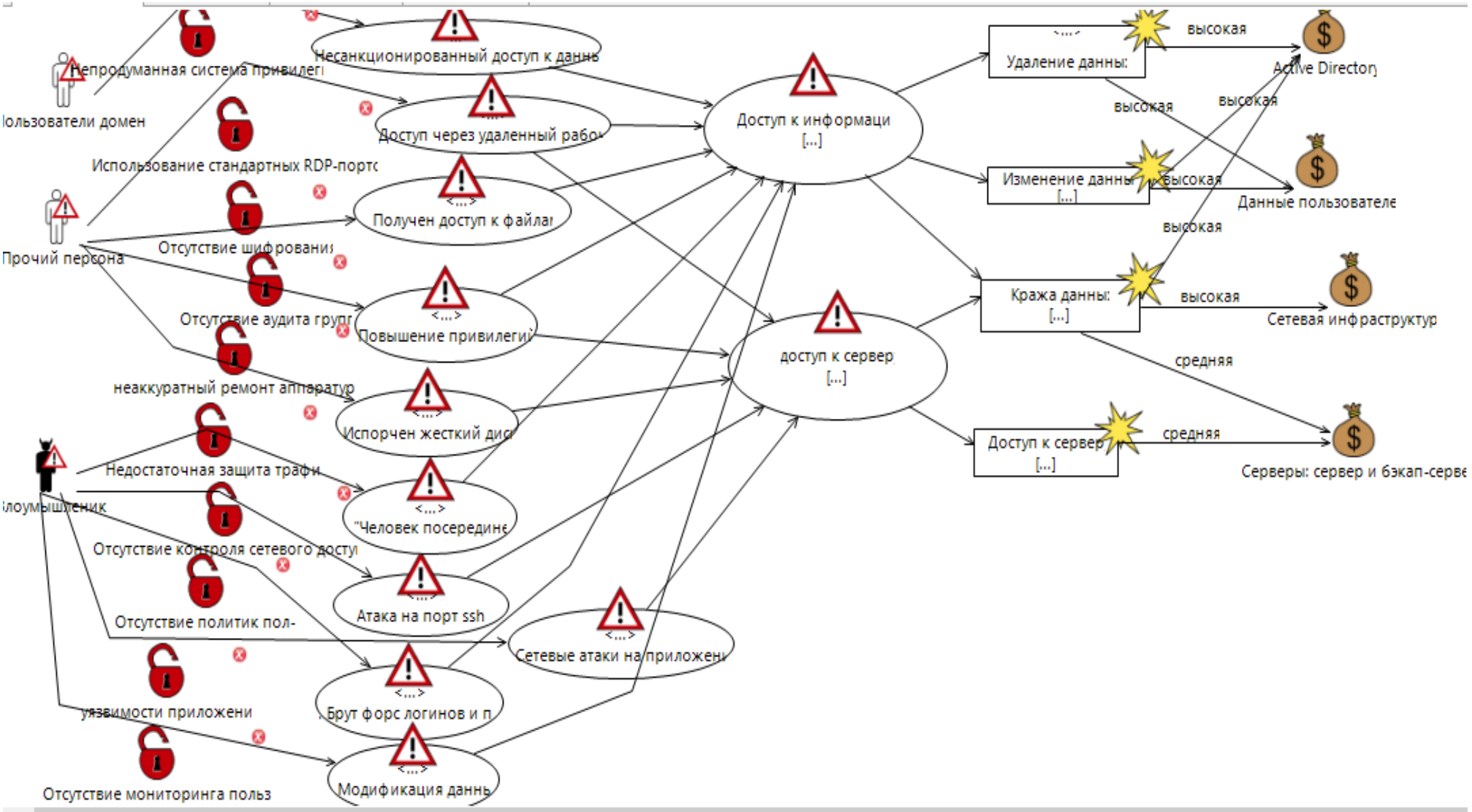


Рисунок 85 – Модель угроз с учетом вероятности возникновения инцидента

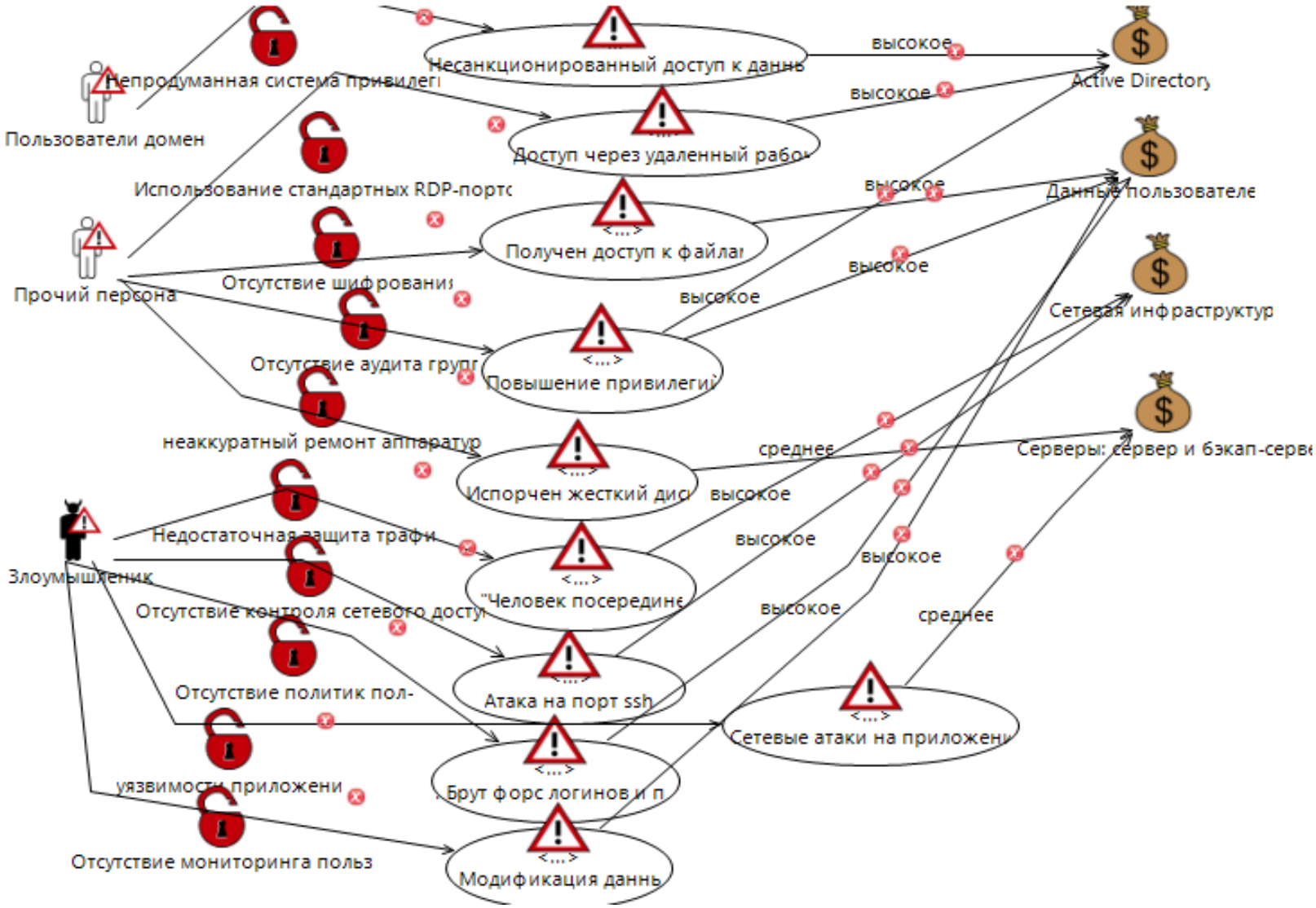


Рисунок 86 – Диаграмма рисков с характеристиками влияния угроз

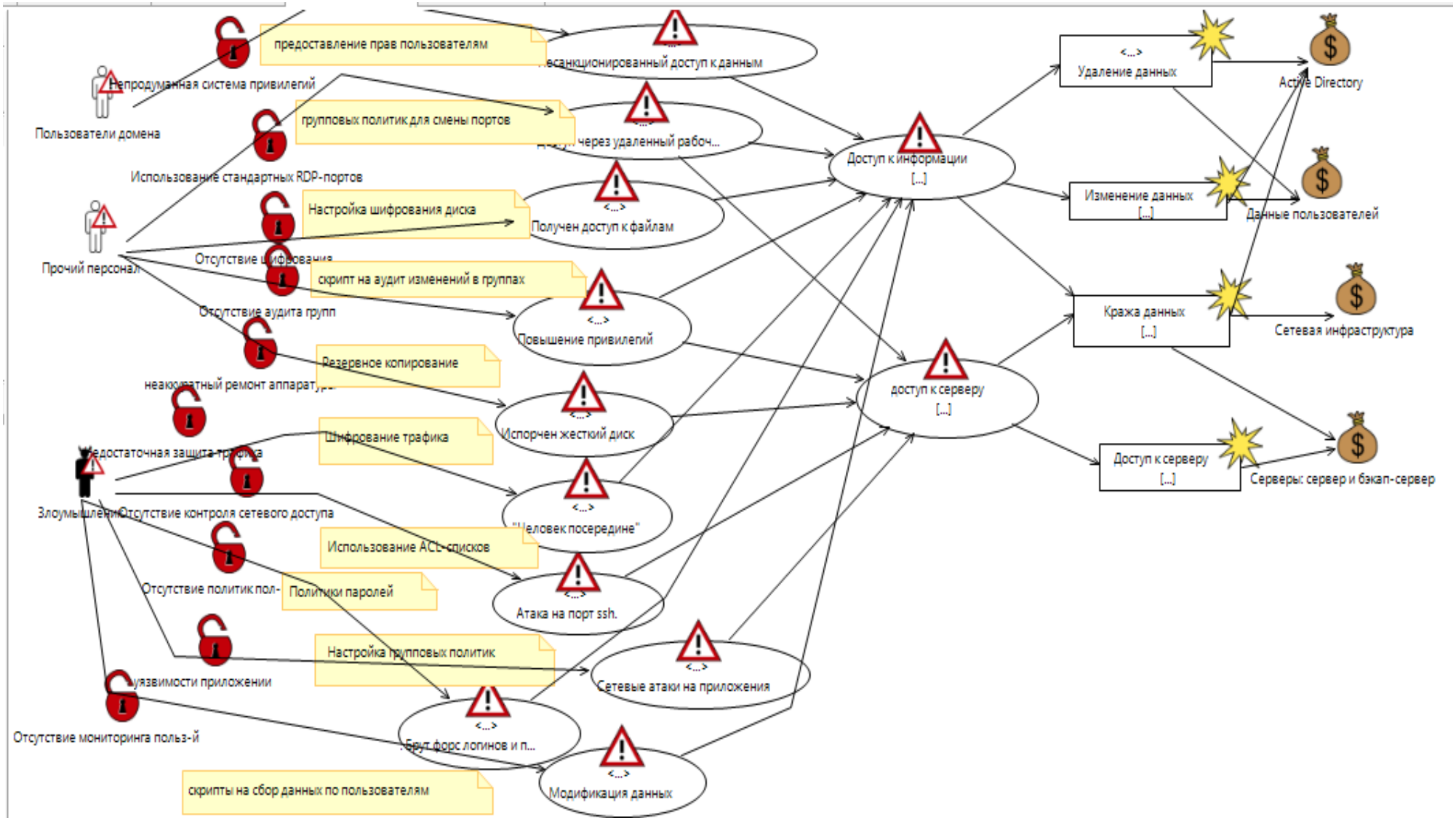


Рисунок 87 – Модель угроз с учетом защитных мер

Рисунок 88 – Диаграмма недопустимых рисков

Выводы: Были описаны и рассчитаны основные риски информационной безопасности для незащищенных активов «Active Directory», «Данные пользователей», «Сетевая инфраструктура» и «Серверы. Сервер и бэкап-сервер». В результате расчета все риски оказались неприемлемыми (от 6 до 8 по 8-ми балльной шкале), поэтому для всех рисков были описаны защитные меры (всё то, что было проделано в данной работе для защиты AD). После введения мер для обработки рисков риски были пересчитаны, получены остаточные риски. Все риски, оставшиеся после перерасчета с учетом защитных мер, стали приемлемыми (от 0 до 2 по 8-ми балльной шкале). Как видно из расчетной таблицы после внедрения защитных мер риски уменьшились в 4 раза (на 25%).

4 Безопасность жизнедеятельности

4.1 Анализ условий труда сотрудников офиса

Наш офис состоит находится на первом этаже состоит из 10 помещений в состав которых входит:

1. Серверная.
2. Уборная.
3. Отдел разработки.
4. Переговорная.
5. Отдел бухгалтерии.
6. Кабинет начальника.
7. Отдел тестирования.
8. Кабинет системного администратор.
9. Место хранения оборудования.
10. Отдел безопасности.

График работы будние дни с 08-00 до 17-00, без учетов праздников и вынужденного выхода на работу по разным обстоятельствам. В офисе одновременно может находится примерно 50 человек и для создания условий для безопасной, и продуктивной работы необходимо учитывать следующие факторы:

1. Микроклимат.
2. Шум.
3. Вибрации.
4. Электрические, магнитные, электромагнитные поля.
5. Качество используемого оборудования.
6. Освещение на рабочих местах.
7. Вентиляция.
8. Пожаробезопасность.
9. Эргономика.

На все эти факторы предусмотренные нормативы, утвержденные СанПин 2.2.4.3359-16, СанПиН 2.2.4.548-12 и т.д. [13]

СанПин устанавливает оптимальные температурные значения на месте работы для создания благоприятного микроклимата. К показателям микроклимата относится (п. 2.2.1 СанПиН 2.2.4.3359-16):

1. Температура воздуха.
2. Температура поверхностей.
3. Относительная влажность воздуха.
4. Скорость движения воздуха.
5. Интенсивность теплового облучения.

Категории работ разграничиваются на основе интенсивности общих энергозатрат организма в ккал/ч(Вт). К категории Iа относятся работы с интенсивностью энергозатрат до 120 ккал/ч к коем можно отнести работу в офисе. [13]

Оптимальные значения параметров микроклимата на рабочих местах производственных и офисных помещений: [13]

Таблица 3 – Оптимальные значения микроклимата

Период года	Категория работ по уровню энергозатрат, Вт*	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Ia	22–24	21–25	60–40	0,1
	Iб	21–23	20–24	60–40	0,1
	IIa	19–21	18–22	60–40	0,2
	IIб	17–19	16–20	60–40	0,2
	III	16–18	15–19	60–40	0,3
Теплый	Ia	23–25	22–26	60–40	0,1
	Iб	22–24	21–25	60–40	0,1
	IIa	20–22	19–23	60–40	0,2
	IIб	19–21	18–22	60–40	0,2
	III	18–20	17–21	60–40	0,3

Допустимые значения параметров микроклимата на рабочих местах производственных и офисных помещений: [13]

Таблица 4 – Значения микроклимата на рабочих местах

Период года	Категория работ по уровню энергозатрат, Вт	Температура воздуха, °С		Температура поверхности, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с	
		диапазон ниже оптимальных величин	диапазон выше оптимальных величин			для температуры воздуха ниже оптимальных	для температуры воздуха выше оптимальных

Продолжение таблицы 4

Холодный	Ia	20,0–21,9	24,1–25,0	19,0–26,0	15–75	0,1	0,1
	Iб	19,0–20,9	23,1–24,0	18,0–25,0	15–75	0,1	0,2
	IIа	17,0–18,9	21,1–23,0	16,0–24,0	15–75	0,1	0,4
	IIб	15,0–16,9	19,1–22,0	14,0–23,0	15–75	0,2	0,3
	III	13,0–15,9	18,1–21,0	12,0–22,0	15–75	0,2	0,4
Теплый	Ia	21,0–22,9	25,1–28,0	20,0–29,0	15–75	0,1	0,2
	Iб	20,0–21,9	24,1–28,0	19,0–28,0	15–75	0,1	0,3
	IIа	18,0–19,9	22,1–27,0	17,0–28,0	15–75	0,1	0,4
	IIб	16,0–17,9	21,1–27,0	15,0–28,0	15–75	0,2	0,5
	III	15,0–16,9	20,1–26,0	14,0–27,0	15–75	0,2	0,5

Для создания продуктивных условий работы также стоит обратить на уровень шума, создаваемый в офисе, уровень шума, не выходящий за нормы, установленные в СН 2.2.4(2.1.8.562.96 Шум на рабочих местах в помещениях жилых общественных зданий и на территории жилой застройки) создает благотворные условия для рабочей деятельности [14].

Таблица 5 – Нормы уровня шума

N п / п	Вид трудовой деятельности, рабочее место	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровни звука (дБА)
		31,5	63	125	250	500	1000	2000	4000	8000	
1	2	3	4	5	6	7	8	9	10	11	12
1	Рабочие места в помещениях, дирекции, проектно-конструкторских бюро, расчетчиков, программистов вычислительных машин, в лабораториях для теоретических работ и обработки данных, приема больных в здравпунктах, творческая и руководящая деятельность, составление логистических запросов, ведения и разработка виртуальных продуктов.	86	71	61	54	49	45	42	40	38	50

Предельно допустимые уровни инфразвука на рабочих местах [15].

Таблица 6 – Предельно допустимые уровни инфразвука

Рабочие места, территория жилой застройки, помещения жилых и общественных зданий	Эквивалентные уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц				Эквивалентный общий уровень звукового давления, дБ
	2	4	8	16	
Работы с различной степенью тяжести и напряженности трудового процесса на рабочих местах:					
- в средствах транспорта	110	105	100	95	110
- работы различной степени тяжести	100	95	90	85	100
- работы различной степени интеллектуально-эмоциональной напряженности	95	90	85	80	95
Примечания: 1. Максимальный текущий общий уровень инфразвука не должен превышать 120 дБ. 2. При сокращенном рабочем дне (менее 40 ч в неделю) ПДУ применяется без изменения.					

Предельно допустимые уровни звукового давления воздушного ультразвука на рабочих местах[15].

Таблица 7 – Предельно допустимые уровни звукового давления воздушного ультразвука

Третьоктавные полосы частот, кГц	Уровни звукового давления, дБ
12,5	80
16,0	90
20,0	100
25,0	105
31,5-100,0	110

Предельно допустимые уровни контактного ультразвука на рабочих местах [15].

Таблица 8 – Предельно допустимые уровни контактного ультразвука

Поддиапазоны частот, кГц	Усредненная во времени пиковая пространственная интенсивность, Вт/см	Усредненная во времени пиковая пространственная интенсивность для совместного действия воздушного и контактного УЗ, Вт/см
11,2-80	0,03	0,017
80-630	0,06	
0,63·10 -5,0·10	0,1	

4.2 Расчет обеспечения безопасности от поражения электрическим током в офисе

Произведём расчеты на основе, что мы имеем офис, находящийся на первом этаже жилого комплекса. Офис используется it- компанией “RenardCompany”, которая активно использует техническое оборудование потребляющие много электроэнергии.

В офисе используется техника, подключенная в сеть электропитания. Следовательно, должны соблюдаться меры предосторожности по использованию техники. Персонал должен быть хорошо осведомлен о технических характеристиках техники и правилах ее использования.

Защитное заземление должно обеспечить безопасность людей от поражения электрическим током при взаимодействии с проводниками электрического тока.

Защитное заземление или зануление электроустановок следует выполнять:

1. При номинальном напряжении 380 В и выше переменного тока 440 В, и выше постоянного тока - во всех случаях.

2. При номинальном напряжении от 42 В до 380 В переменного тока и от 110 В до 440 В постоянного тока.

3. При работах в условиях с повышенной опасностью и особо опасных по ГОСТ 12.1.013-78.

Материал, конструкция заземляющих защитных проводников должны обеспечить устойчивость к механическим, химическим и термическим воздействиям

Для питания аппаратуры на предприятиях используется трехфазный ток напряжением 380-220В. В таком случае потенциал не должен превышать 125В [8].

Сопротивление высчитывается по формуле [6]:

$$R_з = 125/I_з, \quad (1)$$

где $R_з$ – сопротивление заземлителя.

$I_з$ – ток замыкания на землю.

Сопротивление не более 4 Ом.

По этой норме в эффективно заземленных сетях электробезопасность считается обеспеченной, если $\varphi \leq 10$ кВ и напряжение прикосновения и шага в любое время года не превышает допустимых значений ГОСТ 12.1.019 – 2017.

Оборудование использует напряжение 380/220В, следовательно, $R_з \leq 4$Ом ГОСТ 12.1.038 – 83. [7]

Значения сопротивления растекания заземлителя определяется путем инструментальных замеров примем $R_е = 19$ Ом.

Значение растекания искусственного заземлителя высчитывается по формуле: [6]

$$R_и = (R_е * R_з)/(R_е - R), \quad (2)$$

Проведем расчеты, где $R_з$ равен 4 Ом и $R_е$ равен 19 Ом, что в итоге получаем:

$R_и = (19*4)/(19–4) = 5{,}1$Ом.

Далее определим удельное сопротивление почвы согласно ГОСТ 12.1.030-81 для вертикальных заземлителей по формуле [6]:

$$\rho_{расч} = \rho_{изм} * \psi, \quad (3)$$

где ψ – коэффициент сезонности равный 1,3;

ρизм – сопротивление грунта (смешанный грунт) равен 100 Ом*м, используя данные значения произведем расчет удельного сопротивления грунта:

$\rho_{расч} = 100 * 1{,}3 = 130$ Ом*м.

Произведя расчет для вертикальных заземлителей по аналогии рассчитаем сопротивление горизонтальных заземлителей, из таблицы берем $\psi = 2{,}3$: [8]

$\rho_{расч} = 100 * 2{,}3 = 230$ Ом*м.

Далее мы определяемся с типом заземлителя. В данном расчете будем использовать стержневой электрод длиной l=2,1 м, диаметром d=0,1 м и глубиной заложения t= 0,7 метра. Верхние концы соединены с помощью горизонтального электрода – стальной полосы сечением 4х65 мм.

Далее определяем сопротивление одиночного вертикального заземлителя. Произведем расчет растекания сопротивления электродов для стержневого заземлителя круглого сечения в земле по формуле [6]:

$$R_в = (p/2\pi l)(\ln 21/d+(\ln(4t+l)/(4t-l))/2, \quad (4)$$

где: ρ – удельное сопротивление грунта при вертикальном заземлителе ρ=130 Ом.

$R_в$ = (130/2х3,14*2,1)(ln2*2,1/0,1+(ln(4*0,7+2,1)/(4*0,7-2,1))/2) ~81,7 Ом

Далее произведем расчеты сопротивления растеканию электродов для стержневого заземлителя в земле по формуле [6]:

$$R_г = (\rho/2\pi L)(\ln L2 /bt) \quad (5)$$

где: L – длина стальной ленты (которая укладывается на расстоянии 1,4м), L=45,5м.

Rг = (230 / 2 * 3,14 * 45,5)(ln 45,5*2 / 0,1 * 0,7) = 88 Ом.

При размещении электродов по периметру на расстоянии 1,4 м от каркаса здания, количество вертикальных электродов составляет n = 32 шт. на расстоянии 3 м друг от друга. Коэффициенты использования электродов составляют – для вертикального ηв = 0,73 для горизонтального - $\eta_г$ = 0,62.

Сопротивление растекания группового заземлителя по формуле [6]:

$$R = RвRг/(Rвηг+Rгηвn), \quad (6)$$

Получаем следующее значение:

R = 81,7 * 88/ (81,7 * 0,62+88 * 0,73 * 32) = 3,4 Ом.

В конце проверяем соблюдение необходимого условия $R_з \geq R$, следовательно, 4≥3,4, что дает нам возможность утверждать, что необходимое условие электробезопасности выполняется.

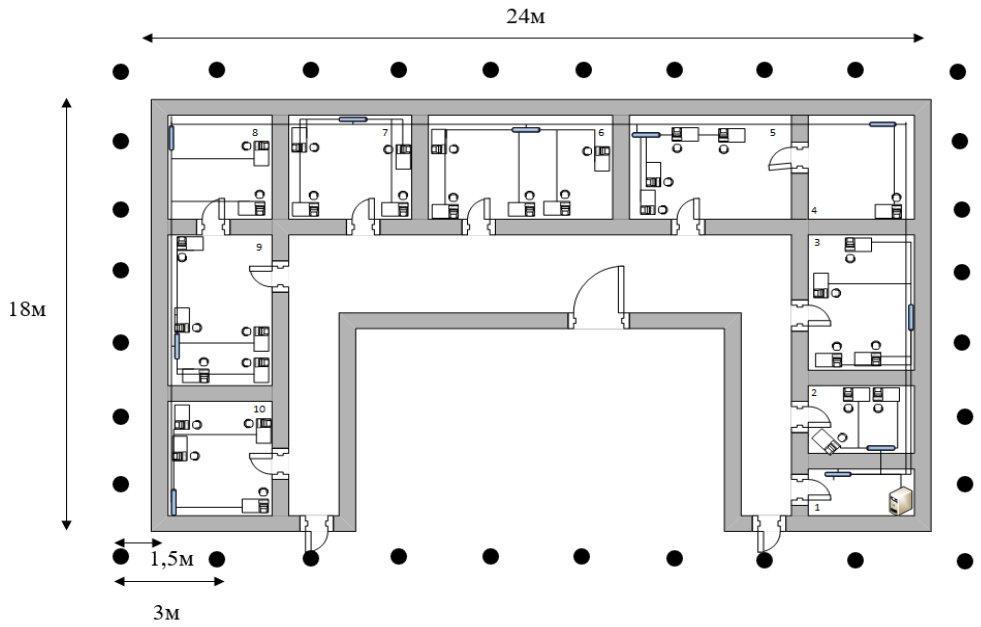


Рисунок 89 – Схема заземления офиса

4.3 Расчет допустимого уровня шума в офисе

Шум на рабочем месте оказывает раздражающее влияние на работника, повышает его утомляемость, а при выполнении задач, требующих внимания и сосредоточенности, способен привести к росту ошибок и увеличению продолжительности выполнения задания. Длительное воздействие шума влечет тугоухость работника вплоть до его полной глухоты.

Внезапные шумы высокой интенсивности, даже кратковременные (взрывы, удары и т.п.), могут вызвать как острые нейросенсорные эффекты (головокружение, звон в ушах, снижение слуха), так и физические повреждения (разрыв барабанной перепонки с кровотечением, поражения среднего уха и улитки).

Кроме общих требований, существуют критерии, применимые к конкретным видам работ, в зависимости от их содержания. Для офисных рабочих также рассчитаны свои показатели:

– для физической работы, требующей точности и аккуратности, воздействие не должно превышать 80 дБ.

– для творческих натур, руководящих должностей и персонала — не выше 50 дб.

– умственная деятельность, требующая слухового контроля и постоянной концентрации, не выше 65 дБ.

– создание новых программ, преподавательская деятельность — не свыше 40 дБ.

– деятельность, связанная сведением переговоров посредством телекоммуникации — не выше 55 дБ.

Основной характеристикой звукового поля является уровень его звукового давления L_p [18].

$$\text{Lp} = 20lg\frac{p}{p_0}db, \qquad (1)$$

где: p – эффективное звуковое давление дин/см^2,

p0 – 2 10-4 дин/см^2 (звуковое давление, принятое за нулевой уровень).

Уровень звукового давления, создаваемого отдельным вентилятором Ni обычно задается в характеристиках вентилятора. Параметр обозначается там как “Noise”.

Для этого значения по формуле (2) можно вычислить эффективное звуковое давление pi. Здесь Ni и pi параметры i-го источника шума, а i=1, 2, … n.

$$p_i = 10(\frac{N_i}{20})\, p_0, \qquad (2)$$

При расчете по формуле 2 получаем следующее значение:

$$p_0 = 2*10^{-4} \text{ дин/м}^2$$

Звуковое давление нескольких источников N суммируется по формуле (3). Поскольку в системном блоке все вентиляторы – источники шума расположены на расстоянии много меньшем контрольного расстояния для замера уровня шума (1м) можно считать, что формула (3) выполняется с достаточной точностью.

$$\text{Lp} = 20lg\frac{p_1+p_2+p_3}{p_0}db, \qquad (3)$$

где: P_1, p_2, p_3 – эффективное звуковое давление, его можно получить из (1) для каждого значения L_{p1}, L_{p2}, L_{p3}.

N – суммарный уровень звукового давления.

Рассчитаем сколько шума производят несколько компьютеров в одном помещении.

Допустим в отделе разработки 4 компьютера. Каждый из них находится в 50см друг от друга. Вентиляторы с уровнем шума 53дб, 46дб, 36дб, 19дб.

Вычисляем эффективное звуковое давление каждого по формуле (2).

$p_1 = 10(\frac{53}{20})*2*10^{-4} = 0.0053$ дин/м^2

$p_2 = 10(\frac{46}{20})*2*10^{-4} = 0.0046$ дин/м^2

$p_3 = 10(\frac{36}{20})*2*10^{-4} = 0.0036$ дин/м^2

$p_4 = 10(\frac{19}{20})*2*10^{-4} = 0.0019$ дин/м^2

В итоге выходит:

$p_{1+}\ p_{2+}\ p_{3+}\ p_4$= 0.0053+0.0046+0.0036+0.0019 = 0.0154 дин/м^2

По формуле (3) вычисляем результирующий уровень шума для этих вентиляторов.

$$\text{Lp} = 20lg\ \frac{0.0154}{2*10^{-4}} = 37.7\text{дб}$$

Теперь рассчитаем уровень звука в 9-часовой рабочий день.
Эквивалентный уровень звука за 9-часовой рабочий день L_{ex9h}, ДБ: Величина, используемая в целях нормирования и оценки шума на рабочем месте и определяемая как [8]

$$L_{ex9h} = L_p + 10[\frac{T_e}{T_0}], \quad (4)$$

где:Lp = 37.7,дБ.

T_e – эффективная длительность номинального рабочего дня (т.е. интервал времени, в течение которого наблюдается воздействие шума, существенного и представительного для данного рабочего места), час; Убрав обеденный перерыв и периодические выходы их помещения получится примерно 6 часов.

T_0 – базовая длительность рабочего дня, равная 9 часов.

L_{ex9h} = 37.7 + 10 $[\frac{6}{9}]$ = 44.4 дб.

Заключение

В ходе выполнения данной работы были выполнены все поставленные задачи по проектированию защиты Active Directory используя недокументированные возможности. Среди них создание и внедрение новой групповой политики для смены RDP-порта, настройка автоматизации процессов поиска старых документов, сбора данных учетных записей пользователей и поиска учетных записей с «вечным паролем», создание базы скомпрометированных паролей пользователей, разработка методики защиты от атаки направленной на получение кэшей паролей пользователей в AD посредством создание сертификатов для протокола LDAPS, и настройка групповых политик для запрета сохранения кэша паролей, настройка аудита на изменение членства в группах пользователей и новый способ поиска и удаления неактивных учетных записей.

Итогом реализации вышеперечисленных задач стали:

а) PowerShell-скрипты для автоматизации процесса сбора данных по пользователям, а так же по защите домена

б) Групповые политики для защиты домена

в) Метод защиты от атак на AD

Приложение А
Групповая политика на замену значения RPD-порта

```
    CLASS MACHINE
    CATEGORY SYSTEM\CurrentControlSet
        POLICY "RDP"
            KEYNAME
"SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp"
            PART PortNumber NUMERIC
                VALUENAME "PortNumber"
            END PART
        END POLICY
    END CATEGORY
```

Приложение Б

Скрипт на поиск документов, хранящихся в памяти больше 1.5 года

```
    $path = "C:\Users\"
            $limit = (Get-Date).AddDays(-548)
            Get-ChildItem $path -Recurse -Force |
Where-Object { !$_.PSIsContainer -and $_.CreationTime -
lt $limit } | Export-Csv c:\outfile.csv -Delimiter ';'
```

Приложение В

Скрипт для сбора данных по пользователям

```
ImportSystemModules ActiveDirectory
$Users = Get-ADUser -Filter * -Properties *
----------------------------------------
$UserCnt = $Users.Count
$Date = Get-Date -Format g
----------------------------------------
$UsrObj = @()
foreach ($user in $Users)
{
$usr = New-Object -TypeName PSObject -Property @{
"Canonical Name" = $User.CanonicalName
"SAM Account Name" = $User.SamAccountName
"Enabled" = if ($User.Enabled -eq $true){"Yes"}
else{"No"}
"Password Expired" = if ($user.PasswordExpired -eq
$true){"Expired"}else{"Not Expired"}
"Date Created" = $User.Created
"Last Logon" = $User.LastLogonDate
"Days Elapsed Since Last Logon" = if
($user.LastLogonDate -ne $null){if($User.lastLogon -ne
0){(new-
TimeSpan([datetime]::FromFileTimeUTC($User.lastLogon))
$(Get-Date)).days}else{0}}else{"Never Logged On"}
"Last Failed Logon" = $User.LastBadPasswordAttempt
"Account Age - Days" = (New-
TimeSpan([datetime]$User.createTimeStamp) $(Get-
Date)).Days
}
$UsrObj += $usr
}
$UsrObj|sort-object -property "Days Elapsed Since
Last Logon" -Descending|
ConvertTo-Html "Canonical Name","SAM Account
Name","Enabled","Password Expired","Date Created","Last
Logon","Days Elapsed Since Last Logon","Last Failed
Logon","Account Age - Days" -head $a -body
"<body><h2>Active Directory Users Last Login
Times</h2><p>Date: $date</p><p>User Count:
$UserCnt</p></body>"|
Out-File c:\Report.html
```

Приложение Г
Скрипт на поиск учетных записей с «вечным» паролем

```
Import-Module ActiveDirectory
# Получите все объекты пользователя в OU, отфильтруйте объекты в OU = ServiceAccounts (если у вас есть OU с учетными записями, которые могут иметь пароль с неограниченным сроком действия, хотя это не рекомендуется)
$Users = Get-ADUser -Filter * -SearchBase "OU=meloman.kz,DC=renard,DC=com" -Property PasswordNeverExpires,DisplayName,Description | Where {($_.DistinguishedName -notlike "OU=Users") -and ($_.PasswordNeverExpires -ne $false)} | Sort samAccountName
Write-Host $Users
# Скрипт вывода
$Output = $Users | ft samAccountName,DisplayName,Description,PasswordNeverExpires -Autosize -Wrap | Out-File c:\file.txt
```

Приложение Д

Скрипт для аудита изменения членства групп пользователей

```
$script:monitorServer = 'WIN-server'
function New-AdGroupMembershipMonitor {
    [OutputType('pscustomobject')]
    [CmdletBinding(SupportsShouldProcess)]
    param
    (
        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$GroupName,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [scriptblock]$Action,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [pscustomobject]$Schedule,

        [Parameter()]
        [ValidateNotNullOrEmpty()]
        [string]$Name   =   ("AD   Group   $GroupName
Monitor" -replace ' ', '_')
    )

    $ErrorActionPreference = 'Stop'

    $monitor =
$monitorStateFilePath = 'C:\ADGroupMembers.csv'
$previousMembers = $null
$previousMembers      =      Import-Csv      -Path
$monitorStateFilePath    |    Sort-Object    -Property
{[datetime]$_.Time} -Descending | Select-Object -First
1 | Select-Object -ExpandProperty Members

$previousMembers = $previousMembers -split ','

$currentMembers   =   Get-AdGroupMember   -Identity
'|GroupName|' | Select-Object -ExpandProperty name

$now = Get-Date -UFormat '%m-%d-%y %H:%M'
[pscustomobject]@{
    'Time'    = $now
```

```
        'Members' = $currentMembers -join ','
    }  |  Export-Csv  -Path  $monitorStateFilePath  -
NoTypeInformation -Append
    ## Compare and report
    if         (Compare-Object         -ReferenceObject
$previousMembers  -DifferenceObject  $currentMembers)  {
Action
    }
```

Продолжение приложения Д

```
        $monitor  =  $monitor  -replace  '\|Action\|',
$Action.ToString() -replace '\|GroupName\|', $GroupName
        $monitor = [scriptblock]::Create($monitor)

        $params = @{
            Name          = $Name
            Scriptblock   = $monitor
            Interval      = $Schedule.Interval
            Time          = $Schedule.Time
            ComputerName = $script:monitorServer
        }
        if ($Schedule.DayOfWeek) {
            $params.DayOfWeek = $Schedule.DayOfWeek
        }
        New-RecurringScheduledTask @params

    }

    function New-RecurringScheduledTask {
        [OutputType([void])]
        [CmdletBinding()]
        param
        (
            [Parameter(Mandatory)]
            [ValidateNotNullOrEmpty()]
            [string]$ComputerName,

            [Parameter(Mandatory)]
            [string]$Name,

            [Parameter(Mandatory)]
            [ValidateNotNullOrEmpty()]
            [scriptblock]$Scriptblock,

            [Parameter(Mandatory)]
```

```
            [ValidateNotNullOrEmpty()]
            [ValidateSet('Daily',  'Weekly')]  ##  Это
могут быть другие интервалы
            [string]$Interval,

            [Parameter(Mandatory)]
            [ValidateNotNullOrEmpty()]
            [string]$Time,

            [Parameter()]
            [ValidateNotNullOrEmpty()]
            [ValidateSet('Monday',           'Tuesday',
'Wednesday',    'Thursday',    'Friday',    'Saturday',
'Sunday')]
            [string]$DayOfWeek,

            [Parameter()]
```

Продолжение приложения Д

```
            [ValidateNotNullOrEmpty()]
            [pscredential]$RunAsCredential
        )

        $createStartSb = {
            param($taskName,    $command,    $interval,
$time, $taskUser)

            ## Создайте сценарий PowerShell, который
будет выполнять запланированное задание
            $scheduledTaskScriptFolder                =
'C:\ScheduledTaskScripts'
            if       (-not       (Test-Path       -Path
$scheduledTaskScriptFolder -PathType Container)) {
                $null      =      New-Item      -Path
$scheduledTaskScriptFolder -ItemType Directory
            }
            $scriptPath                                =
"$scheduledTaskScriptFolder\$taskName.ps1"
            Set-Content   -Path   $scriptPath   -Value
$command

            ## Create the scheduled task
            schtasks /create /SC $interval /ST $time
/TN  $taskName  /TR  "powershell.exe  -NonInteractive  -
```

```
NoProfile -File `"$scriptPath`"" /F /RU $taskUser /RL
HIGHEST
        }

        $icmParams = @{
            ComputerName = $ComputerName
            ScriptBlock  = $createStartSb
            ArgumentList            =            $Name,
$Scriptblock.ToString(), $Interval, $Time
        }
        if
($PSBoundParameters.ContainsKey('Credential')) {
            $icmParams.ArgumentList                  +=
$RunAsCredential.UserName
        } else {
            $icmParams.ArgumentList += 'SYSTEM'
        }
        Invoke-Command @icmParams

    }

    function Get-MonitorSchedule {
        [OutputType('pscustomobject')]
        [CmdletBinding(SupportsShouldProcess)]
        param
        (
            [Parameter(Mandatory)]
            [ValidateNotNullOrEmpty()]
            [ValidateSet('Daily', 'Weekly')]
```

Продолжение приложения Д

```
            [string]$Interval,

            [Parameter(Mandatory)]
            [ValidateNotNullOrEmpty()]
            [string]$Time,

            [Parameter()]
            [ValidateNotNullOrEmpty()]
            [ValidateSet('Monday',           'Tuesday',
'Wednesday',    'Thursday',    'Friday',    'Saturday',
'Sunday')]
            [string]$DayOfWeek
        )
        $ErrorActionPreference = 'Stop'
```

```
        [pscustomobject]@{
            Interval  = $Interval
            Time      = $Time
            DayOfWeek = $DayOfWeek
        }
    }
```

Приложение Ж

Скрипт на поиск и удаление неактивных учетных записей пользователей

```
    $remove_users_found = $false
    $today_object = Get-Date
    $today_string = get-date -Format 'MM-dd-yyyy hh:mm
tt'
    $unused_conditions_met = {
        ## Убедитесь, что ни один пользовательский
объект AD не был удален случайно
        !$_.isCriticalSystemObject -and
        ## Учетная запись отключена (учетная запись не
может быть использована)
        (!$_.Enabled -or
        ## Срок действия пароля истек (учетная запись
не может быть использована)
        $_.PasswordExpired -or
        ## Аккаунт никогда не использовался
        !$_.LastLogonDate -or
        ## Аккаунт не использовался в течение 60 дней
        ($_.LastLogonDate.AddDays(60)                -lt
$today_object))
    }
    $unused_accounts = Get-ADUser -Filter * -Properties
passwordexpired,lastlogondate,isCriticalSystemobject  |
Where-Object $unused_conditions_met |
        Select-Object
@{Name='Username';Expression={$_.samAccountName}},

@{Name='FirstName';Expression={$_.givenName}},
            @{Name='LastName';Expression={$_.surName}},
            @{Name='Enabled';Expression={$_.Enabled}},

@{Name='PasswordExpired';Expression={$_.PasswordExpired
}},
            @{Name='LastLoggedOnDaysAgo';Expression={if
(!$_.LastLogonDate) { 'Never' } else { ($today_object -
$_.LastLogonDate).Days}}},
            @{Name='Operation';Expression={'Found'}},
            @{Name='On';Expression={$today_string}}

    $unused_accounts | Out-File c:\file1.txt
    if ($remove_users_found) {
        foreach ($account in $unused_accounts) {
```

```
            Remove-ADUser       $account.Username       -
Confirm:$false
            Add-Content                                 -Value
"$($account.UserName),,,,,,Removed,$today_string"  -Path
c:\file1.txt
        }
    }
```

Список литературы

1. Скотт Калп «Десять непреложных законов управления безопасностью» URL:https://www.securitylab.ru/blog/personal/Informacionnaya_ bezopasnost_v_detalyah/324858.php (дата обращения: 27.02.2020).
2. Введения в основные понятия Active Directory URL: http://pyatilistnik.org/vvedenie-v-osnovnyie-ponyatiya-active-directory/ (дата обращения: 01.03.2020).
3. Лекция 10: Описание Active Directory URL: https://www.intuit.ru/studies/courses/1043/274/lecture/6937?page=5 (дата обращения: 01.03.2020).
4. Best Practices for Securing Active Directory URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory (дата обращения: 06.03.2020).
5. Робби Аллен Active Directory Сборник рецептов – СПб.: Питер, Киев: BHV, 2004- 590с.
6. Джек Козион, Крис Энли Искусство взлома и защиты систем СПб.: Питер, 2006- 416с.
7. Свен Шрайбер Недокументированные возможности Active Directory СПб.: Питер 2002 г.- 544с.
8. Александр Кенин Практическое руководство системного администратора 2-е издание СПб.: БХВ-Петербург, 2013. — 544 с.
9. Рэнд Моримото и др. Microsoft Windows Server 2012. Полное руководство 2013- 1456с.
10. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности, дата введения 2011-12-01.
11. Ефремова О.С. Документация по охране труда в организации. [Текст] Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с.
12. Ефремов О.С. Охрана труда в организации в схемах и таблицах. [Текст] / О.С. Ефремова 7-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2018 г. – 124 с.
13. СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений [Текст] / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.
14. СН 2.2.4/2.1.8.562-96. Санитарные нормы. Шум на рабочих местах, в жилых помещениях, общественных зданиях и на территории жилой застройки [Текст] / Санитарные нормы. -М.: Издательский центр Минздрава РФ. 1996. – 25 с.

15. СанПиН 2.2.4.3359-16 Санитарно-эпидемиологические требования к физическим факторам на рабочих местах [Текст] / М.: Информационно-издательский центр Минздрава Казахстана. 2016 – 47с.

16. ГОСТ Р 50571ю3-2009(МЭК 60363-4-41:2005. Электроустановки низковольтные. Требования для обеспечения безопасности. Защита от поражения электрическим током [Текст] / М.: Издательский центр Стандартинформ, 2009.-70 с.

17. ГОСТ 12.1.038-82. Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений и токов [Текст] / М.: ИПК издательство стандартов, 2001-15с.

18. ГОСТ 12.1.003-2014 Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности (Переиздание) 2015 – 26с.