

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

ДОПУСТИТЬ К ЗАЩИТЕ

Зам. декана по УР факультета СПО,

к. э. н.

должность, уч. степень, звание

Чернова 03.06.2024

подпись, дата

Н. А. Чернова

инициалы, фамилия

ДИПЛОМНЫЙ ПРОЕКТ

на тему Обеспечение защиты информации инфраструктуры факультета СПО ГУАП

выполнен

Кустовым Александром Михайловичем

фамилия, имя, отчество студента в творительном падеже

по специальности

09.02.06

код

Сетевое и системное администрирование

наименование специальности

Студент группы №

C042

[Подпись] 30.05.2024

подпись, дата

А. М. Кустов

инициалы, фамилия

Руководитель

Преподаватель

должность, уч. степень, звание

[Подпись] 30.05.2024

подпись, дата

И. В. Козлов

инициалы, фамилия

Санкт-Петербург 2024

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

УТВЕРЖДАЮ

Зам. декана по УР факультета СПО,

К. Э. Н.

должность, уч. степень, звание

Чернова

04.04.2024

подпись, дата

Н. А. Чернова

инициалы, фамилия

ЗАДАНИЕ НА ВЫПОЛНЕНИЕ
ДИПЛОМНОГО ПРОЕКТА

по специальности

09.02.06 Сетевое и системное администрирование

код, наименование специальности

студенту группы №

C042

Кустов Александр Михайлович

фамилия, имя, отчество

на тему

Обеспечение защиты информации инфраструктуры ФСПО ГУАП

утвержденную приказом ГУАП от

01.04.2024

№

11-435/24

1. Основные исходные данные

Минимальные требования к оборудованию и ПО:

Количество серверов – не менее 1

Количество клиентов – не менее 2

ПО для серверов – с системой отказоустойчивости и высокой производительностью, с системой безопасности

2. Перечень и примерное содержание обязательных разделов дипломного проекта

Введение

1 Теоретическая часть

1.1 Актуальность выбранной темы

1.2 Анализ предметной области

1.3 Описание структуры файлового хранилища и сети факультета

1.4 Выбор ОС и ПО

1.5 Постановка задачи

2 Проектная часть

2.1 Организация сетевого администрирования

2.2 Тестирование работоспособности файлового хранилища

Заключение

3. Задание на научно-библиографический поиск

1. Jordan Krause, Освоение Windows Server 2019: полное руководство для системных администраторов по установке, управлению и развертыванию новых возможностей в Windows Server 2019 / Jordan Krause. — Великобритания : Издательство «Packt», 2021. — 690 с. - ISBN: 978-1-8010-7934-1 . - Текст : электрон иный. - URL: <http://ieeexplore.ieee.org/document/10162898>

2. Thomas Lee, Руководство по автоматизации Windows Server 2019 с помощью PowerShell — третье издание: эффективные способы автоматизации административных задач Windows и управления ими, 3-е издание. / Thomas Lee. — Великобритания : Издательство «Packt», 2019. — 542 с. - ISBN 978-1-7898-0853-7. - Текст: электронный. - URL: <https://www.amazon.com/Windows-Server-Automation-PowerShell-Cookbook/dp/1789808537>

3. Orin Thomas, Windows Server 2019 “вдоль и поперек” 1-е издание / Orin Thomas. — Великобритания : Издательство « Microsoft Press», 2020. — 912 с. - ISBN 978-0-1354-9227-7. - Текст : электронный. - URL: <https://www.amazon.com/Windows-Server-2019-Inside-Out/dp/0135492270>

Срок сдачи дипломного проекта 30.05.2024 г.

Руководитель

03.04.2024

И.В. Козлов

должность, уч. степень, звание

подпись, дата

инициалы, фамилия

Задание рассмотрено на заседании цикловой комиссии

Вычислительной техники и
программирования

№ 11

от 04.04.2024

наименование цикловой комиссии

протокол №

дата

Председатель цикловой комиссии

Преподаватель

04.04.2024

И.Л.Рохманько

должность, уч. степень, звание

подпись, дата

инициалы, фамилия

Задание принял к исполнению

студент группы №

C042

05.04.2024




А.М. Кустов

подпись, дата

инициалы, фамилия

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1 Теоретическая часть	8
1.1 Актуальность выбранной темы.....	8
1.2 Анализ предметной области.....	10
1.3 Описание структуры файлового хранилища и сети факультета.....	13
1.3.1 Описание физического файлового сервера и компьютерной сети СПО ГУАП.....	17
1.3.2 Описание компьютерных лабораторий СПО ГУАП.....	20
1.4 Выбор операционной системы и ПО.....	21
1.4.1 Сравнение популярных семейств ОС	21
1.4.2 Выбор версии ОС Windows Server.....	24
1.4.3 Выбор программного обеспечения файлового сервера.....	25
1.5 Постановка задачи	27
2 Практическая часть.....	28
2.2 Организация сетевого администрирования.....	28
2.2.1 Подготовка сервера и клиентских ПК	28
2.2.2 Создание сценариев на PowerShell для развертывания файловой инфраструктуры и создания резервных копий.....	29
2.2.3 Автоматизация сценариев PowerShell на сервере	31
2.2.4 Создание графического приложения для организации подключения сетевых директорий.....	34
2.2.5 Создание графического приложения для смены пароля доменных пользователей.....	35
2.2.6 Конвертация пользовательских сценариев PowerShell в исполняемые файлы	36

<h3 style="margin: 0;">ДП.09.02.06.09ПЗ</h3>									
Изм.	Лист	№ докум.	Подп.	Дата	Обеспечение защиты информации инфраструктуры факультета СПО ГУАП Пояснительная записка	Лит.	Лист	Листов	
Разраб.		Кустов А.М.		30.09				4	55
Пров.		Козлов И.В.		30.09					
Н. контр.		Преснухина Ю.В.		30.09.24					
Утв.						ГУАП ФСПО			

2.2.7 Конфигурирование групповых политик для пользователей сетевого диска	38
2.3 Тестирование файловой инфраструктуры	40
2.3.1 Тестирование автоматического запуска задач в Диспетчере заданий.	40
2.3.2 Тестирование графических приложений для подключения пользовательских директорий и смены пароля	44
2.3.3 Тестирование работы групповой политики.....	49
ЗАКЛЮЧЕНИЕ	51
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	53
ПРИЛОЖЕНИЕ А. Файл SyncUsersAndGroups.ps1	
ПРИЛОЖЕНИЕ Б. Файл SyncSharedFolders.ps1	
ПРИЛОЖЕНИЕ В. Файл AssignUsersAccessRights.ps1	
ПРИЛОЖЕНИЕ Г. Файл BackupUsersData.ps1	
ПРИЛОЖЕНИЕ Д. Файл ConnectToNetDisk.ps1	
ПРИЛОЖЕНИЕ Е. Файл ChangePassword.ps1	

ВВЕДЕНИЕ

В современных условиях стремительного развития информационных технологий, увеличения объема обрабатываемых данных и повышения качества услуг Интернет-провайдеров вопрос хранения и защиты информации становится все более и более важным для образовательных учреждений и предприятий. Двенадцатый факультет среднего профессионального образования не стал исключением в данном вопросе.

Файловое хранилище – это специализированное программное обеспечение для хранения, защиты, управления и обмена файлами между пользователями хранилища, по средствам локальной сети или/и глобальной сети Интернет. Главной задачей большинства подобных программных решений является организация хранилища файлов пользователей в понятном для него формате. Естественно существуют и альтернативные файловые хранилища, главной задачей которых значится защита пользовательской информации или оптимизация занимаемого места на диске. Подобные файловые хранилища решают специфические задачи, изучение которых выходит за рамки данной дипломной работы [1].

Современные программные решения файловых хранилищ обладают разнообразной функциональностью и способны решать задачи разнообразной сложности. Большинство программных реализаций имеет как графический интерфейс, так и интерфейс командной строки для настройки параметров сервера или взаимодействия с его содержимым. Основным набором функций подавляющей части программного обеспечения является:

— управление доступом. Различные системы и методы аутентификации пользователей, а также контроль доступа на основе групп пользователей и мандатов,

— совместный доступ. Поддержка одновременного доступа нескольких пользователей к одним и тем же файлам, а также функции

блокировки файлов, предотвращающие конфликты при одновременном редактировании,

— единое место хранения данных. Оптимизация использования дискового пространства за счет функций дедупликации,

— сетевой доступ. Поддержка различных сетевых протоколов, например, NFS [2], SMB [3], FTP [4] для обеспечения доступа к данным с разных платформ, в том числе интеграция с облачными сервисами для гибридного хранения и синхронизации данных.

Целью данной дипломной работы является создание инфраструктуры контроля управления доступом к компьютерной информационной системе.

1 Теоретическая часть

1.1 Актуальность выбранной темы

Тема формирования, организации, модернизации подходов к защите информации пользователей становится все более актуальной для учебных заведений по всему Миру, в том числе и факультета СПО ГУАП. Сетевые файловые хранилища позволяют обмениваться информацией с коллегами, преподавателями, студентами и много кем ещё. Файловые хранилища предназначены для хранения различной информации.

Жесткие диски, на которых хранятся файлы, являются не очень надежными деталями в сервере, поэтому следует использовать технологию Redundant Array of Independent Disks (сокращено - RAID) [5]. Технология RAID используется для повышения надежности хранения данных и повышения производительности дисковой системы путем объединения нескольких физических дисков в единый логический диск.

На некоторых предприятиях есть необходимость в ограничении доступа к файлам пользователей посторонних лиц. Зачастую это условие также относится и к файловым хранилищам учебных заведений, ведь студенты постоянно копируют информацию друг у друга. Также проблема неограниченных прав доступа касается предприятий, которые работают с персональными данными своих пользователей, например, банки. Каждый день десятки тысяч клиентов посещают отделения банков и совершают различные операции, которые сопровождаются бумажным документом с персональными данными пользователей. Все документы сканируются и загружаются на корпоративное файловое хранилище, где круг лиц, имеющих доступ к подобным файлам, сильно ограничен. Престиж компании, особенно банка, сильно пострадает, если к файловому хранилищу, с персональными данными пользователей, получат доступ злоумышленники. Подобные происшествия снизят прибыль компании, что является недопустимым.

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№	докум.№	Подп.По		8

Разграничение прав доступа, создание пользовательских учетных записей, создание резервных копий файлового хранилища – все это отражает качество файлового хранилища. В большинстве компаний, в том числе и учебных заведений, файловое хранилище представляет собой общедоступный ресурс, к которому у всех пользователей есть неограниченный доступ. У каждого пользователя есть своя директория, в которой он хранит все необходимые для работы файлы. В подобных файловых инфраструктурах пользователи наделены соответствующими правами для редактирования чужих файлов. Конечно, коллеги или студенты редко портят чужие файлы нарочно, но подобные недостатки являются критическими для файлового хранилища.

Отсутствие пользовательских учетных записей делает невозможным отследить действия пользователей. На файловом сервере без учетных записей пользователи могут совершать любые операции с файлами и оставаться незамеченными. Критике подвергаются также сервисы без настроенных инструментов архивации данных. Подобные файловые хранилища, которые не защищены от аппаратных сбоев, способна вывести из строя любая поломка или ошибка в коде программного обеспечения. Потеря пользовательских данных является серьёзной технической проблемой, которая приводит к падению прибыли компании.

Перед файловым хранилищем факультета ГУАП не стоит задача сохранить персональные данные клиентов банка или файлы государственной важности. Это не отменяет того факта, что вышеперечисленные проблемы также актуальны для файловой инфраструктуры факультета. Прогресс не стоит на месте, поэтому стагнация области информационных технологий является плохим признаком. Пользователи файлового хранилища факультета создают все больше файлов каждый год, чаще обмениваются файлами друг с другом, так что модернизация и повышение требований к файловому хранилищу является абсолютно нормальным и естественным.

Актуальность выбранной темы также обосновывается тем фактом, что хранение файлов на сервере значитя крайне популярным среди пользователей глобальной сети Интернет по всему Миру. Создание файлового хранилища для факультета не только увеличит престиж учебного заведения, в глазах будущий студентов, но и даст возможность всем студентам и преподавателям факультета СПО хранить свои файлы на внутреннем сервере, без необходимости искать сторонние сервисы.

1.2 Анализ предметной области

К настоящему времени техническая реализация файлового хранилища, а также формат и тип данных, которые планируется хранить, играет ключевую роль при формировании задач по модернизации текущей инфраструктуры.

Файловые хранилища бывают разными, например, некоторые пользователи используют популярные социальные сети в роли файловых хранилищ [6]. Пользователи создают второй аккаунт в понравившейся им социальной сети и начинают переписку между двумя учетными записями: настоящим аккаунтом и только что созданным. Во многих социальных сетях есть возможность обмениваться файлами внутри переписки, чем подобные пользователи активно пользуются. Зачастую подобные решения не располагают большой квотой на размер файла, так как владельцам социальных сетей не выгодно хранить файлы пользователей, ограничения на размер файла составляет в среднем 2 ГБ. Из этого следует, что построить полноценную файловую вложенную структуру не получится: пользователям, в большинстве популярных социальных сетей, запрещено создавать директории в пределах переписки, загружать директории на сервис без архивации, загружать файлы с некоторыми расширениями, например, .exe и тому подобное. Также проблемой является управление доступом к файлам: крайне трудно предоставить общий доступ к информации пользователя, или наоборот – ограничить круг лиц, у которых есть допуск.

С похожими проблемами сталкиваются пользователи электронной почты. Некоторые клиенты почтовых сервисов создают второй почтовый ящик и пишут письма, с прикрепленными файлами, на него. Перечень проблем, с которыми сталкиваются пользователи, аналогичен тому, что уже изложен выше. У пользователей электронных почтовых ящиков точно также существуют ограничения на размер файлов и др.

Два вышеизложенных примера описывают файловые хранилища, которые пользователи создают для личного использования. Зачастую, целью подобных технических решений является сохранение важных пользовательских файлов на дополнительном ресурсе, или/и синхронизация информации, например, с рабочего компьютера на домашний и наоборот. Зачастую, перед подобными техническими решениями не стоит задачи обмена файлами между большим кругом лиц.

Говоря о полноценных файловых хранилищах, стоит выделить готовые облачные решения. В основном, крупные и не очень компании предлагают создать учетную запись на ресурсе и получить в пользование небольшое свободное пространство. Компании как бы предлагают пользователю опробовать их сервис перед тем, как приобрести платную подписку для расширения объема свободного пространства [7].

На просторах глобальной сети Интернет можно найти сервисы с необычайно большим объемом свободного пространства, например, 100 ГБ бесплатно. Часто подобные ресурсы обладают крайне низкой пропускной способностью, примерно 100 Кбит/с. Занимаемое место на диске пользователя файлами исчисляется МБ и ГБ, поэтому сервисы с низкой пропускной способностью не пользуются большой популярностью: пользователи не готовы долго ждать, пока нужная им информация окажется на облачном хранилище. В основном, пользователи, и небольшие компании, готовы заплатить некоторую сумму денежных средств и получить готовое решение,

которое не требует знаний и навыков специалиста для обслуживания и поддержания сервиса в должном виде.

Некоторые пользователи не готовы хранить свои файлы на чужих серверах. Многие объясняют свою точку зрения тем, что никто не может гарантировать пользователям 100% конфиденциальность информации. Несмотря на то, что все компании убеждают своих клиентов об отсутствии закладок для просмотра файлов третьими лицами, никто не может сказать наверняка, имеют ли сотрудники подобных ресурсов доступ к пользовательской информации. Также никто не знает, как именно хранятся файлы пользователей на серверах компаний: используется ли шифрование данных при записи на диски компаний, кто имеет доступ к ключам шифрования, каковы шансы, что завтра взломают сервера компании и украдут файлы пользователей, а в случае взлома какие меры будут предприняты.

По этим причинам существуют проекты для создания своего собственного файлового хранилища, например, проект NextCloud [8]. Задачей данного проекта является упрощение создание локального файлового хранилища. Пользователю не нужно самостоятельно проектировать файловое хранилище, достаточно установить соответствующие программное обеспечение и запустить сервис. Это один из популярных примеров подобных проектов. По большей части подобные проекты создаются под ОС семейства Linux. Проект NextCloud является открытым, то есть любой желающий может прочитать исходные файлы и проверить программное обеспечение на наличие бэкдоров. В глобальной сети Интернет огромное количество подобных проектов с открытым исходным кодом: OwnCloud, Seafile, Syncany, FTPbox и многие другие [9]. Все эти решения объединяет открытый исходный код, необходимость в ручной конфигурации и наличие выделенного сервера или виртуальной машины для работы сервиса.

1.3 Описание структуры файлового хранилища и сети факультета

На сегодняшний день в стенах учебного заведения ФСПО ГУАП существует инфраструктура, которая позволяет студентам и преподавателям хранить критически важные для них файлы, организован доступ к файлам практически из любой аудитории. Основными проблемами нынешней инфраструктуры являются:

- отсутствие прав доступа,
- отсутствие единой логической структуры,
- отсутствие автоматического обновления файловой инфраструктуры,
- отсутствие возможности восстановления удаленных файлов и каталогов,
- отсутствие доступа к файловому хранилищу за пределами локальной сети,
- отсутствие доступа к файловому хранилищу, через беспроводную сеть WI-FI.

Пользователи сетевого файлового хранилища имеют неограниченные права доступа ко всем файлам на ресурсе, то есть любой желающий может прочитать, изменить, исполнить или вовсе удалить файл, который даже не принадлежит ему. Пользователи, в частности студенты, зачастую хранят на файловом сервере свои отчеты за весь семестр, курсовые проекты, архивы учебных проектов и многое другое, что имеет непосредственную связь с учебным процессом и итоговыми результатами обучения. Отсутствие средств защиты и контроля доступа способствует несанкционированному копированию информации пользователей друг у друга.

Отсутствие возможности ограничения на доступ к файлам, в том числе, негативно воздействует и на рабочий процесс преподавателей. Например, преподаватель не может хранить файлы с экзаменационными билетами на общем файловом хранилище, ведь высока вероятность, что студенты найдут

данные файлы. При этом найти виновного является крайне сложной задачей - все студенты посещают файловое хранилище, используя анонимную учетную запись. Из этого следует, что определить злоумышленника возможно только по записям с камер видеонаблюдения. Во многом из-за этого большинство студентов и преподавателей факультета СПО ГУАП пользуются сторонними сетевыми хранилищами.

Отсутствие прав доступа к файловым ресурсам, как и отсутствие единой иерархической структуры файлового хранилища негативно влияют на эффективность труда пользователей. Каждый рабочий день пользователи файлового хранилища обмениваются сотнями файлов, используя файловые хранилища учебного заведения. При работе с сетевым файловым хранилищем все пользователи руководствуются своей собственной интуицией, и через определенный момент времени файловая инфраструктура превращается в огромную “помойку”. Пользователи не готовы мириться с данными проблемами, поэтому многие используют сторонние файловые хранилища, которые могут обеспечить соответствующий уровень сохранности данных, конфиденциальность и удовлетворительное время на поиск необходимого документа. Зачастую студенты и преподаватели предпочитают использовать собственные флэш-накопители, реже используют сторонние облачные файловые хранилища. Данная проблема также актуальна и для лабораторий с локальными сетевыми хранилищами.

Еще одной проблемой текущей файловой структуры является отсутствие возможности оперативно найти нужный файл на файловом хранилище. Зачастую файлы расположены не в интуитивно понятной директории, большая часть директорий имеет названия, которые не отражают действительности. Например, в директории “soft”, на сетевом диске “М”, можно найти не только программное обеспечение, но также образы различных ОС в формате “.iso”, или файлы с методическими указаниями можно найти в директории преподавателя, а можно в каталоге старосты группы. К

сожалению, структура файлов и директорий сетевого хранилища зависит не от внутрикорпоративных правил пользования, которые а от предпочтений пользователей.

Любые изменения, даже те, которые обладают некоторой периодичностью, производятся в ручном режиме. Например, в начале каждого учебного года в файловом хранилище факультета СПО создаются отдельные директории для каждой группы первокурсников. Внутри директорий групп создаются директории студентов, в качестве названия выступают фамилия и имя обучающегося. Все вышеперечисленные действия совершаются в ручном режиме студентами и\или кураторами групп. Важно уточнить, что каждый год студенты не только поступают на факультет СПО, но и отчисляются с него. Неактуальные директории удаляют, но это происходит не всегда своевременно и крайне хаотично. Лучше дела обстоят в тех компьютерных лабораториях, где заведующие самостоятельно контролируют свои файловые хранилища. Данное явление объясняется тем, что локальными файловыми хранилищами лабораторий, зачастую, пользуется меньший круг лиц.

Ручная работа постоянно сопряжена с человеческим фактором: системный администратор может, по невнимательности, удалить директории группы студентов, которые еще не окончили свое обучение на факультете СПО.

Любые манипуляции с файлами пользователей являются необратимыми: общее файловое хранилище колледжа не предусматривает восстановление утраченных файлов и директорий. Эта проблема особенно важна, ведь отсутствие ограничений на доступ к ресурсам сетевого хранилища позволяют удалить\изменить местоположение файла или целой директории любому пользователю. Автор диплома лично столкнулся с данной проблемой на втором курсе: часть файлов, относящихся к отчету по курсовому проекту, была перемещена в директорию студента другой группы.

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№ докум.	№	Подп.По		15

В начале каждого семестра всех студентов предупреждают, что файловые хранилища в колледже, особенно общее файловое хранилище, крайне не надежное место для хранения данных: любой желающий может удалить вашу директорию, или, если жесткий диск выйдет из строя и вся информация на нем уничтожится. Естественно такой подход к реализации файлового хранилища не допустим.

Отсутствие точек восстановления негативно сказывается на доверии студентов и преподавателей учебного заведения к общему файловому хранилищу колледжа: никто не готов рисковать своей информацией, а тем более рабочим местом или итоговой оценкой за семестр.

Поскольку доступ к файловому хранилищу, извне компьютерных аудиторий, учебного заведения не предусмотрен, пользователи вынуждены дублировать файлы на внешний носитель, дабы продолжить работу за пределами факультета СПО. Также пользователям приходится обмениваться информацией, в том числе и на аудиторных занятиях, используя сторонние файлообменники, например, Облако Mail.ru, Яндекс Диск или Google Drive. Данная проблема стояла особенно остро во время пандемии: каждый преподаватель организовывал учебный процесс со студентами так, как ему было удобно. Это вносило некоторую путаницу и несобранность в учебный процесс.

Данная проблема также актуальна для локальных сетевых файловых хранилищ в компьютерных лабораториях. Ни одна файловая инфраструктура недоступна извне, все зона покрытия ограничивается локальной сетью лаборатории. Данное утверждение относится и к тем лабораториям, которые оборудованы беспроводными точками доступа WI-FI [10]: стены факультета СПО достаточно толстые, поэтому уровня сигнала не всегда хватает для комфортной работы с файловым хранилищем за пределами лаборатории.

На данный момент, в факультет СПО сложилась ситуация, при которой файловое хранилище доступно не всем учащимся, например, пользователи мобильных устройств и ноутбуков “отрезаны” от своих файлов. В локальной сети факультета не предусмотрено использование беспроводной сети WI-FI для работы с файловым хранилищем. Чтобы загрузить файлы на общее сетевое хранилище, пользователь вынужден дублировать информацию на внешний носитель, а после - копировать его на файловый сервер.

Аналогичная ситуация и в компьютерных лабораториях с локальным файловым хранилищем. Конечно, в некоторых лабораториях, которые оборудованы точкой доступа и локальным файловым хранилищем, есть возможность использовать файловое хранилище по беспроводному каналу связи, но данный функционал реализован только в лаборатории “Разработки программ для мобильных устройств”.

1.3.1 Описание физического файлового сервера и компьютерной сети СПО ГУАП.

На сегодняшний день сеть СПО ГУАП оборудована одним физическим сервером, который выполняет следующие функции внутри сетевой инфраструктуры факультета СПО:

- контроллер доменной структуры Active Directory домена “stdm2.local”,
- роль DNS сервера,
- роль DHCP сервера,
- роль сетевого файлового хранилища [11].

Физический сервер работает под управлением серверной ОС Microsoft Windows Server 2012 R2 Datacenter. Сервер установлен в отдельном помещении именуемой серверной комнатой. Сервер имеет следующие аппаратные характеристики:

- центральный процессор Intel core I7-2600K 3400 МГц на 4 ядра,

— оперативная память 16 ГБ DDR3-1333 двумя планками по 8 гигабайт от компании ADATA,

— твердотельный SATA накопитель Kingston A400 на 256 ГБ,

— жесткий диск WD Black7200 об/мин на 500 ГБ.

Локальная сеть факультета соединяет компьютеры учебных лабораторий, компьютеры преподавателей, а также компьютеры в некоторых преподавательских кабинетах. В каждой учебной лаборатории, где расположены компьютеры, установлен отдельный неуправляемый коммутатор. От коммутаторов, установленных, в кабинетах проложен кабель, подключенный в управляемый коммутатор на лестничной клетке.

На пятом этаже установлен сетевой шкаф, в котором расположен управляемый коммутатор с настроенными VLAN-интерфейсами [12]. Доступ к управляемому коммутатору и маршрутизатору имеет только группа системных администраторов главного корпуса ГУАП. Управляемый коммутатор подключен в единый пограничный маршрутизатор факультета, который находится в серверной комнате на четвертом этаже.

Пятый этаж факультета СПО является самым крупным по количеству компьютерных лабораторий, так что вопрос защиты информации самый приоритетный, поэтому дипломный проект следует реализовать именно на нем.

Доступ к глобальной сети Интернет ограничен для пользователей на всех компьютерах в аудиториях, кроме ПК в преподавательских кабинетах. Доступ в глобальную сеть Интернет осуществляется по заявке только от преподавателя системному администратору факультета, поэтому студенты ограничены в использовании сторонних сервисов, например, файловых хранилищ или систем контроля версий, которые размещены за пределами локальной сети факультета СПО.

Важно отметить, что преподаватели также ограничены в использовании глобальной сети Интернет, так как преподавательские компьютеры в

лабораториях не имеют выделенного канала связи, а подключены в общий коммутатор со студенческими компьютерами. Постоянное подключение в глобальную сеть Интернет на преподавательских компьютерах не организовано.

Также, в компьютерных лабораториях преподавательские компьютеры не оборудованы беспроводным интерфейсом WI-FI, поэтому не все преподаватели могут использовать мобильную точку доступа сотового телефона для взаимодействия со сторонними сервисами в глобальной сети Интернет.

Необходимо отметить, что не во всех преподавательских кабинетах есть достаточное количество персональных компьютеров, из-за чего, периодически, образуются небольшие очереди из преподавателей на перерывах между парами. В некоторых аудиториях, например, кабинет №523 “Кабинет информатики и информационных технологий”, преподавательский компьютер установлен, но к локальной сети факультета СПО он не подключен.

На рисунке 1 изображена схема локальной сети компьютеров на пятом этаже факультета СПО.

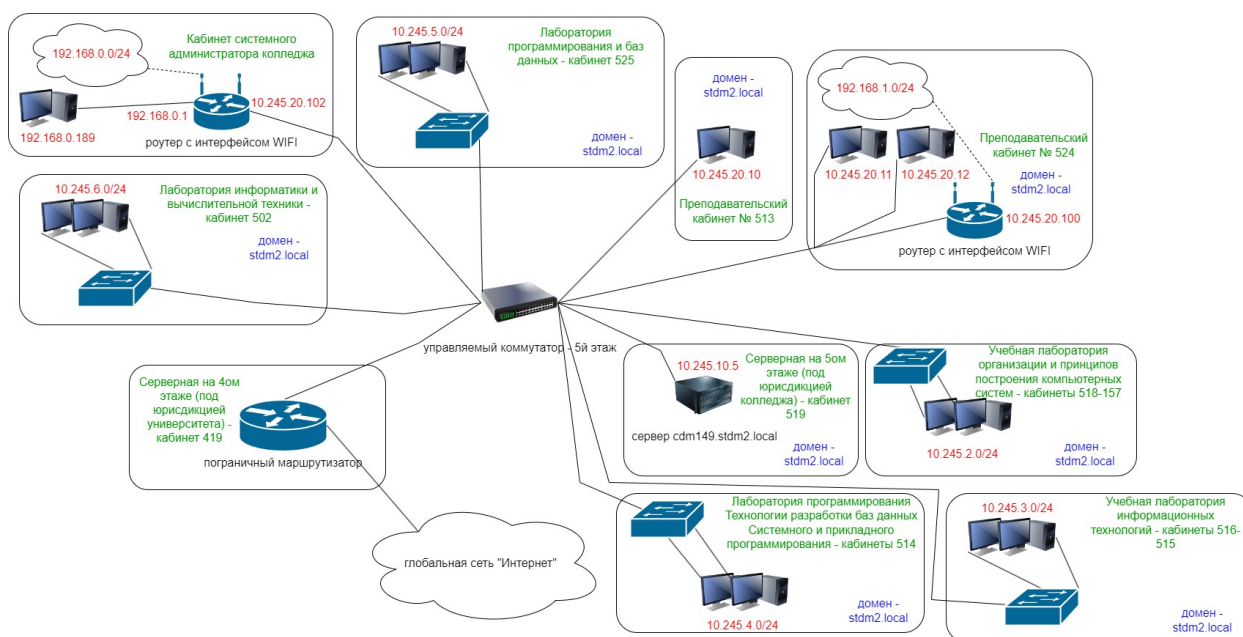


Рисунок 1 – Схема сети пятого этажа факультета

На рисунке 1 отражены все кабинеты, лаборатории и прочие помещения, в которых находятся компьютеры, подключенные к локальной сети факультета на пятом этаже. Все конечные устройства подключены либо в управляемый коммутатор на лестничной площадке, либо в неуправляемый коммутатор внутри помещения лаборатории, либо в пограничный маршрутизатор лаборатории.

1.3.2 Описание компьютерных лабораторий ФСПО ГУАП.

Компьютерные лаборатории Информатики и вычислительной техники, Программирования и баз данных, Учебной лаборатории информационных технологий, Учебной лаборатории организации и принципов построения компьютерных систем и Лаборатория программирования технологии разработки баз данных системного и прикладного программирования находятся в общем домене факультета - stdm2.local. Во всех вышеперечисленных лабораториях организован доступ к общему сетевому хранилищу ФСПО ГУАП. В каждой лаборатории есть возможность заказать доступ к глобальной сети Интернет.

На всех пользовательских компьютерах, которые находятся в домене stdm2.local, используются сетевые профили. Для каждой аудитории используется свой сетевой профиль, например, для учебного кабинета Программирования и баз данных перемещаемый профиль - user525, где 525 это номер аудитории.

После того, как пользователь выходит из системы сетевой профиль удаляется с жесткого диска ПК, а при начале нового сеанса эталонная копия загружается с контроллера домена cdm149.stdm2.local. Все настройки необходимые настройки уже произведены, так что пользователи могут начать работать сразу после окончания загрузки профиля. Данный тезис применим ко всем компьютерным аудиториям в составе домена stdm2.local.

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№ докум.	№	Подп.По		20

В качестве коммутирующего устройства действует неуправляемый коммутатор TP-Link TL-SG1024D на 24 порта с пропускной способностью 100 или 1000 мбит/с на каждый порт. Данная модель установлена во всех компьютерных аудиториях, где это необходимо согласно рисунку 1.

В учебных лабораториях, на пятом этаже факультета СПО ГУАП, есть выделенные рабочие места для преподавателей. Компьютеры для преподавателей, зачастую, не отличаются по своим аппаратным и программным возможностям от студенческих рабочих мест. Все отличия ограничиваются разным объемом оперативной памяти, так как преподавателям необходимо запускать куда больше программ для проведения занятий или практических работ.

На пятом этаже факультета расположена библиотека, где любой желающий может выйти в глобальную сеть Интернет с локальных компьютеров. Важно отметить, что библиотека не является частью факультета, следовательно, доступ к общему файловому хранилищу с локальных компьютеров ограничен.

1.4 Выбор операционной системы и ПО

1.4.1 Сравнение популярных семейств ОС.

За последние 40 лет развития вычислительной техники появилось огромное количество ОС под любые задачи и аппаратные характеристики. На сегодняшний день самыми популярными являются ОС семейства Windows, UNIX и UNIX-подобные системы [13]. Для выполнения дипломной работы необходимо рассматривать ОС предназначенные для серверов, ведь в системах такого рода уделено особое внимание надежности и безопасности.

Системы на базе ядра UNIX [14] являются представителями самого долгоживущего семейства ОС в настоящий момент. К данному семейству ОС относятся такие популярные дистрибутивы систем как:

— BSD - Berkeley Software Distribution. BSD являлась основой для многих современных ОС и отличается своей стабильностью, безопасностью и производительностью. В настоящее время существует несколько усовершенствованных версий BSD, каждая из которых имеет свои особенности и области применения. Популярность данного дистрибутива падает, так как проект является проприетарным и не способен конкурировать с аналогами,

— FreeBSD является бесплатной реализацией ОС BSD и распространяется под свободной лицензией. Проект создавался как открытая и бесплатная альтернатива системе BSD, в остальном она очень похожа на ОС BSD: популярность проекта также уменьшается с каждым годом все больше. Существуют также и аналогичные проекты OpenBSD, NetBSD и др [15].

UNIX системы до сих пор используются на огромном количестве серверов и сетевого оборудования, к сожалению практически все проекты утратили свою актуальность и проектировать файловую инфраструктуру факультета СПО будет нецелесообразно.

Говоря об ОС UNIX-подобных систем необходимо отметить, что самым популярными проектами являются дистрибутивы, основанные на ядре Linux [16]. Он изначально создавался как свободная альтернатива коммерческим UNIX-системам с открытым исходным кодом, который поддерживается тысячами разработчиков до сих пор. ОС на базе ядра Linux можно встретить не только на домашних ПК, но и на высоконагруженных серверах, в системе управления умным домом и др. Далее будут представлены самые популярные серверные дистрибутивы Linux:

— CentOS — дистрибутив, основанный, на платном проекте Red Hat Enterprise Linux и полностью совместим с ним. Является одним из самых стабильных дистрибутивов, содержащий все необходимое ПО для работы сервера. Может использоваться как на домашнем ПК с графическим интерфейсом, так и на сервере с интерфейсом командной строки,

— Debian — стабильный, популярный дистрибутив Linux. Является самым старым, из списка популярных, проектов на данный момент. В основном используется на персональных ПК, но выполнения серверных задач он также рассчитан. Debian лежит в основе многих дистрибутивов, включая такой популярный проект как Ubuntu,

— Ubuntu Server считается одним из самых популярных и простых серверных дистрибутивов ОС на базе ядра Linux. Огромное количество инструкций и статей посвящено данному проекту, поэтому многие молодые системные администраторы начинают знакомство с Linux-системами именно с данной ОС [17].

Системы на базе ядра Linux становятся популярней с каждым годом не только среди системных администраторов, но и обычных пользователей. К сожалению, дистрибутивы Linux плохо взаимодействуют с системами Windows, которые все ещё являются лидерами рынка. Модернизация файловой инфраструктуры, которая была сформирована вокруг ОС семейства Windows, может обернуться сбоями в работе.

Уже несколько десятилетий компания Microsoft выпускает ОС Windows, которая является самой популярной среди системных администраторов и рядовых пользователей. Семейство систем Windows включает в себя подсемейство Windows Server, среди которого представлено несколько редакций ОС:

— Foundation. Самая минимально-доступная редакция системы, предназначенная для малого бизнеса с небольшой квотой на количество пользователей. Включает в себя базовые функции сервера, такие как файловые и печатные службы, но имеет серьезные функциональные ограничения по сравнению с другими редакциями,

— Essentials. Логическое продолжение редакции Foundation, рассчитанное на предприятия малого и среднего бизнеса. Имеет весь

функционал младшей редакции и увеличенную квоту на количество пользователей,

— Standard. С данной версии появляется возможность запускать виртуальные машины, также снимается ограничение на количество пользователей – теперь можно добавить неограниченное число новых учетных записей. Всего можно запустить две виртуальные машины, что является вполне приемлемым для компаний среднего размера,

— Datacenter. Редакция Datacenter рассчитана на крупные предприятия и дата-центры, которым большое количество виртуальных машин и масштабируемость. Эта версия предоставляет полный набор функций и возможностей Windows Server 2012 R2, а также неограниченные права на виртуализацию [18].

В ходе выбора семейства ОС в качестве серверной системы была выбрана Windows Server Standard. Данная редакция удовлетворяет всем требованиям колледжа и при этом не придется переплачивать за более дорогую лицензию.

1.4.2 Выбор версии ОС Windows Server.

На сегодняшний день существует несколько версий Windows Server, все они привязаны к году выпуска – 2003, 2008, 2012, 2016, 2019 и 2022. В каждой новой версии компания Microsoft дополняла свою ОС новыми функциями и совершенствовала уже имеющиеся. Самыми популярными и успешными версиями являются 2012, 2016, 2019, так как в них сочетается надежность, стабильность и широкий функционал для решения большинства задач.

Версии Windows Server 2016 и 2019 до сих пор включены в список актуальных ОС и получают обновления безопасности. Системы зарекомендовали себя среди системных администраторов, все больше серверов стараются перевести на одну из этих версий Windows Server. Также ОС имеют встроенную поддержку облачной платформы Microsoft Azure, это

является минусом для данного дипломного проекта, ведь в использовании сервиса Azure не необходимости, а лишних ресурсов у физического сервера нет.

Куда лучше обстоят дела у версии 2012 года: ОС Windows Server 2012 Standard поддерживает все необходимые службы и компоненты для поддержания современной сетевой инфраструктуры компании, например, работа в домене, DHCP и DNS сервера, SMB сервер и др. Версия прошла большую проверку временем – Windows Server 2012 до сих пор используется во многих компаниях, из чего следует, что система надежная и отказоустойчивая. К тому же аппаратные характеристики сервера слабые, так что ОС должна достаточно эффективно использовать ресурсы, чтобы выдержать рабочую нагрузку и не выйти из строя.

1.4.3 Выбор программного обеспечения файлового сервера.

В современных версиях ОС Windows Server есть возможность создать файловый сервер штатными средствами системы. Для этого необходимо всего лишь скачать и установить недостающие компоненты системы, а конкретней:

— Файловый SMB-сервер поддерживает работу с учетными записями и группами Active Directory, с помощью которой возможно наладить контроль доступа к информации пользователя. Данный пакет программного обеспечения не требует дополнительной оплаты: необходимо лишь скачать и установить службы сервера Файлового сервера и Диспетчера ресурсов,

— FTP-сервер Windows позволяет обмениваться файлами клиентам через интернет или локальную сеть, что делает его отличным вариантом для использования в глобальной сети Интернет. К сожалению, у данной службы нет интеграции с Active Directory и такого широкого спектра настроек контроля доступа, как в файловом SMB-сервере.

Говоря об альтернативном ПО для реализации файлового сервера, с контролем доступа, необходимо отметить, что достойных вариантов нет. Все

сторонние технические решения либо являются переносом с системы семейства Linux/UNIX систем, либо обладают слишком скудной функционалом. Главными недостатками подобных портированных решений является огромное количество ошибок в коде ПО и отсутствие систем взаимодействия с Active Directory.

В ходе исследования различных вариантов реализации файлового хранилища с контролем доступа был выбран штатный сервис файлового SMB-сервера. Данное ПО отлично взаимодействует с серверной ОС Windows Server 2012 R2 Standard и не требует дополнительных вложений [19].

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№ докум.	№	Подп.По	Дата	26

1.5 Постановка задачи

Информацию пользователей, хранящуюся на файловом хранилище факультета СПО ГУАП, необходимо защитить от несанкционированного доступа. Для достижения поставленной цели следует создать учетную запись под каждого пользователя файлового хранилища факультета СПО.

Учетные записи следует расположить в базе данных пользователей Active Directory по средствам скриптов на языке PowerShell [20]. ФИО, пол, курс, дата рождения и группа всех студентов факультета уже записаны в единый excel-файл, который следует конвертировать в формат .csv. В таком случае будет проще импортировать пользователей в скрипт.

Студенты поступают и отчисляются в течении года, следовательно было бы разумно автоматизировать процесс синхронизации пользователей с помощью утилиты Планировщик Задач. Данное ПО позволяет запускать программы в заранее определенное время и дату, используя привычный графический интерфейс.

Автоматизированное создание пользовательских директорий также не должно оставаться в стороне: формирования директорий, так же как и назначение прав на них, следует автоматизировать. Суть та же, что и с автоматическим созданием пользователей: PowerShell-скрипт добавляется в утилиту Планировщик Задач, далее раз в неделю все лишние директории будут удаляться, а все недостающие – создаваться. Также необходимо автоматизировать создание резервных копий файлов пользователей сетевого ресурса.

Пользователи должны иметь удобный интерфейс для подключения и отключения сетевых дисков, ведь при подключении к общему ресурсу ОС Windows Server 2012 R2 будет требоваться пароль. Также необходимо организовать простой способ сменить пароль без участия системного администратора. Для решения данных задач следует создать графические приложения на языке PowerShell в связке с библиотеками .NET [21].

2 Практическая часть

2.2 Организация сетевого администрирования

2.2.1 Подготовка сервера и клиентских ПК.

Информация о пользователях и группах факультета СПО хранится в формате электронных таблиц Excel, но для работы с файлами формата .xlsx необходимо установить программный пакет Microsoft Office, в составе которого содержатся соответствующие модули для языка PowerShell. К сожалению, на сервере sdm149 нет данного ПО, поэтому файлы баз данных факультета экспортируются в универсальном формате CSV [22]. Данная операция совершается с использованием программы Microsoft Excel, результат которой отображен на рисунке 2.

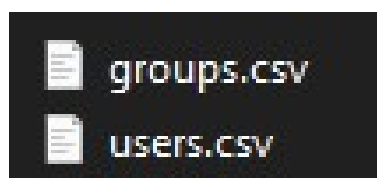


Рисунок 2 – Новые файлы с пользователями и группами в формате CSV

Все файлы сетевого ресурса хранятся в директории FSPOSUAI, которая расположена в корне диска C. Данная директория является общедоступной для всех пользователей домена, как изображено на рисунке 3. В противном случае использование сетевого ресурса не представляется возможным.

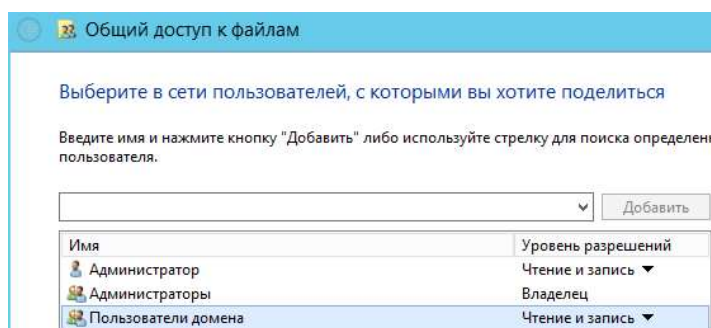
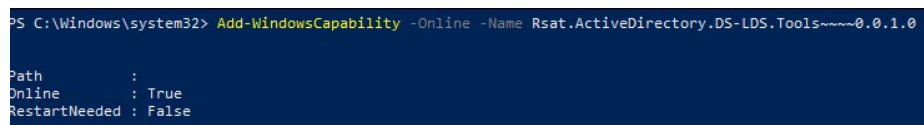


Рисунок 3 – Добавление пользователей в общий доступ

Смена пароля от учетной записи пользователя домена осуществляется через графическое приложение, в котором используются соответствующие модули Active Directory для взаимодействия с объектами домена на клиентском ПК. Данный модуль не является встроенным в ОС, поэтому необходимо установить его с помощью команды изображенной на рисунке 4



```
PS C:\Windows\system32> Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
Path :
Online : True
RestartNeeded : False
```

Рисунок 4 – Установка Rsat.ActiveDirectory.DS-LDS.Tools

Таким образом подготовлена файловая инфраструктура база данных пользователей и установлены всех необходимые модули на клиентских ПК, которые необходимы для дальнейшей работы.

2.2.2 Создание сценариев на PowerShell для развертывания файловой инфраструктуры и создания резервных копий.

Сценарий SyncUsersAndGroups.ps1, который представлен в приложении А, используется для синхронизации учетных записей пользователей в базе данных Active Directory с базой факультета СПО. В начале файла сценария содержится необходимый модуль PowerShell для корректной работы, а именно ActiveDirectory. С его помощью организована вся работа с пользователями и группами в домене на сервере.

Новые пользователи и группы импортируются из файлов баз данных формата .CSV в соответствующие переменные сценария через командлет Import-Csv. Все переменные, в которых хранятся записи баз данных факультета, являются объектами .NET.

Основной задачей сценария SyncSharedFolders.ps1, который представлен в приложении Б, является синхронизация групповых и пользовательских директорий в корневом каталоге FSPOSUAI с объектами домена Active

Directory. Все сведения о существующих пользователях и группах домена определяются в сценарии благодаря командам Get-ADGroup и Get-ADGroupMember, которые являются составной частью модуля ActiveDirectory.

С помощью сценария AssignUsersAccessRights.ps1 представленного в приложении В, распределяются права доступа на пользовательские и групповые директории в соответствии с объектами домена Active Directory. К студенческой директории доступ на создание\редактирование\просмотр файлов в пределах личной предоставляется для конкретного студента. В директории каждой группы существует общая папка для всех студентов группы с правами на создание\редактирование\просмотр файлов. Преподавателям дозволено не только создание\редактирование\просмотр файлов в рамках директории собственной группы, но также в директориях всех студентов.

Конфигурация прав доступа, в сценарии AssignUsersAccessRights.ps1, к общему файловому ресурсу реализована с использованием стороннего модуля PowerShell – NTFSSecurity [23]. Модуль не является встроенным в окружение PowerShell по умолчанию, поэтому его необходимо отдельно скачать из глобальной сети Интернет.

В двух файлах сценариев AssignUsersAccessRights.ps1 и SyncUsersAndGroups.ps1 используется командлет Compare-Object, с помощью которого производится сравнение база данных пользователей\групп факультета и объектов домена Active Directory. Основными параметрами данного командлета являются ReferenceObject – определяет эталонный массив объектов, и DifferenceObject – ссылается на массив объектов, который сравниваются с эталонным. Образцовым массивом является база данных факультета СПО, а сравниваемым с ним – массивы с пользователями и группами Active Directory.

Сценарий BackupUsersData.ps1 предназначен для создания резервных копий всех файлов и директорий общего сетевого ресурса пользователей факультета СПО. Основным компонентом сценария является класс .NET

System.IO.Compression.FileSystem, благодаря которому данные сжимаются в zip-архив. В качестве уникального имени архива используется метка даты и времени для генерации уникального имени. Листинг сценария размещен в приложении Г.

Таким образом, составлены файлы сценариев PowerShell для синхронизации пользователей Active Directory с базой данных факультета, синхронизация групповых и пользовательских директорий, выдачи соответствующий прав доступа и сценарий создания резервных копий.

2.2.3 Автоматизация сценариев PowerShell на сервере.

ОС Windows Server 2012 R2 Standard оснащена встроенной утилитой Планировщик заданий. Данная утилита используется для автоматизации запуска PowerShell сценариев SyncUsersAndGroups.ps1, AssignUsersAccessRights.ps1 и BackupUsersData.ps1 с привязкой к определенному времени. Все сценарии необходимо последовательно запускать раз в сутки в период с 01:00-03:20 утра, ведь изменение в базе данных факультета может произойти в любой рабочий день. На рисунке 5 изображен один из возможных способов запуска утилиты.

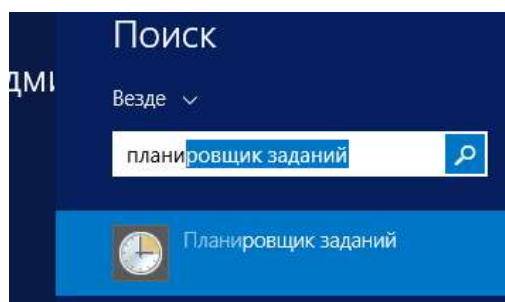


Рисунок 5 – Запуск планировщика заданий

В открывшемся окне утилиты создаем новую задачу для запуска сценария PowerShell SyncUsersAndGroups, представленную в приложении А. Во вкладке Общие указываем имя задачи, описание, в области Параметры

безопасности включаем пункт Выполнять с наивысшими правами и выбираем запуск программы для всех пользователей, как показано на рисунке 6.

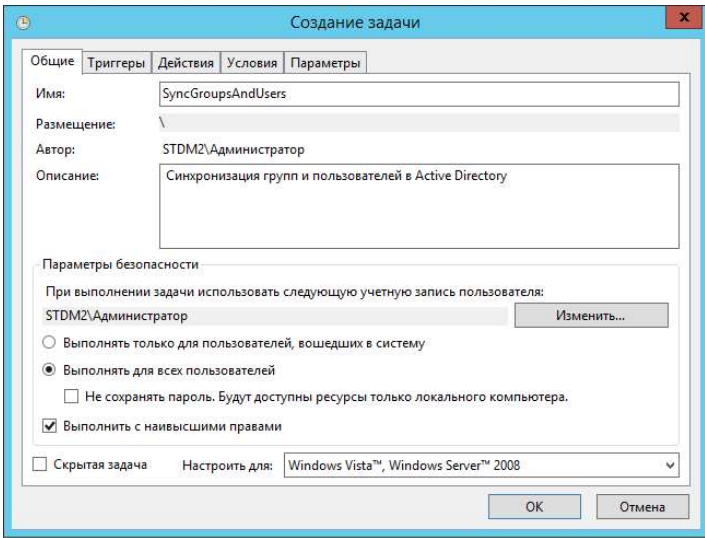


Рисунок 6 – Вкладка Общее в окне создания задачи

Флажок Выполнять с наивысшими правами позволяет избежать проблем с недостатком прав на выполнение сценария. Во вкладке Триггеры нажимаем кнопку Создать и настраиваем параметры таймера для запуска задачи, как на рисунке 7.

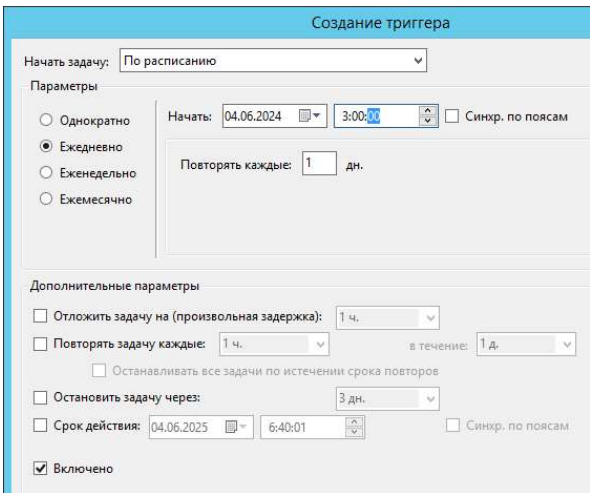


Рисунок 7 – Настройка триггера для задачи

Во вкладке Действия нажимаем кнопку Создать и настраиваем параметры запуска сценария, как это изображено на рисунке 8.

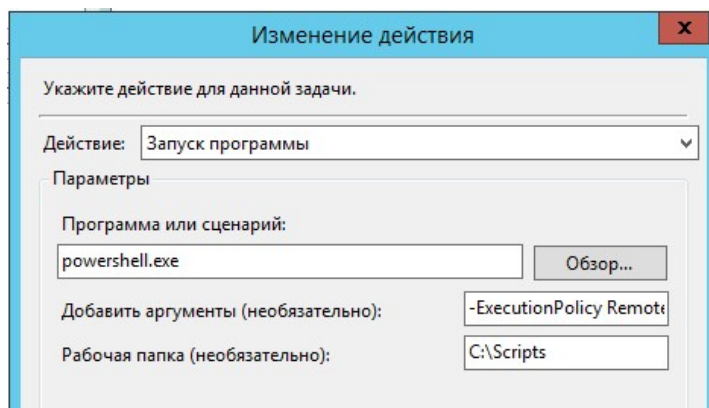


Рисунок 8 – Изменение действия задачи

В параметрах действия указываются дополнительные аргументы для запуска сценария – -ExecutionPolicy RemoteSigned -File "C:\Scripts\SyncUsersAndGroups.ps1" и C:\Scripts. Таким образом, задается политика выполнения сценариев и рабочая директория. На этом данном этапе создание новой задачи считается оконченной.

Для двух других сценариев SyncSharedFolders.ps1 и AssignUsersAccessRights.ps1 создано две аналогичные задачи с привязкой ко времени. Разница во времени запуска – 10 минут относительно каждой следующей задачи. Для сценария PowerShell BackupUsersData временной меткой триггера является 01:00 ночи, так как процесс создания резервной копии запускается до процессов синхронизации групп и пользователей. Итогом создания задач в утилите Планировщик заданий является три задачи, которые изображены на рисунке 9.

Файл	Сост...	Триггеры
BackupUsersData	Готово	В 1:00 каждый день
SyncGroupsAndUsers	Готово	В 3:00 каждый день
SyncSharedFolders	Готово	В 3:10 каждый день
AssignUsersAccessRight	Готово	В 3:20 каждый день

Рисунок 9 – Задачи в Планировщика заданий

Таким образом, настроен автоматический запуск сценариев PowerShell для синхронизации групп, пользователей, пользовательских и групповых директорий, а также назначения прав доступа для пользователей и групп.

2.2.4 Создание графического приложения для организации подключения сетевых директорий.

Все пользователи используют общую учетную запись компьютерной аудитории, поэтому идентифицировать человека необходимо после начала работы за ПК. Для решения данной задачи используется сценарий PowerShell ConnectNetDisk.ps1 с графическим интерфейсом, который реализован с помощью библиотек .NET. Все содержимое сценария файла ConnectNetDisk.ps1 представлено в приложении Г.

Основным командлетом сценария подключения\отключения сетевых ресурсов является New-SmbMapping [24]. Через его параметры есть возможность передать не только название общего ресурса, но и имя пользователя, его пароль, а также букву нового сетевого диска.

В связи с тем, что процесс аутентификации и подключения сетевых ресурсов связан с появлением ошибок, весь связанный код находится в логической конструкции PowerShell – try/catch. Данная конструкция предназначено для обработки ошибок и исключений, что позволяет более гибко настроить поведение программы. При возникновении ошибки подключения к сетевому ресурсу пользователю выводится соответствующее сообщение, аналогично при успешном\неудачном отключении\подключении сетевого ресурса.

Функционал графического интерфейса приложения позволяет отсоединять сетевой ресурс без перезагрузки ПК и\или выхода из пользовательской учетной записи, а затем подключить сетевую директорию другого пользователя.

Для реализации графического интерфейса используется библиотека классов .NET, встроенная в ОС Windows 10. Импорт библиотек осуществляется с помощью командлета Add-Type.

Таким образом, графическое приложение для обработки пользовательских запросов на подключение и отключение сетевых ресурсов готово к эксплуатации в локальной сети факультета СПО.

2.2.5 Создание графического приложения для смены пароля доменных пользователей.

Пользовательские учетные записи в домене Active Directory создаются с одинаковым паролем P@ssw0rd, что является серьезной уязвимостью в системе, поэтому пользователям доступа программа для смены пароля учетной записи домена. Для смены пароля используется приложение с графическим интерфейсом, написанным с использованием библиотек классов .NET.

Работа с объектами доменной структуры Active Directory за пользовательским ПК требует дополнительных пакетов PowerShell - Remote Server Administration Tools (с англ. Инструменты удаленного администрирования сервера), а конкретнее компонент ОС Windows отвечающий за взаимодействие с объектами домена. Для установки данного компонента необходимо запустить команду PowerShell Add-WindowsCapability -Online -Name Rsat.Active Directory.DS-LDS.Tools~~~0.0.1.0 с правами администратора ОС.

Основным командлетом, вокруг которого выстроен весь функционал файла сценария ChangePassword.ps1, является Set-ADAccountPassword. Данный командлет создан таким образом, что для смены пароля требуется указать не только новый, но и старый пароли, благодаря чему возможно исключить посторонних лиц из процесса смены пароля и несанкционированного изменения со стороны других пользователей. В том

случае, если пароль от учетной записи утерян, то доступ возможно вернуть обратившись к системному администратору. О номере кабинета пользователя сигнализирует соответствующее сообщение, в случае возникновения ошибки. Полный листинг кода сценария размещен в приложении Д.

Таким образом, графическое приложение для смены пароля пользователя от учетной доменной записи готово к дальнейшей эксплуатации в локальной сети факультета СПО.

2.2.6 Конвертация пользовательских сценариев PowerShell в исполняемые файлы.

Приложения с графическим интерфейсом, написанные на языке PowerShell запускаются только в соответствующей оболочке. Пользователям не следует давать доступ на редактирование, а тем более исполнение отредактированных файлов сценариев PowerShell, особенно если это связано с работой данными учетных записей пользователей. Оптимальным решением данной задачи является конвертация файлов сценариев в исполняемые файлы, например, формата .exe.

Штатными инструментами оболочки PowerShell произвести конвертацию файлов не представляется возможным, поэтому необходимо скачать стороннее ПО для решения данной задачи. ISESteroids [25] - это среда разработки сценариев PowerShell, разработанная компанией Dr. Tobias Weltner. Одной из основных функций данного ПО является конвертация файлов .ps1 в исполняемый ОС .exe формат.

Установка соответствующего модуля осуществляется командой `Install-Module -Name ISESteroids`. После успешной установки следует запустить ISESteroids командой `Start-Steroids` и открыть файл `ConnectNetDisk.ps1` → вкладка Сервис → Функция Turn Code into EXE... и начать процесс конвертации в .exe, как показано на рисунке 10.

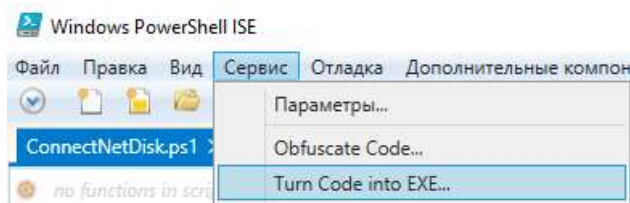


Рисунок 10 – Запуск конвектора кода PowerShell

Внешний вид приложения - только графический интерфейс, в дополнительных настройках необходимо указать полный путь до иконки программы, как показано на рисунке 11.

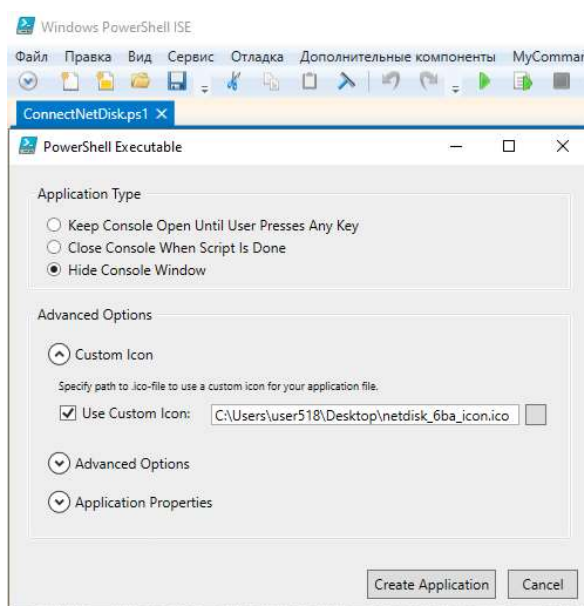


Рисунок 11 – Конвертация сценария PowerShell в исполняемый файл

Далее указываем полный путь до исполняемого файла, и на этом процесс конвертации можно считать оконченным. Аналогичные действия нужно произвести с файлом сценария ChangePassword.ps1, чтобы создать второй исполняемый файл для нужд пользователей файлового хранилища.

Таким образом, графические приложения для смены пароля пользователя от учетной доменной записи и подключения\отключения сетевого ресурса конвертированы в исполняемые файлы Windows для дальнейшей эксплуатации в локальной сети факультета СПО.

2.2.7 Конфигурирование групповых политик для пользователей сетевого диска.

Работа с сетевыми дисками в ОС Windows 10 организована таким образом, что при выходе из системы или перезагрузке ОС все подключения сетевых ресурсов сохраняются. Пользователи не всегда отключают сетевые ресурсы по окончании работы за ПК, поэтому задана соответствующая политика на запуск сценария PowerShell, которая принудительно отключает все сетевые ресурсы от компьютера.

Для конфигурации групповой политики необходимо запустить утилиту Управление групповой политикой → в домене stdm2.local создать новый объект групповой политики и указать название NetDiskUsersPolicy → выбирать пункт Изменить в контекстном меню. На рисунке 12 изображен путь до политики, которую необходимо отредактировать.

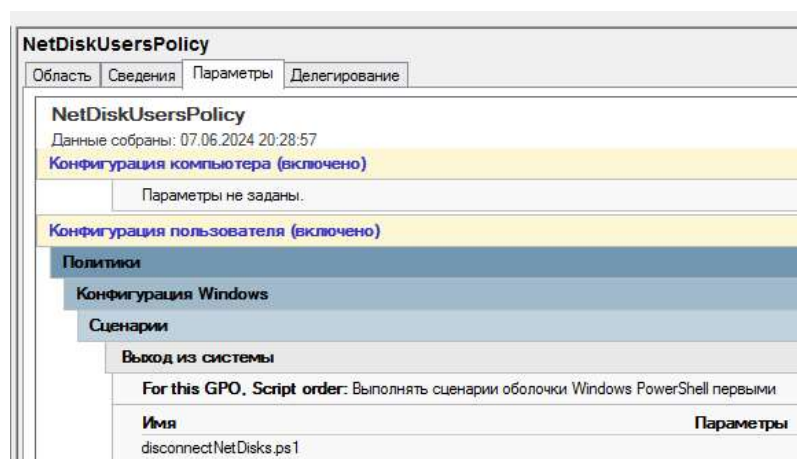


Рисунок 12 – Политика принудительного отключения сетевых ресурсов

Файл сценария PowerShell состоит из единственной строки кода – Remove-SmbMapping –Force, данный файл также расположен на общем сетевом ресурсе.

Так как все исполняемые пользовательские файлы для подключения\отключения сетевых дисков и смена пароля расположены на системном диске необходимо создать ярлыки на рабочем столе пользователя

для более комфортного взаимодействия. Решением данной задачи является определение дополнительных политик, которые создают ярлыки при каждом входе в систему. На рисунке 13 изображено полное название пути соответствующей политике.

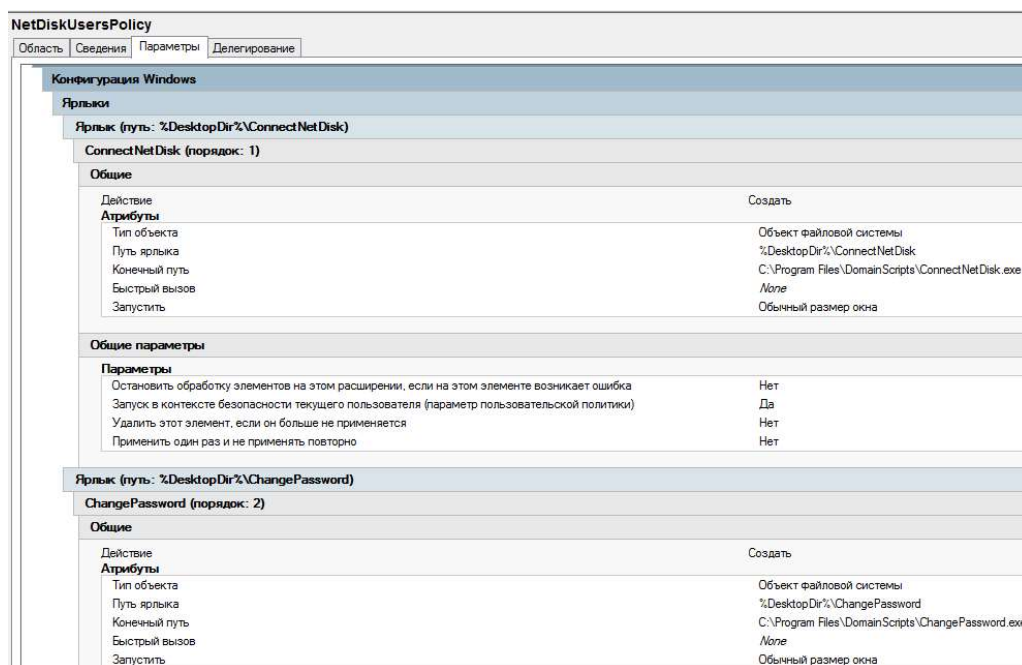


Рисунок 13 – Политики создания ярлыков исполняемых файлов

При каждом входе в общий сетевой профиль автоматически создаются ярлыки для программ ConnectNetDisk.exe и ChangePassword.exe, расположенных на системном диске пользовательских ПК.

По окончании конфигурирования групповой политики добавляем доменного общего пользователя, для которого они актуальны. Добавление пользователей и групп выполняется через Фильтр безопасности объекта групповой политики.

Таким образом, настроены групповые политики для работы для дальнейшей эксплуатации в локальной сети факультета СПО.

2.3 Тестирование файловой инфраструктуры

2.3.1 Тестирование автоматического запуска задач в Диспетчере заданий.

Первым шагом в тестировании работоспособности инфраструктуры является проверка создания пользователей, пользовательских групп и пользовательских директорий в автоматическом режиме. Для начала процесса синхронизации пользователей и групп необходимо изменить время через Панель управления, чтобы активировать триггер. На рисунке 14 продемонстрирована работа задачи SyncGroupsAndUsers.

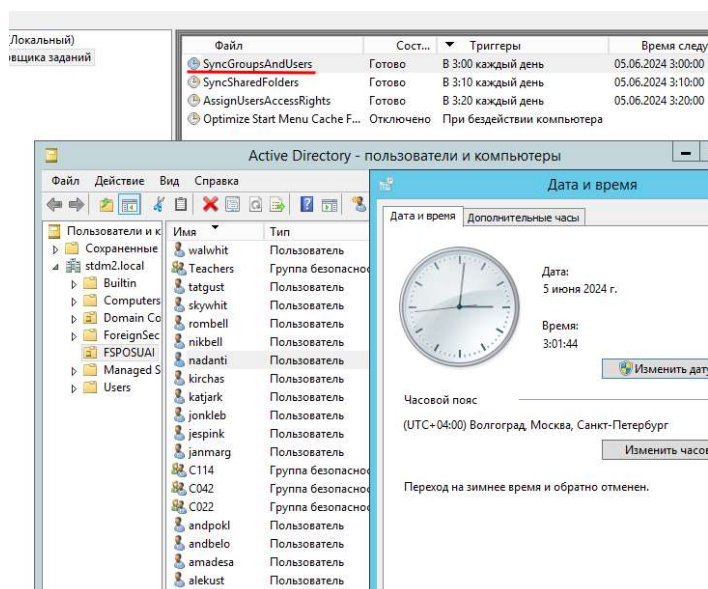


Рисунок 14 – Запуск задачи SyncGroupsAndUsers

Через 10 минут активируется задача синхронизации групповых и пользовательских директорий на сетевом ресурсе домена, на рисунке 15 изображен итог выполнения задачи SyncSharedFolders.

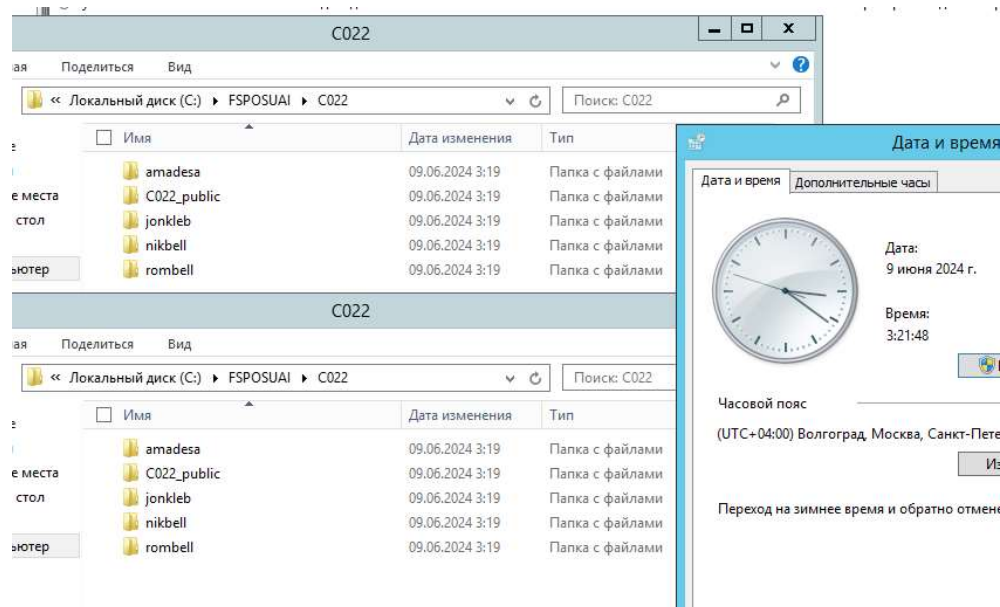


Рисунок 15 – Запуск задачи SyncSharedFolders

Задача AssignUsersAccessFight выполняется после двух предыдущих, так как настройка доступа производится при наличии пользователей, групп и директорий. Результат работы изображен на рисунке 16.

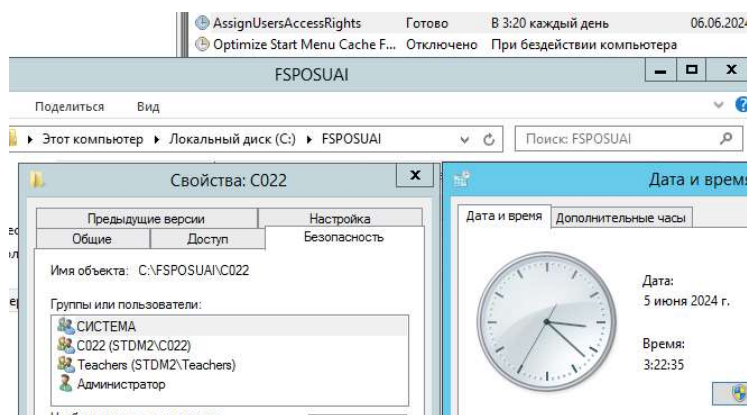
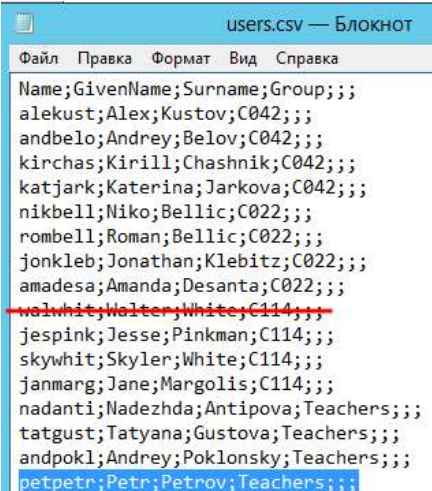


Рисунок 16 - Запуск задачи AssignUsersAccessFight

Далее переходим к проверке синхронизации пользователей и удаления устаревших записей: в данной ситуации в базе данных факультета появился новый пользователь Petr Petrov и пропал уже существующий – Walter White. Обновленная база данных пользователей изображена на рисунке 17.



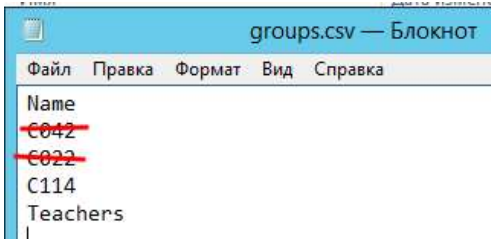
```

Name;GivenName;Surname;Group;;;
alekust;Alex;Kustov;C042;;;
andbelo;Andrey;Belov;C042;;;
kirchas;Kirill;Chashnik;C042;;;
katjark;Katerina;Jarkova;C042;;;
nikbell;Niko;Bellic;C022;;;
rombell;Roman;Bellic;C022;;;
jonkleb;Jonathan;Klebitz;C022;;;
amadesa;Amanda;Desanta;C022;;;
walwhit;Walter;White;C114;;;;
jespink;Jesse;Pinkman;C114;;;
skywhit;Skyler;White;C114;;;
janmarg;Jane;Margolis;C114;;;
nadanti;Nadezhda;Antipova;Teachers;;;
tatgust;Tatyana;Gustova;Teachers;;;
andpokl;Andrey;Poklonsky;Teachers;;;
petpetr;Petr;Petrov;Teachers;;;

```

Рисунок 17 – Обновленная база данных пользователей

Также изменилась база данных групп факультета - группы C042 и C022 окончили свое обучение и информацию о них, а также о студентах групп, следует удалить из Active Directory. Обновленная база данных групп изображена на рисунке 18.



```

Name
C042
C022
C114
Teachers

```

Рисунок 18 – Новая база данных групп

Результат обновления объектов Active Direcorty изображен на рисунке 19. Все неактуальные учетные записи и группы удалены, также удален пользователь Walter White и добавлен новый пользователь группы Teachers – Petr Petrov.

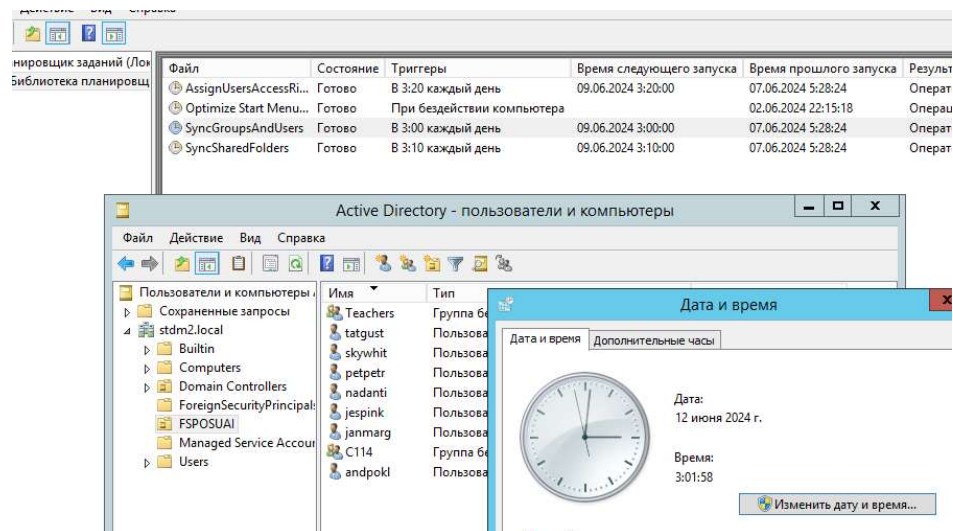


Рисунок 19 – Обновленные записи в Active Directory

Через некоторое время задачи SyncSharedFolders и AssignUsersAccessRights также выполнились, итог работы которых изображен на рисунке 20.

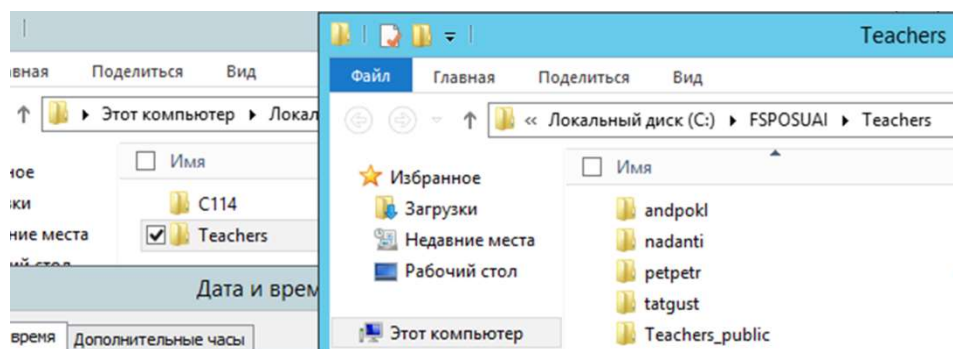


Рисунок 20 – Обновление рабочих директорий и прав доступа

Тест автоматического запуска сценария, благодаря которому создаются резервные копии пользовательских файлов и директорий изображен на рисунке 21.

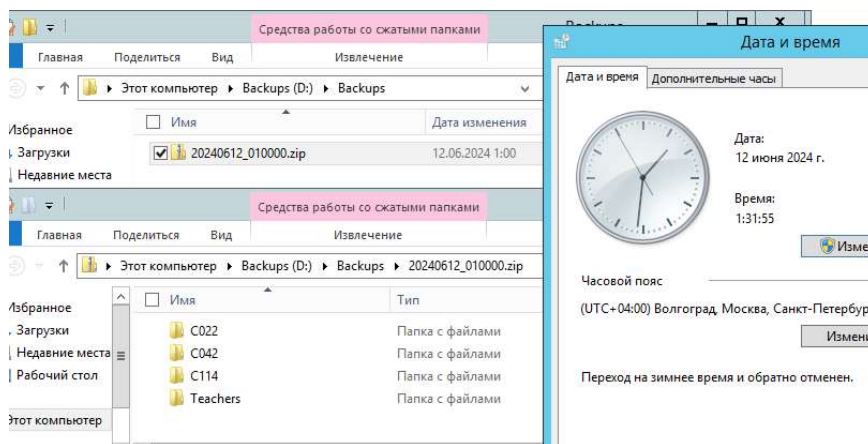


Рисунок 21 – Создание резервной копии сетевого ресурса факультета

На рисунке 21 видно, что файлом резервной копии является обычный zip-архив, с которым можно работать через Проводник ОС Windows.

Таким образом, проверены созданные задачи в утилите Планировщик заданий и сценарии синхронизации пользователей, групп, директорий пользователя и контроля доступа. Все тесты успешно пройдены.

2.3.2 Тестирование графический приложений для подключения пользовательских директорий и смены пароля.

Для подключения сетевой директории пользователя необходимо запустить исполняемый файл ConnectNetDisk.exe, которая расположена по пути C:\Program Files\DomainScripts\ConnectToNetDisk.exe. На рисунке 22 изображен пример подключения, с использованием логина alekust и пароль P@ssw0rd от учетной записи пользователя Александра Кустова.

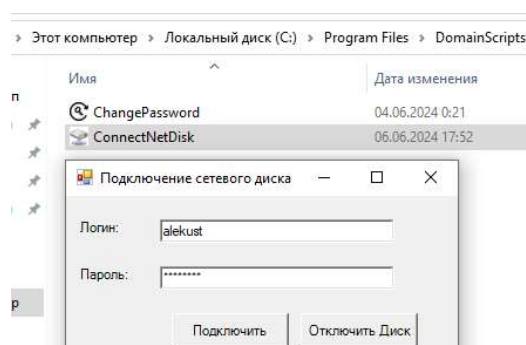


Рисунок 22 – Подключение сетевой директории пользователя alekust

После подключения сетевой директории программа автоматически откроет в Проводнике Windows только что подключенную сетевую директорию, если логин и пароль введены верно. На рисунке 23 изображено успешное подключение сетевого ресурса и все доступные пользователю директории.

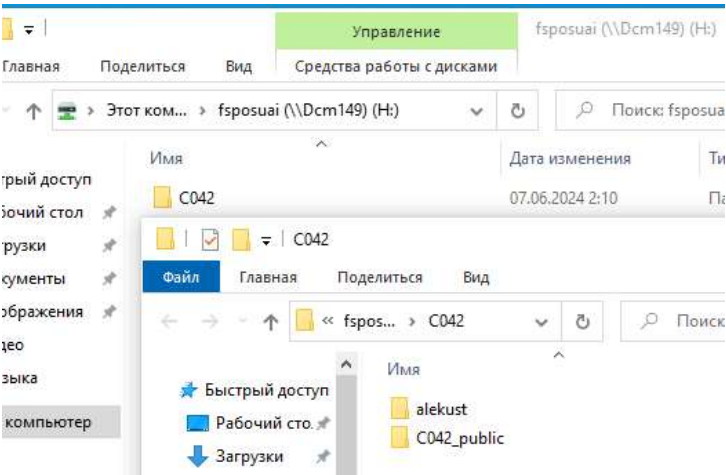


Рисунок 23 – Доступные ресурсы пользователю alekust

Пользователю разрешено создавать, исполнять и читать файлы в своей директории. На рисунке 24 изображено, как работают права доступа для пользователя в рамках его директории.

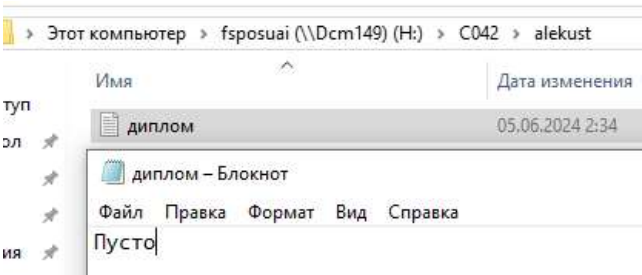


Рисунок 24 – Работа с директорией студента

Студенты имеют соответствующие правила на создание директорий/файлов, исполнение и чтение файлов в общей директории группы.

На рисунке 25 изображен пример работы в директории группы с использованием учётных данных студента Александра Кустова.

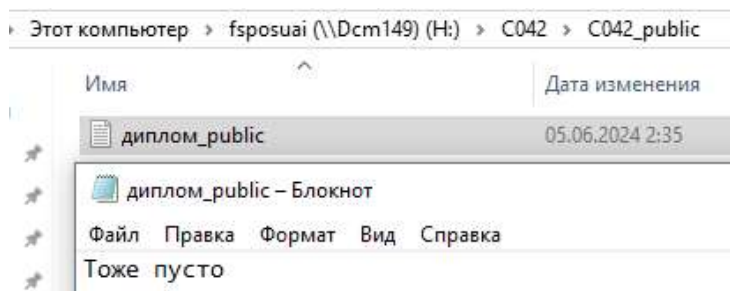


Рисунок 25 - Работа с директорией группы

Пользователь в праве отключить свой сетевой ресурс от ПК в любой момент, для этого необходимо использовать кнопку Отключить диск в программе ConnectNetDisk.exe, никаких учетных данных не требуется. Результат отключения сетевой директории пользователя изображен на рисунке 26.

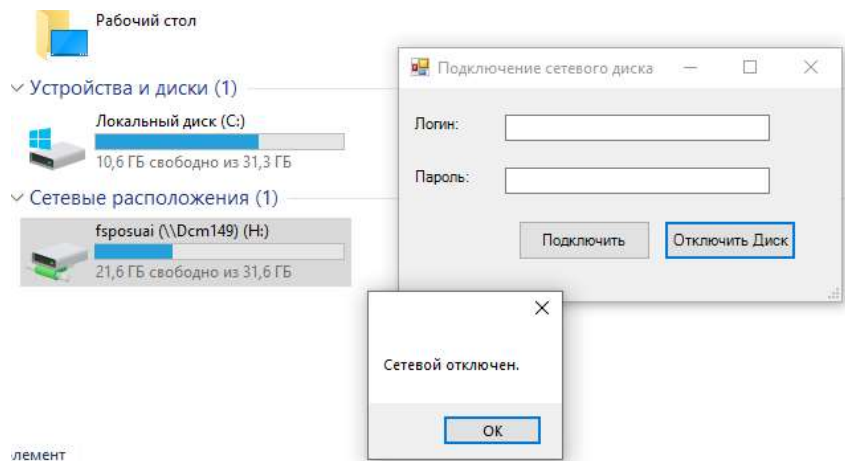


Рисунок 26 – Отключение сетевой директории пользователя

Преподаватели работают с сетевыми ресурсами точно так же, как и студенты: для подключения необходимо указать свой логин и пароль, как показано на рисунке 27.

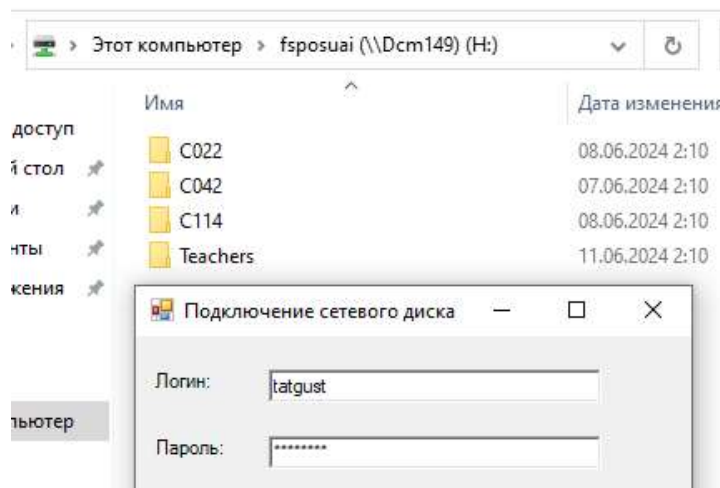


Рисунок 27 – Подключение сетевого ресурса преподавателя

Исходя из результатов представленных на рисунке 27, можно сделать вывод, что члены группы Teachers в том числе имеют доступ к директориям студентов. Следовательно все правила доступа функционируют в должном режиме, подтверждение тому изображено на рисунке 28.

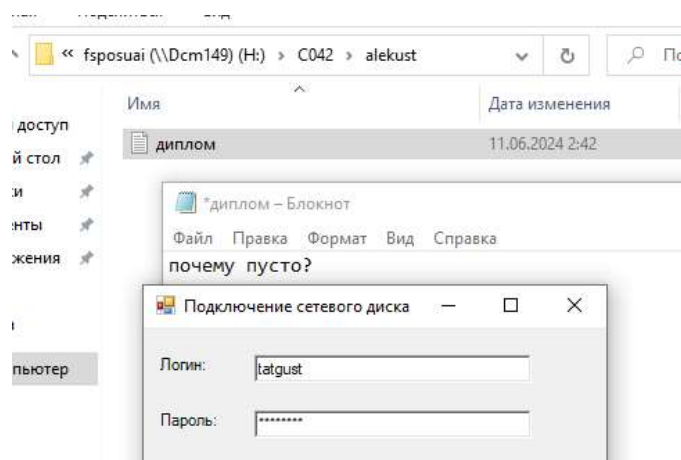


Рисунок 28 – Демонстрация прав доступа преподавателей

Пользователи вправе изменить пароль от своей учетной записи, для этого используется программа ChangePassword.exe, которая расположена в той же директории. На рисунке 29 изображен результат смены пароля от учетной записи студента Куцова Александра.

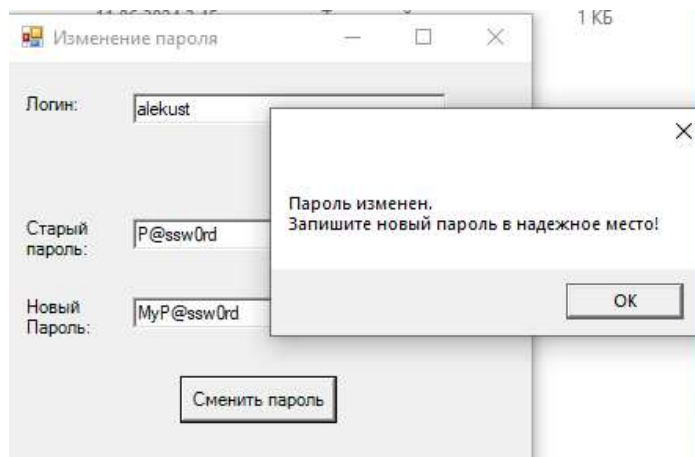


Рисунок 29 – Смена пароля от учетной записи пользователя

При неудачной попытке смены пароля программа выведет соответствующее сообщение пользователю об ошибке, как это продемонстрировано на рисунке 30.

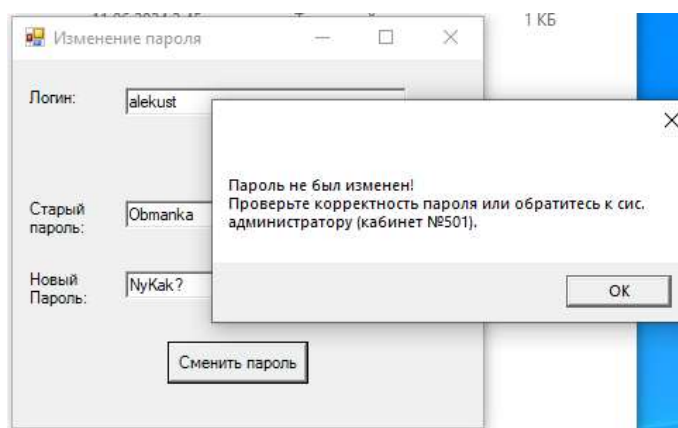


Рисунок 30 – Неудачная попытка смены пароля

Таким образом, проверены графические приложения ConnectNetDisk.exe и ChangePassword.exe для подключения сетевого ресурса пользователя и смены пароля от учетной записи соответственно. Все тесты успешно пройдены.

2.3.3 Тестирование работы групповой политики.

После входа в систему пользователю доступно два ярлыка программ ConnectNetDisk.exe и ChangePassword.exe. Ярлыки создаются автоматически в соответствии с групповой политикой NetDiskUsersPolicy. На рисунке 31 изображен перечень ярлыков, которые доступны пользователю сразу после входа.



Рисунок 31 – Ярлыки рабочего стола пользователя user518

После выхода из системы, в соответствии с политикой NetDiskUsersPolicy все подключенные сетевые ресурсы отключаются. На рисунке 32 продемонстрирована работа политики.

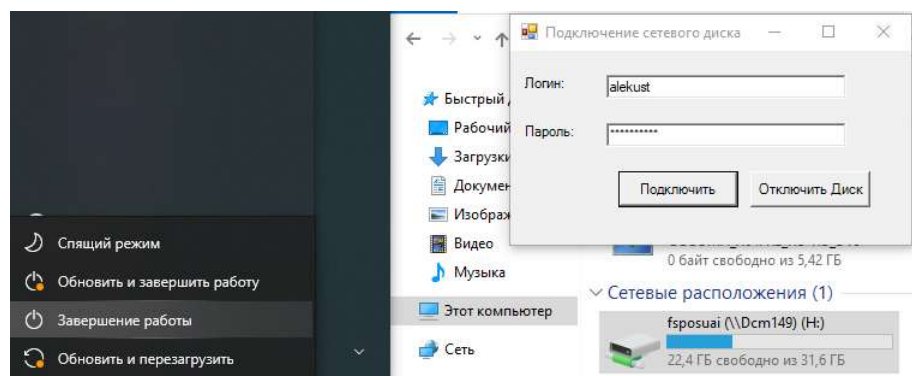


Рисунок 32 – Завершение работы с подключенным сетевым ресурсом

На рисунке 33 продемонстрировано, как при последующем включении ПК все сетевые подключения исчезли в соответствии с групповой политикой домена.



Рисунок 33 – Список сетевых подключений после входа в систему

Таким образом, проверена функционирования элементов групповой политики NetDiskUsersPolicy, благодаря которой создаются ярлыки графических приложений ConnectNetDisk.exe и ChangePassword.exe, а также запускается сценарий для отключения всех сетевых ресурсов.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данного дипломного проекта была приведена значительная работа по изучению проблем, связанных с организацией, взаимодействием и администрированию сетевых файловых хранилищ. Также были рассмотрены текущие проблемы действующего файлового хранилища факультета и разобраны существующие решения в Море. Основная цель проекта заключалась в создании защищенной файловой инфраструктуры факультета, которая позволяет обеспечить санкционированный доступ к пользовательским данным, а также поднять уровень надежности ресурса.

В рамках данной дипломной работы были достигнуты следующие результаты:

1) анализ существующих файловых хранилищ: были изучены ведущие технические решения организации файловых хранилищ как уже готовые решения от ИТ-компаний, так и требующие специфических знаний и подготовки для их создания;

2) выбор ОС для сервера: были проанализированы самые популярные ОС, которые используются в качестве серверной системы. Также были описаны все плюсы и минусы каждой из них;

3) конфигурация файлового хранилища: были написаны несколько сценариев PowerShell, которые позволили автоматизировать все процессы, связанные с поддержанием инфраструктуры в актуальном состоянии;

4) создание графических приложений: были созданы два графических приложения, которые позволяют пользователям сетевого хранилища комфортно взаимодействовать с файловой инфраструктурой. Также было создано приложение для комфортной смены пароля учетной записи пользователя;

5) тестирование файловой инфраструктуры: были проведены тесты PowerShell сценариев, файлового хранилища и пользовательских графических

приложений на их работоспособность. Все результаты отражены в соответствующем разделе.

Дальнейшим развитием проекта может послужить создание связи между базой данной личного кабинета факультета СПО и объектами Active Directory. Подобное усовершенствование позволит автоматизировать, а также ускорить процесс синхронизации базы данных пользователей и групп.

Дипломный проект выполнен полностью и в соответствии с заданием на дипломное проектирование.

					ДП.09.02.06.09ПЗ	Лист
						52
Изм.	Лист	№	докум.№	Подп.По		

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Статья об облачных хранилищах и зачем они нужны, URL: <https://cloud.vk.com/blog/more-dannyh-cto-takoe-oblachnye-hranilishha> (дата обращения 04.04.2024).
2. Статья о сетевой файловой системе NFS, URL: https://www.inp.nsk.su/~bolkhov/teach/inpunix/setup_nfs.ru.html (дата обращения 04.04.2024).
3. Статья о протоколе SMB, URL: <https://wiki.dieg.info/smb> (дата обращения 05.04.2024).
4. Статья о протоколе FTP и зачем он нужен, URL: <https://skillbox.ru/media/code/protokol-ftp-cto-eto-takoe-i-kak-s-nim-rabotat/> (дата обращения 05.04.2024).
5. Статья о технологии RAID, URL: <https://ddos-guard.net/ru/technologies/raid> (дата обращения 05.04.2024).
6. Статья об использовании социальной сети в качестве файлового хранилища, URL: https://habr.com/ru/companies/innopolis_university/articles/324010/ (дата обращения 05.04.2024).
7. Статья о облачных хранилищах-сервисах от сторонних компаний, URL: <https://journal.tinkoff.ru/list/best-cloud-services/> (дата обращения 06.04.2024).
8. Статья о проекте NextCloud, URL: <https://habr.com/ru/companies/hostkey/articles/738136/> (дата обращения 06.04.2024).
9. Статья о лучших альтернативах NextCloud, URL: <https://www.amediaclub.com/ru/nextcloud-alternatives/> (дата обращения 06.04.2024).
10. Статья о технологии WI-FI, URL: <https://www.tp-link.com/ru/WI-FI/> (дата обращения 07.04.2024).
11. Статья о ролях в ОС Windows Server, URL: <https://firstvds.ru/technology/roli-servera-v-os-windows> (дата обращения 06.04.2024).

12. Компьютерные сети: учебное пособие / Ракитин Р. Ю., Москаленко Е. В. - Барнаул : АлтГПУ, 2019. — 340 с. — ISBN 978-5-.88210-942-3. — Текст : электронный. — URL: <https://e.lanbook.com/book/139182> (дата обращения 06.04.2024).

13. Статья об основах операционных систем: компоненты, виды и история развития, URL: <https://skillbox.ru/media/code/osnovy-operatsionnykh-sistem-komponenty-vidy-i-istoriya-razvitiya/> (дата обращения 07.04.2024).

14. Статья о UNIX и зачем он нужен, URL: <https://thecode.media/unix/> (дата обращения 07.04.2024).

15. Статья о UNIX-подобных ОС, URL: <https://en.wikipedia.org/wiki/Unix-like> (дата обращения 07.04.2024).

16. Статья об Linux, URL: <https://blog.skillfactory.ru/glossary/linux/> (дата обращения 08.04.2024).

17. Статья о лучших дистрибутивах на базе ядра Linux, URL: <https://timeweb.cloud/blog/top-luchshih-distributivov-linuks> (дата обращения 08.04.2024).

18. Статья о Microsoft Windows Server: версиях, редакциях, лицензировании, URL: <https://serverspace.ru/support/help/windows-server-versions-editions-licensing/> (дата обращения 08.04.2024).

19. Jordan Krause, Освоение Windows Server 2019: полное руководство для системных администраторов по установке, управлению и развертыванию новых возможностей в Windows Server 2019 / Jordan Krause. — Великобритания : Издательство «Packt», 2021. — 690 с. - ISBN: 978-1-8010-7934-1 . - Текст : электронный. - URL: <http://ieeexplore.ieee.org/document/10162898> (дата обращения 08.04.2024).

20. Современный PowerShell / Андрей Попов. — Санкт-Петербург : Издательство «БХВ-Петербург», 2022. — 368 с. – ISBN 978-5-9775-6874-6 . – Текст : электронный. - URL: <https://bhv.ru/product/sovremennyj-powershell/> (дата обращения 09.04.2024).

21. Статья о библиотеке классов .NET, URL: <https://learn.microsoft.com/ru-ru/dotnet/standard/class-libraries> (дата обращения 09.04.2024).

22. Статья о текстовом формате CSV, URL: <https://blog.skillfactory.ru/glossary/csv-format/> (дата обращения 09.04.2024).

23. Документация к модулю NTFSSecurity, URL: <https://ntfssecurity.readthedocs.io/en/latest/> (дата обращения 10.04.2024).

24. Документация к командлету New-SmbMapping, URL: <https://learn.microsoft.com/en-us/powershell/module/smbshare/new-smbmapping> (дата обращения 11.04.2024).

25. Статья о программе ISESteroids, URL: <https://powershell.one/isesteroids/quickstart/overview> (дата обращения 12.04.2024).

ПРИЛОЖЕНИЕ А

Файл SyncUsersAndGroups.ps1

```
import-module ActiveDirectory
```

```
$x500Domain = 'OU=FSPOSUAI,DC=STDM2,DC=LOCAL'
```

```
$UsersDB = $(Import-Csv -Path ".\db\users.csv" -Delimiter ";" )
```

```
$GroupsDB = $(Import-Csv -Path ".\db\groups.csv" -Delimiter ";" ).Name
```

```
$ADUsersDB = $(Get-ADUser -Filter * -SearchBase $x500Domain)
```

```
$ADGroupsDB = $(Get-ADGroup -Filter * -SearchBase $x500Domain).Name
```

```
function SyncADGroups($DomainPath, $Groups, $ADGroups) {
```

```
    if ($ADGroups -eq $null) {
```

```
        $GroupsArrToAdd = $Groups
```

```
    } else {
```

```
        $CompareGroups = $(Compare-Object -ReferenceObject $Groups -  
DifferenceObject $ADGroups)
```

```
        $GroupsArrToAdd = $($CompareGroups | where SideIndicator -EQ  
"<=").InputObject
```

```
        $GroupsArrToDel = $($CompareGroups | where SideIndicator -EQ  
"=>").InputObject
```

```
    }
```



```

if ($GroupsArrToDel.count -gt 0) {

    foreach ($Group in $GroupsArrToDel) {

        $ADUsersListOfGroup = $(Get-ADGroupMember "$Group").Name

        foreach ($User in $ADUsersListOfGroup) {

            Remove-ADUser -Identity $User -Confirm:$False

        }

        Remove-ADGroup -Identity $Group -Confirm:$False

    }

}

if ($GroupsArrToAdd.count -gt 0) {

    foreach ($Group in $GroupsArrToAdd) {

        New-ADGroup -Name $Group `
            -SamAccountName $Group `
            -GroupCategory Security `
            -GroupScope Global `
            -DisplayName $Group `
            -Path $DomainPath `
            -Description "Группа для $Group"

    }

}

```

```
}
```

```
function SyncADUsers($DomainPath, $Users, $ADUsers) {
```

```
    if ($ADUsers -eq $null) {
```

```
        $UsersArrToAdd = $Users
```

```
    } else {
```

```
        $CompareUsers = $(Compare-Object -ReferenceObject $Users `
```

```
            -DifferenceObject $ADUsers `
```

```
            -Property Name `
```

```
            -IncludeEqual `
```

```
            -PassThru)
```

```
        $UsersArrToAdd = @($CompareUsers | where SideIndicator -EQ "<=")
```

```
        $UsersArrToDel = $($CompareUsers | where SideIndicator -EQ "=>").Name
```

```
    }
```

```
    if ($UsersArrToDel.count -gt 0) {
```

```
        foreach ($User in $UsersArrToDel) {
```

```
            Remove-ADUser -Identity $User -Confirm:$False
```

```
        }
```

```
    }
```

```
    if ($UsersArrToAdd.count -gt 0) {
```

```
        foreach ($User in $UsersArrToAdd) {
```

```
            New-ADUser -Name $User.Name `
```

					ДП.09.02.06.09ПЗ	Лист
						58
Изм.	Лист	№	докум.№	Подп.По		Дата

```

-SamAccountName $User.Name `
-Path $DomainPath `
-GivenName $User.GivenName `
-Surname $User.Surname `
-Initials "$($User.GivenName [0]).$($User.Surname [0])." `
-AccountPassword $(ConvertTo-SecureString "P@ssw0rd" -
AsPlainText -Force) `
-Enable $True `
-ChangePasswordAtLogon $False

```

```

Add-ADGroupMember -Identity $User.Group -Members $User.Name
}
}
}

```

SyncADGroups \$x500Domain \$GroupsDB \$ADGroupsDB

SyncADUsers \$x500Domain \$UsersDB \$ADUsersDB

ПРИЛОЖЕНИЕ Б

Файл SyncSharedFolders.ps1

Import-module ActiveDirectory

\$RootFolder = 'C:\FSPOSUAI'

\$x500Domain = 'OU=FSPOSUAI,DC=STDM2,DC=LOCAL'

\$GroupsSharedFolders = \$(Get-ADGroup -Filter * -SearchBase
\$x500Domain).Name

function SyncGroupsFolders(\$Domain, \$RootFolder, \$GroupsFolders) {

if (\$(Get-ChildItem -Path "\$RootFolder" -directory).Name -eq \$null) {

 \$GFArrToAdd = \$GroupsFolders

} elseif (\$GroupsFolders -eq \$null) {

 \$GFArrToDel = \$(Get-ChildItem -Path "\$RootFolder" -directory).Name

} else {

 \$CurrGroupsFolders = \$(Get-ChildItem -Path "\$RootFolder" -
directory).Name

 \$CompareGroupsFolders = \$(Compare-Object -ReferenceObject
\$GroupsFolders `

 -DifferenceObject \$CurrGroupsFolders `

 -IncludeEqual)

 \$GFArrToDel = \$(\$CompareGroupsFolders | where SideIndicator -EQ
"=>").InputObject

 \$GFArrToAdd = \$(\$CompareGroupsFolders | where SideIndicator -EQ
"<=").InputObject

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№	докум.№	Подп.По		60

```
}
```

```
if ($GFArrToDel.count -gt 0) {
```

```
    foreach ($Group in $GFArrToDel) {
```

```
        Remove-Item -Path "$RootFolder\$Group" `
```

```
        -Recurse `
```

```
        -Force
```

```
    }
```

```
}
```

```
if ($GFArrToAdd.count -gt 0) {
```

```
    foreach ($Group in $GFArrToAdd) {
```

```
        New-Item -Path "$RootFolder\$Group" `
```

```
        -ItemType Directory
```

```
    }
```

```
}
```

```
}
```

```
function SyncUsersFolders($Domain, $RootFolder, $Groups) {
```

```
    foreach ($Group in $Groups) {
```

```
        $GroupMembers = $(Get-ADGroupMember -Identity $Group).Name
```

```
        $GroupMembers += "$($Group)_public"
```

						Лист
						61
Изм.	Лист	№	докум.№	Подп.По	Дата	

ДП.09.02.06.09ПЗ

```

if ($(Get-ChildItem -Path "$RootFolder\$Group" -directory).Name -eq $null)
{
    $UFArrToAdd = $GroupMembers
} else {
    $CurrUsersFolders = $(Get-ChildItem -Path "$RootFolder\$Group" -
directory).Name
    $CompareUsersFolders = $(Compare-Object -ReferenceObject
$GroupMembers `
        -DifferenceObject $CurrUsersFolders `
        -IncludeEqual)
    $UFArrToDel = $($CompareUsersFolders | where SideIndicator -EQ
"=>").InputObject
    $UFArrToAdd = $($CompareUsersFolders | where SideIndicator -EQ
"<=").InputObject
}

if ($UFArrToDel.count -gt 0) {
    foreach ($Folder in $UFArrToDel) {
        Remove-Item -Path "$RootFolder\$Group\$Folder" `
            -Recurse `
            -Force
    }
}

if ($UFArrToAdd.count -gt 0) {
    foreach ($Folder in $UFArrToAdd) {

```

New-Item -Path "\$RootFolder\\$Group\\$Folder" `

-ItemType Directory

}

}

}

}

SyncGroupsFolders \$x500Domain \$RootFolder \$GroupsSharedFolders

SyncUsersFolders \$x500Domain \$RootFolder \$GroupsSharedFolders

					ДП.09.02.06.09ПЗ	Лист
						63
Изм.	Лист	№	докум.№	Подп.По	Дата	

ПРИЛОЖЕНИЕ В

Файл AssignUsersAccessRights.ps1

Import-Module NTFSSecurity

Import-module ActiveDirectory

\$RootFolder = 'C:\FSPOSUAI'

\$x500Domain = 'OU=FSPOSUAI,DC=STDM2,DC=LOCAL'

\$GroupsSharedFolders = \$(Get-ADGroup -Filter * -SearchBase
\$x500Domain).Name

function SetAccessFolders(\$Domain, \$RootFolder, \$GroupsFolders) {

foreach(\$Group in \$GroupsFolders) {

Clear-NTFSAccess -Path "\$RootFolder\\$Group" -DisableInheritance

Add-NTFSAccess `

-Path "\$RootFolder\\$Group" `

-Account "STDM2\\$Group", "STDM2\Teachers" `

-AccessRights Write, Delete, ReadPermissions, Read, ReadAndExecute,
Modify `

-AccessType Allow

Add-NTFSAccess `

-Path "\$RootFolder\\$Group" `

						Лист
						64
Изм.	Лист	№	докум.№	Подп.По	Дата	

ДП.09.02.06.09ПЗ

-Account "SYSTEM", 'STDM2\Администратор' `

-AccessRights Full `

-AccessType Allow

\$GroupMembers = \$(Get-ADGroupMember -Identity \$Group).Name

foreach(\$Folder in \$GroupMembers) {

Clear-NTFSAccess -Path "\$RootFolder\\$Group\\$Folder" -
DisableInheritance

if (\$Group -eq "Teachers") {

Add-NTFSAccess `

-Path "\$RootFolder\\$Group\\$Folder" `

-Account "STDM2\\$Folder"

-AccessRights Write, Delete, ReadPermissions, Read,
ReadAndExecute, Modify `

-AccessType Allow

} else {

Add-NTFSAccess `

-Path "\$RootFolder\\$Group\\$Folder" `

-Account "STDM2\\$Folder", "STDM2\Teachers" `

-AccessRights Write, Delete, ReadPermissions, Read,
ReadAndExecute, Modify `

-AccessType Allow

					ДП.09.02.06.09ПЗ	Лист
						65
Изм.	Лист	№	докум.№	Подп.По		Дата

}

Add-NTFSAccess `

-Path "\$RootFolder\\$Group\\$Folder" `

-Account "SYSTEM", 'STDM2\Администратор' `

-AccessRights Full `

-AccessType Allow

}

}

}

SetAccessFolders \$x500Domain \$RootFolder \$GroupsSharedFolders

					ДП.09.02.06.09ПЗ	Лист
						66
Изм.	Лист	№	докум.№	Подп.По	Дата	

ПРИЛОЖЕНИЕ Г

Файл BackupUsersData.ps1

Add-Type -AssemblyName "System.IO.Compression.FileSystem"

\$Date = Get-Date -Format "yyyyMMdd_HH:mm:ss"

\$SourceDir = "C:\FSPOSUAI"

\$BackupDir = "\$(\$Join-Path -Path "D:\Backups" -ChildPath \$Date).zip"

```
if ((Test-Path -Path $SourceDir) -and (Test-Path -Path "D:\Backups")) {  
    [System.IO.Compression.ZipFile]::CreateFromDirectory($SourceDir,  
    $BackupDir)  
}
```

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№ докум.	№	Подп.По	Дата	67

ПРИЛОЖЕНИЕ Д
Файл ConnectToNetDisk.ps1

Import-Module SmbShare

Add-Type -AssemblyName System.Windows.Forms

Add-Type -AssemblyName System.Drawing

\$form = New-Object System.Windows.Forms.Form

\$form.Text = "Подключение сетевого диска"

\$form.Size = New-Object System.Drawing.Size(350, 200)

\$form.StartPosition = "CenterScreen"

\$labelUser = New-Object System.Windows.Forms.Label

\$labelUser.Text = "ЛОГИН:"

\$labelUser.Size = New-Object System.Drawing.Size(60, 20)

\$labelUser.Location = New-Object System.Drawing.Point(10, 20)

\$form.Controls.Add(\$labelUser)

\$textBoxUser = New-Object System.Windows.Forms.TextBox

\$textBoxUser.Size = New-Object System.Drawing.Size(200, 20)

\$textBoxUser.Location = New-Object System.Drawing.Point(80, 20)

\$form.Controls.Add(\$textBoxUser)

\$labelPassword = New-Object System.Windows.Forms.Label

\$labelPassword.Text = "Пароль:"

\$labelPassword.Size = New-Object System.Drawing.Size(60, 20)

\$labelPassword.Location = New-Object System.Drawing.Point(10, 60)

					ДП.09.02.06.09ПЗ	Лист
						68
Изм.	Лист	№	докум.№	Подп.По		Дата

```
$form.Controls.Add($labelPassword)
```

```
$textBoxPassword = New-Object System.Windows.Forms.TextBox
```

```
$textBoxPassword.Size = New-Object System.Drawing.Size(200, 20)
```

```
$textBoxPassword.Location = New-Object System.Drawing.Point(80, 60)
```

```
$textBoxPassword.UseSystemPasswordChar = $true
```

```
$form.Controls.Add($textBoxPassword)
```

```
$buttonLogin = New-Object System.Windows.Forms.Button
```

```
$buttonLogin.Text = "Подключить"
```

```
$buttonLogin.Size = New-Object System.Drawing.Size(100, 30)
```

```
$buttonLogin.Location = New-Object System.Drawing.Point(90, 100)
```

```
$form.Controls.Add($buttonLogin)
```

```
$buttonDisconnectDisk = New-Object System.Windows.Forms.Button
```

```
$buttonDisconnectDisk.Text = "Отключить Диск"
```

```
$buttonDisconnectDisk.Size = New-Object System.Drawing.Size(100, 30)
```

```
$buttonDisconnectDisk.Location = New-Object System.Drawing.Point(200, 100)
```

```
$form.Controls.Add($buttonDisconnectDisk)
```

```
$buttonLogin.Add_Click({
```

```
    $username = $textBoxUser.Text
```

```
    $password = $textBoxPassword.Text
```

```
    Remove-SmbMapping -LocalPath 'H:' `
```

```
-Force `
-UpdateProfile
```

```
try {
```

```
    New-SmbMapping -LocalPath 'H:' `
```

```
        -UserName "$username" `
```

```
        -Password "$password" `
```

```
        -RemotePath "\\Dcm149\fsposuai" `
```

```
        -ErrorAction Stop
```

```
    Stop-Process -Name 'explorer' | Start-Process -FilePath
'C:\Windows\explorer.exe'
```

```
    start H:\
```

```
    } catch {
```

```
        [System.Windows.Forms.MessageBox]::Show("Сетевой диск не удалось
подключить. Проверьте логин и пароль! Возможно, другой диск уже
подключен.")
```

```
    }
```

```
}}
```

```
$buttonDisconnectDisk.Add_Click({
```

```
try {
```

						ДП.09.02.06.09ПЗ	Лист
							70
Изм.	Лист	№	докум.№	Подп.По	Дата		

```

Remove-SmbMapping -LocalPath 'H:' -Force -ErrorAction Stop

[System.Windows.Forms.MessageBox]::Show("Сетевой отключен.")

Stop-Process -Name 'explorer' | Start-Process -FilePath
'C:\Windows\explorer.exe'

} catch {

[System.Windows.Forms.MessageBox]::Show("Ниодного сетевого диска
не подключено.")

}

})

$form.ShowDialog()

```

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№ докум.	№	Подп.По	Дата	71

ПРИЛОЖЕНИЕ Е

Файл ChangePassword.ps1

Import-module ActiveDirectory

Add-Type -AssemblyName System.Windows.Forms

Add-Type -AssemblyName System.Drawing

\$form = New-Object System.Windows.Forms.Form

\$form.Text = "Изменение пароля"

\$form.Size = New-Object System.Drawing.Size(350, 300)

\$form.StartPosition = "CenterScreen"

\$labelUser = New-Object System.Windows.Forms.Label

\$labelUser.Text = "Логин:"

\$labelUser.Size = New-Object System.Drawing.Size(60, 30)

\$labelUser.Location = New-Object System.Drawing.Point(10, 20)

\$form.Controls.Add(\$labelUser)

\$textUser = New-Object System.Windows.Forms.TextBox

\$textUser.Size = New-Object System.Drawing.Size(200, 20)

\$textUser.Location = New-Object System.Drawing.Point(80, 20)

\$form.Controls.Add(\$textUser)

\$labelOldPass = New-Object System.Windows.Forms.Label

\$labelOldPass.Text = "Старый пароль:"

\$labelOldPass.Size = New-Object System.Drawing.Size(60, 30)

\$labelOldPass.Location = New-Object System.Drawing.Point(10, 100)

\$form.Controls.Add(\$labelOldPass)

\$textOldPass = New-Object System.Windows.Forms.TextBox

\$textOldPass.Size = New-Object System.Drawing.Size(200, 20)

					ДП.09.02.06.09ПЗ	Лист
Изм.	Лист	№	докум.№	Подп.По		72


```
$textOldPass.Location = New-Object System.Drawing.Point(80, 100)
$form.Controls.Add($textOldPass)
```

```
$labelNewPass = New-Object System.Windows.Forms.Label
$labelNewPass.Text = "Новый Пароль:"
$labelNewPass.Size = New-Object System.Drawing.Size(60, 30)
$labelNewPass.Location = New-Object System.Drawing.Point(10, 150)
$form.Controls.Add($labelNewPass)
```

```
$textNewPass = New-Object System.Windows.Forms.TextBox
$textNewPass.Size = New-Object System.Drawing.Size(200, 20)
$textNewPass.Location = New-Object System.Drawing.Point(80, 150)
$form.Controls.Add($textNewPass)
```

```
$buttonChange = New-Object System.Windows.Forms.Button
$buttonChange.Text = "Сменить пароль"
$buttonChange.Size = New-Object System.Drawing.Size(100, 30)
$buttonChange.Location = New-Object System.Drawing.Point(110, 200)
$form.Controls.Add($buttonChange)
```

```
$buttonChange.Add_Click({
    $User = $textUser.Text
    $OldPass = $textOldPass.Text
    $NewPass = $textNewPass.Text

    try {
        Set-ADAccountPassword -Identity "$User" `
            -OldPassword (ConvertTo-SecureString -AsPlainText
"$OldPass" -Force) `
```

```

        -NewPassword (ConvertTo-SecureString -AsPlainText
"$NewPass" -Force) `
        -Server "DCM149" `
        -ErrorAction Stop

[System.Windows.Forms.MessageBox]::Show("Пароль
изменен.`nЗапишите новый пароль в надежное место!")

    } catch {

        [System.Windows.Forms.MessageBox]::Show("Пароль не был
изменен!`nПроверьте корректность пароля или обратитесь к сис.
администратору (кабинет №501).")

    }

})

$form.ShowDialog()

```

ОТЗЫВ РУКОВОДИТЕЛЯ
НА ДИПЛОМНЫЙ ПРОЕКТ

на тему Обеспечение защиты информации инфраструктуры факультета СПО ГУАП

выполненный студентом группы № C042

Кустовом Александром Михайловичем

фамилия, имя, отчество студента

по специальности 09.02.06 Сетевое и системное администрирование

код

наименование специальности

наименование специальности

Актуальность, практическая значимость и новизна темы работы:

Актуальностью данной темы является повышение уровня защиты информации студентов и преподавателей в связи с развитием сетевых технологий.

Характерные особенности работы:

Характерной особенностью работы является создание защищенной файловой инфраструктуры факультета СПО ГУАП.

Достоинства и недостатки работы:

Достоинствами работы являются:

- актуальность выбранной темы,
- логичность и последовательность структурных элементов пояснительной записки,
- работоспособность файлового хранилища в соответствии с заявленными требованиями.

Отношение выпускника к выполнению дипломного проекта, проявленные (не проявленные) им способности:

Автор проекта проявил профессиональные способности, выражающиеся в умении решать конкретные технические задачи, связанные с модернизацией файловой инфраструктуры, работать с технической литературой и документацией.

Уровень освоения общих и профессиональных компетенций; знания, умения, продемонстрированные при выполнении дипломного проекта:

Кустов А.М. показал хороший уровень освоения следующих общих и профессиональных компетенций: ОК 1–11, ПК 1.1 – ПК 1.5, ПК 2.1 – ПК 2.4, ПК 3.1 – ПК 3.6 по специальности «Сетевое и системное администрирование». Автор проекта

продемонстрировал знания и умения в соответствии с требованиями ФГОС СПО 09.02.06 «Сетевое и системное администрирование».

Степень самостоятельности выпускника, проявленная при выполнении дипломного проекта и его личный вклад в раскрытие проблем и разработку предложений по их решению:

Автор проекта проявил самостоятельность и организованность при выполнении заданий дипломного проекта. Для решения поставленной задачи Кустов А.М. проанализировал и сделал выбор необходимого ПО и серверных ОС, продемонстрировал настройку файлового хранилища и проверку работоспособности локальной сети бухгалтерии, а также предложил грамотные технические решения.

Замечания по теме дипломного проекта:

Замечаний по теме дипломного проекта нет.

Общая оценка выполнения поставленной перед выпускником задачи:

Дипломный проект по теме «Обеспечение защиты информации инфраструктуры факультета СПО ГУАП» выполнен в полном объеме и в соответствии с заданием.

Общий вывод о возможности (невозможности) допуска дипломного проекта к защите:

Дипломный проект может быть допущен к защите, так как выполнен с соблюдением необходимых требований к структуре и содержанию по программам подготовки специалистов среднего звена.

Оценка:

Считаю, что дипломный проект Кустова А.М., может претендовать на оценку «отлично» при соответствующей защите, а студент Кустов А.М. заслуживает присвоения квалификации сетевой и системный администратор по специальности 09.02.06 «Сетевое и системное администрирование».

Руководитель

преподаватель

должность, уч. степень, звание

подпись, дата

И.В. Козлов

инициалы, фамилия

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

ОЦЕНОЧНЫЙ ЛИСТ ДИПЛОМНОЙ РАБОТЫ

Студента группы № С042 Куцова Александра Михайловича
фамилия, имя, отчество

ФИО	Отзыв	Оценка
Преснухина Ю.В.	Дипломный проект выполнен в соответствии с требованиями ЕСКД	5 (отлично) Пресс 30.05.24г

С оценочным листом знакомлен(а)  30.05.2024г.
подпись, дата