

М. В. Ляхова¹, Н. Г. Сеникова¹

¹ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ SFTP (SSH FTP) НА БАЗЕ WINDOWS SERVER. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. В статье рассматривается задача безопасной передачи файлов в корпоративных сетях на базе Windows Server. Актуальность работы связана с сохранением в инфраструктуре организаций устаревшего протокола FTP, передающего учетные данные и содержимое файлов без шифрования и создающего риск перехвата и несанкционированного доступа. Цель исследования заключается в разработке и экспериментальной проверке методики развертывания SFTP-сервера на основе OpenSSH-Win64 в доменной среде Windows. Предложенная методика включает подготовку объектов Active Directory, организацию каталогов и NTFS-разрешений по принципу наименьших привилегий, настройку службы sshd и брандмауэра Windows, ограничение пользовательской сессии SFTP-функционалом и подключение с клиентской станции через WinSCP. Эксперимент выполнен в изолированном стенде Oracle VirtualBox с Windows Server 2022 и Windows 11. Функциональное тестирование подтвердило успешную доменную аутентификацию, передачу файлов, изоляцию пользователя в разрешенном каталоге и корректную реакцию на ошибочные учетные данные и потерю сетевого соединения. Дополнительно проанализированы сценарии brute-force, попытки выхода за пределы разрешенного каталога, получения shell-доступа и доступа к журналам. Показано, что сочетание механизмов Active Directory, NTFS и OpenSSH обеспечивает управляемое разграничение доступа, однако блокировка учетной записи при переборе паролей может использоваться для DoS-воздействия и требует дополнительных мер защиты на уровне источника подключения. Рассмотрены также ограничения изоляции OpenSSH в Windows по сравнению с механизмом chroot в Linux.

Ключевые слова: SFTP, SSH, безопасная передача файлов, OpenSSH для Windows, Active Directory, аутентификация по ключам, изоляция пользователей.

Введение

В условиях стремительного роста объемов корпоративных данных и увеличения числа распределенных инфраструктур вопросы безопасной передачи информации приобретают особую значимость. Большинство утечек корпоративных данных связаны с перехватом незашифрованного трафика и использованием уязвимых протоколов обмена файлами. В особенности уязвимыми призваны устаревшие FTP-сервера, которые продолжают использоваться в организациях из-за простоты администрирования, но при этом передают учетные данные и файлы в открытом виде.

Протокол SFTP (SSH File Transfer Protocol) является современной альтернативой FTP и FTPS, обеспечивающей полный контроль целостности и конфиденциальности данных благодаря шифрованию SSH и строгим политикам аутентификации. Однако даже при использовании SFTP ошибки конфигурации могут приводить к угрозам: несанкционированному доступу, выходу пользователя за пределы рабочего каталога, эскалации привилегий или обходу механизмов регистрации.

Дополнительным фактором актуальности является то, что многие российские предприятия переходят на локальные инфраструктуры на базе Windows Server, где требуется интеграция SFTP с доменной аутентификацией Active Directory и строгим разграничением прав. Несмотря на востребованность, отсутствуют полные, структурированные и доступные методики развертывания SFTP под Windows с акцентом на безопасность, что затрудняет внедрение технологий защищенного обмена файлами в промышленной среде.

Объектом исследования выступают корпоративные информационные системы, использующие доменную инфраструктуру Windows Server и сервисы Active Directory для централизованного контроля доступа.

Предметом исследования являются механизмы и методы настройки безопасного протокола передачи файлов SFTP на базе OpenSSH, интегрированного в среду Windows Server.

Целью исследования является разработка и экспериментальная проверка методики развертывания безопасного SFTP-сервера в доменной среде Windows с использованием OpenSSH, а также анализ механизмов защиты и оценка устойчивости к типовым угрозам.

Для достижения цели были поставлены следующие задачи:

1. Проверить корректность функционирования доменной инфраструктуры и соединения клиентских устройств.
2. Создать специализированное организационное подразделение, группу безопасности и пользователя для работы с SFTP.
3. Настроить файловую структуру и разрешения NTFS для обеспечения изоляции пользователей.
4. Установить и сконфигурировать OpenSSH-Win на Windows Server.
5. Настроить брандмауэр Windows для безопасного доступа к SSH-сервису.
6. Выполнить настройку файла `sshd_config` с учетом требований безопасности.
7. Подготовить клиентскую станцию и выполнить подключение через WinSCP.
8. Провести серию функциональных и нагрузочных тестов для проверки работы сервиса.
9. Проанализировать результаты тестирования и сформировать выводы о безопасности и правильности конфигурации.

Литературный обзор

В современных условиях цифровизации бизнес-процессов и роста объемов данных безопасная передача файлов между системами и пользователями становится критически важной задачей. Протокол FTP (File Transfer Protocol), долгое время являвшийся стандартом, обладает фундаментальными недостатками в области безопасности, такими как передача учетных данных и данных в открытом виде, что делает его уязвимым к перехвату и атакам «человек посередине» (Man-in-the-Middle) [1, 2]. В ответ на эти угрозы был разработан и получил широкое распространение протокол SSH File Transfer Protocol (SFTP).

SFTP – это безопасный протокол передачи файлов, функционирующий как подсистема протокола Secure Shell (SSH). В отличие от своего предшественника FTPS (FTP over SSL/TLS), SFTP не использует отдельный канал данных, а инкапсулирует все команды и данные в единый, зашифрованный SSH-туннель [3]. Это обеспечивает:

1. Конфиденциальность: Шифрование всего трафика, включая логины, пароли и передаваемые файлы, с использованием современных криптографических алгоритмов (например, AES, ChaCha20).
2. Целостность данных: Гарантия того, что данные не были изменены при передаче.
3. Аутентификацию: Поддержка различных методов аутентификации: по паролю, с использованием ключевой пары (публичный/приватный ключ), а также интеграция с внешними системами, такими как Kerberos или Active Directory [4].

Интеграция SFTP-сервера в инфраструктуру на базе Windows Server представляет особый интерес для организаций, чья ИТ-среда построена преимущественно на продуктах Microsoft. Исторически Windows Server не включал встроенный SSH-сервер, что вынуждало администраторов использовать сторонние решения (Cygwin, Bitvise). Ситуация изменилась с проектом OpenSSH-Win64, разрабатываемым Microsoft и сообществом, который предоставляет полноценный порт OpenSSH для Windows [5]. Его включение в состав современных версий Windows Server в качестве дополнительного компонента знаменует поворот к нативным возможностям безопасной удаленной работы.

Таким образом, актуальность темы обусловлена растущей потребностью в безопасных, стандартизированных и легко интегрируемых в существующую Windows-инфраструктуру решениях для обмена файлами.

Данное исследование направлено на практическое изучение процесса развертывания, настройки и тестирования SFTP-сервера на базе OpenSSH-Win64 в доменной среде Windows Server, с фокусом на реализацию механизмов безопасности.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Сравнительный анализ решений для защищенной передачи файлов в среде Windows Server

Несмотря на наличие различных решений для безопасной передачи файлов в среде Windows Server, выбор конкретной технологии должен определяться совокупностью факторов: безопасностью, удобством интеграции, стоимостью и сложностью администрирования.

FTPS (FTP over SSL/TLS) на базе IIS

Данное решение представляет собой развитие классического FTP с добавлением шифрования через SSL/TLS. К его преимуществам можно отнести глубокую интеграцию с операционной системой и Active Directory, а также наличие графического интерфейса управления. Однако FTPS обладает существенными недостатками: сложность настройки из-за необходимости управления SSL-сертификатами и двумя каналами связи (командным и данными), что увеличивает поверхность атаки. Кроме того, протокол считается устаревающим в сравнении с более современными и безопасными альтернативами [4].

Сторонние SFTP-серверы (Bitvise, FileZilla Server Pro)

Коммерческие и бесплатные сторонние решения, такие как Bitvise SSH Server или FileZilla Server Pro, предлагают готовые к развертыванию SFTP-серверы с графическим интерфейсом конфигурации. Их основные преимущества – быстрота развертывания и расширенные функции (например, встроенный Web-интерфейс или поддержка подробного аудита). Однако они часто требуют дополнительных лицензионных затрат, могут иметь ограниченную поддержку централизованной доменной аутентификации или создавать зависимость от стороннего вендора, что не всегда приемлемо в строго регулируемых корпоративных средах.

OpenSSH для Windows (OpenSSH-Win64)

Решение на базе OpenSSH-Win64, рассмотренное в данной работе, представляет собой нативный порт проверенного временем открытого программного обеспечения. Его ключевые преимущества:

1. Бесплатность и открытость: Отсутствие лицензионных отчислений и возможность аудита кода.
2. Стандартизация и безопасность: Реализация протокола SSH/SFTP, являющегося отраслевым стандартом для защищенного удаленного доступа.
3. Глубокая интеграция с Windows: Возможность использования доменной аутентификации через Active Directory и управления доступом на основе NTFS-прав.
4. Гибкость конфигурации: Тонкая настройка через текстовые конфигурационные файлы (sshd_config), что позволяет реализовывать строгие политики безопасности.

Проведенный анализ позволяет утверждать, что развертывание SFTP на основе OpenSSH-Win64 является оптимальным компромиссом для организаций с развитой инфраструктурой Windows Server. Оно сочетает в себе корпоративный уровень безопасности, бесплатность, отсутствие зависимостей от сторонних вендоров и возможность глубокой интеграции с существующими системами управления идентификацией и доступом. В то время как FTPS отягощен архитектурными недостатками, а сторонние решения добавляют стоимость и сложность управления, OpenSSH-Win64 предоставляет стандартизированный, безопасный и контролируемый канал для защищенного обмена файлами.

Методы исследования

Исследование носит прикладной характер и выполнено в области сетевой безопасности и администрирования информационных систем. Основным методом стало экспериментальное моделирование, направленное на построение, конфигурацию и всестороннее тестирование работоспособной SFTP-инфраструктуры в контролируемых условиях.

Эксперимент проводился в изолированной виртуальной среде на базе платформы Oracle VirtualBox. Стенд моделировал типичную доменную инфраструктуру организации и включал следующие ключевые компоненты:

Контроллер домена (DC): Виртуальная машина с операционной системой Windows Server 2022. На сервере были развернуты и настроены основные роли: Active Directory Domain Services (AD DS) для централизованного управления идентификацией, DNS-сервер и служба хранения файлов. Серверу был назначен статический IP-адрес 10.0.0.2 и создан домен sftp.test. В качестве SFTP-сервера использовался порт OpenSSH-Win64, установленный вне стандартного мастера ролей для детального контроля процесса.

Рабочая станция (CLI): Виртуальная машина под управлением Windows 11, присоединенная к домену sftp.test. Использовалась для эмуляции конечного пользователя и выполнения всех тестовых подключений. Для подключения по протоколу SFTP использовался графический клиент WinSCP версии 6.5.5, как одно из наиболее распространенных решений в данной категории.

Таблица 1 – Конфигурация лабораторного стенда

Роль	ОС	IP-адрес	Домен	Назначение
DC	Windows Server 2022	10.0.0.2	sftp.test	Контроллер домена, DNS, SFTP-сервер
CLI	Windows 11	10.0.0.11	sftp.test	Клиентская станция для тестирования

Исследование проводилось в виде четкой последовательности этапов, имитирующих реальный процесс развертывания сервиса в корпоративной среде:

Подготовка доменной среды и создание субъектов безопасности.

Первоначально была подтверждена корректность доменного окружения проверкой атрибута «Домен» с помощью команды systeminfo на обеих машинах.

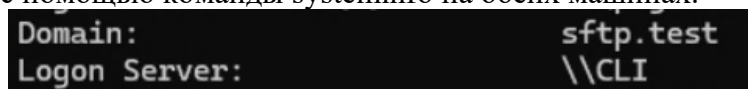


Рис. 1. Проверка домена на машине CLI



Рис. 2. Проверка домена на машине DC

На контроллере домена с использованием оснастки Active Directory Users And Computers были созданы и настроены объекты безопасности:

1. Создано организационное подразделение SFTP_Users для логической группировки учетных записей.
2. Внутри него создана глобальная группа безопасности SFTP_Group.
3. Создана тестовая учетная запись пользователя sftp_user с паролем P@ssw0rd и добавлена в группу SFTP_Group.

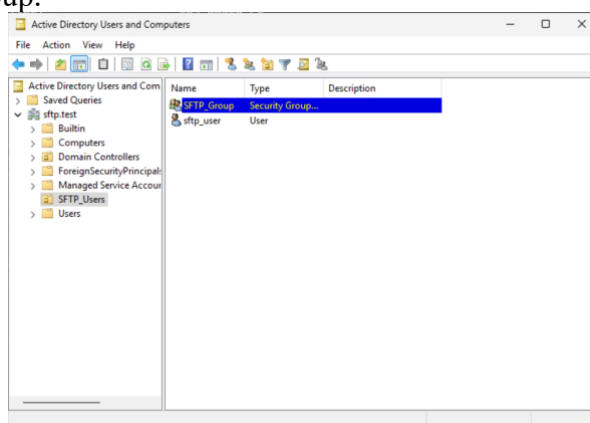


Рис. 3. Активные объекты безопасности SFTP в оснастке Active Directory

Организация файловой системы и управление доступом

На сервере DC создана структура каталогов: корневая папка C:\SFTP_Folder и личный каталог пользователя C:\SFTP_Folder\sftp_user. Права доступа были назначены в соответствии с принципом наименьших привилегий:

1. Группе SFTP_Group на папку C:\SFTP_Folder даны права на чтение и выполнение, на список содержимого папки.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

2. Пользователю sftp_user на папку C:\SFTP_Folder\sftp_user предоставлены права полного доступа.

Наследование разрешений было отключено для обеспечения строгой изоляции.

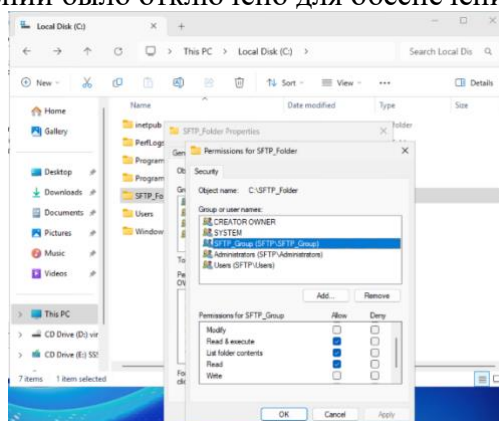


Рис. 4. Права на папку C:\SFTP_Folder

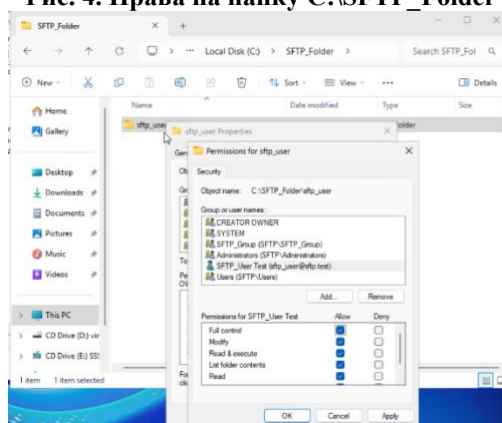


Рис. 5. Права на папку C:\SFTP_Folder\sftp_user

Установка и базовая настройка службы OpenSSH Server

Ввиду отсутствия соответствующей роли в Диспетчере сервера, установка выполнялась вручную:

1. Архив OpenSSH-Win64.zip загружен с официального репозитория GitHub и распакован в C:\SSH\OpenSSH-Win64 [5, 6].
2. С помощью сценария PowerShell .\install-sshd.ps1 установлены службы.
3. Служба sshd переведена в автоматический режим запуска командой Set-Service и активирована.

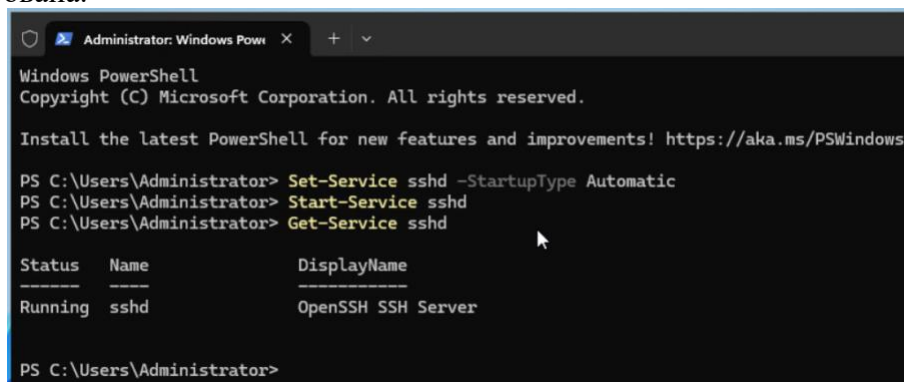


Рис. 6. Запуск сервиса sshd

Настройка сетевого доступа и конфигурация SSH-сервера

Для разрешения входящих подключений в Брандмауэре Защитника Windows создано правило, разрешающее трафик по TCP-порту 22.

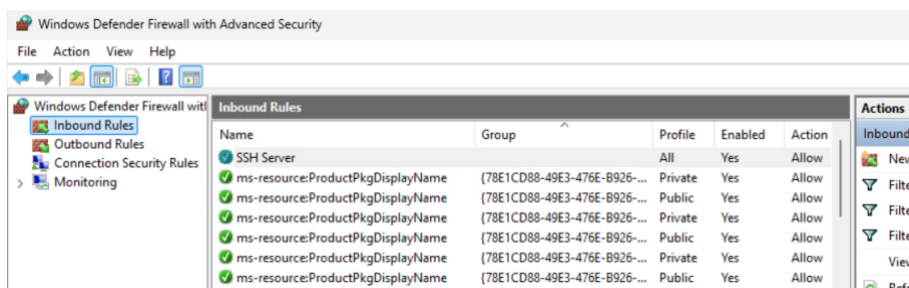


Рис. 7. Правило для порта 22

Основная конфигурация безопасности выполнена путем правки файла C:\ProgramData\ssh\sshd_config. Были проверены и установлены ключевые параметры, включая PasswordAuthentication, PubkeyAuthentication и активацию подсистемы SFTP.

```
sshd_config - Notepad
File Edit Format View Help
ListenAddress 0.0.0.0
LogLevel VERBOSE
Protocol 2

# override default of no subsystems
Subsystem sftp C:\SSH\OpenSSH-Win64\sftp-server.exe

# ===== НАСТРОЙКИ ДЛЯ SFTP ПОЛЬЗОВАТЕЛЕЙ =====

# Изоляция пользователей группы SFTP_Group
Match Group SFTP_Group
  ChrootDirectory C:\SFTP_Folder
  ForceCommand internal-sftp
  AllowTcpForwarding no
  X11Forwarding no

PasswordAuthentication yes
PubkeyAuthentication yes
PermitEmptyPasswords no
```

Рис. 8. Исправленный файл C:\ProgramData\ssh\sshd_config

Установка и настройка SFTP-клиента WinSCP на рабочей станции

Для тестирования функциональности развернутого SFTP-сервера на клиентской виртуальной машине (CLI) была произведена установка графического клиента WinSCP. Данное ПО было выбрано как одно из наиболее распространенных, удобных и функциональных решений для работы по протоколу SFTP в среде Windows. Процедура включала следующие шаги:

1. На машину CLI была загружена последняя версия установочного пакета WinSCP 6.5.5 с официального сайта [7].
2. Установка выполнялась с параметрами по умолчанию, что подразумевало установку всех необходимых компонентов и создание ярлыка на рабочем столе.

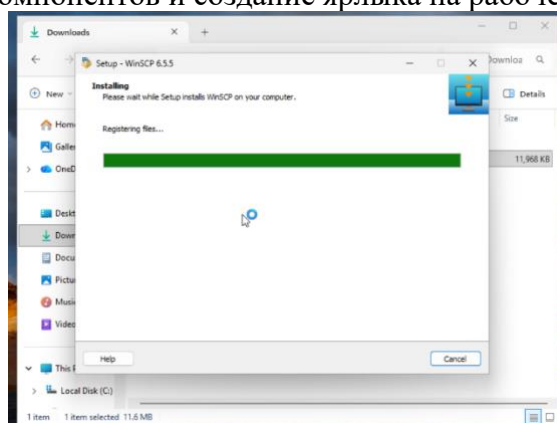


Рис. 9. Окно успешной установки WinSCP на клиентской машине CLI

Функциональное тестирование подключения и операций с файлами

Ключевым этапом исследования являлось тестирование работоспособности всей настроенной инфраструктуры. Подключение инициировалось с клиентской машины CLI с использованием установленного WinSCP. Параметры сессии были заданы следующим образом:

Имя хоста (Host name): 10.0.0.2 (IP-адрес сервера DC).

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Имя пользователя (User name): sftp_user.

Пароль (Password): P@ssw0rd.

Протокол (File protocol): SFTP.

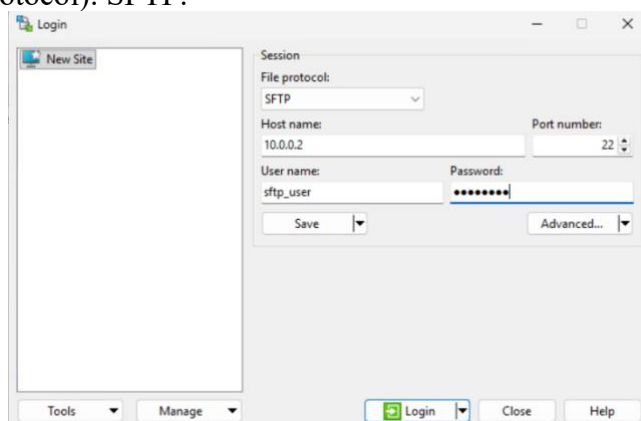


Рис. 10. Подключение с использованием установленного WinSCP

Успешное подключение привело к открытию интерфейса WinSCP, где в правой панели отобразилось содержимое домашнего каталога пользователя – C:\SFTP_Folder\sftp_user. Это подтвердило корректность настройки маршрутизации сессии в личную директорию.

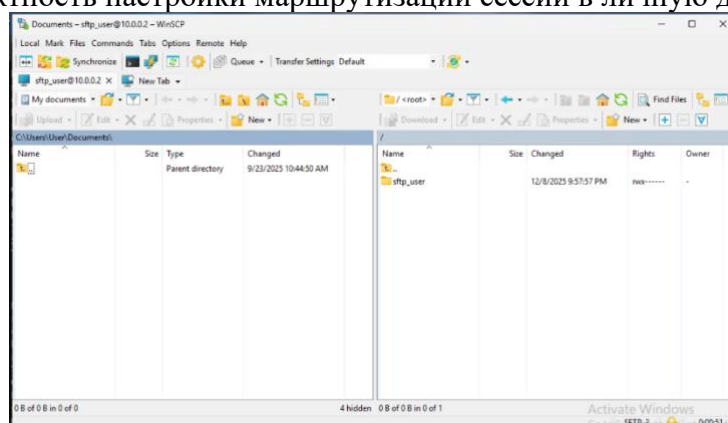


Рис. 11. Интерфейс WinSCP с установленной SFTP-сессией и отображением файлов в домашнем каталоге пользователя

Для всесторонней оценки были проведены следующие тестовые сценарии:

1. Тест успешной аутентификации и навигации: Убедились, что вход выполняется, а пользователь видит файлы только в разрешенной папке.
2. Тест передачи файла: С локального диска клиента (CLI) в домашний каталог на сервере был успешно передан тестовый текстовый файл.
3. Тест изоляции сессии: Была предпринята попытка навигации на уровень выше (/ или C:\SFTP_Folder) с помощью кнопки «Наверх» в WinSCP. Система корректно отклонила запрос, отобразив ошибку «Отказано в доступе» (Permission denied), что свидетельствует об эффективной работе ограничений на основе прав NTFS.
4. Негативное тестирование аутентификации: Попытка входа с неверным паролем привела к ожидаемой ошибке «Аутентификация не удалась» (Authentication failed), подтверждая надежность механизма проверки учетных данных.
5. Тест реакции на отсутствие сети: Моделировалась ситуация разрыва сетевого соединения, в ходе которой сессия WinSCP корректно прерывалась.

Результаты исследования

Экспериментальное развертывание и тестирование SFTP-инфраструктуры на базе Windows Server в доменной среде подтвердило полную достижимость поставленных целей. Результаты исследования демонстрируют корректную работу всех ключевых компонентов системы.

1. Успешное развертывание и запуск служб. На контроллере домена была установлена и запущена служба OpenSSH-Win64. Интеграция с операционной системой прошла

успешно: служба sshd функционировала в режиме автоматического запуска, а конфигурационный файл sshd_config был адаптирован для поддержки доменной аутентификации.

2. Функционирование системы управления доступом. Модель безопасности, основанная на связке Active Directory и прав NTFS, подтвердила свою эффективность. Созданная учетная запись sftp_user успешно аутентифицировалась в домене. Назначенные права доступа к файловой системе обеспечили реализацию принципа наименьших привилегий: пользователь имел полный контроль только в рамках своего изолированного каталога (C:\SFTP_Folder\sftp_user).
3. Подтверждение базовой функциональности SFTP. Тестовые подключения с использованием клиента WinSCP доказали полную работоспособность сервера. Вход по доменным учетным данным выполнялся стабильно. Копирование тестового файла происходило успешно, что подтверждает практическую пригодность системы. Попытки выхода за пределы разрешенного домашнего каталога немедленно блокировались системой с возвратом стандартной ошибки «Отказано в доступе» (Permission denied).
4. Результаты тестирования безопасности и выявленные уязвимости. В ходе исследования была проведена серия тестов для оценки устойчивости системы к типовым угрозам. Результаты представлены в Таблице 2.

Таблица 2 – Анализ угроз безопасности SFTP-сервера и результаты тестирования

Тип атаки	Описание	Условия	Последствия
Brute-force	Перебор паролей SFTP-пользователя	Слабая политика паролей, отсутствие блокировки аккаунтов	Взлом учетной записи, получение доступа к данным
Попытка выхода за пределы chroot (Chroot Escape)	Пользователь пытается перейти в каталог выше /sftp_user	Ошибки NTFS-прав	Просмотр/изменение системных файлов
Получение shell-доступа вместо SFTP	Попытка вызвать команду вместо SFTP	ForceCommand не настроен	Вредоносные команды, изучение структуры сервера
Перехват логов и сессий	Попытка доступа к логам sshd	Неограниченные права на ProgramData\ssh	Сбор логинов, следов активности

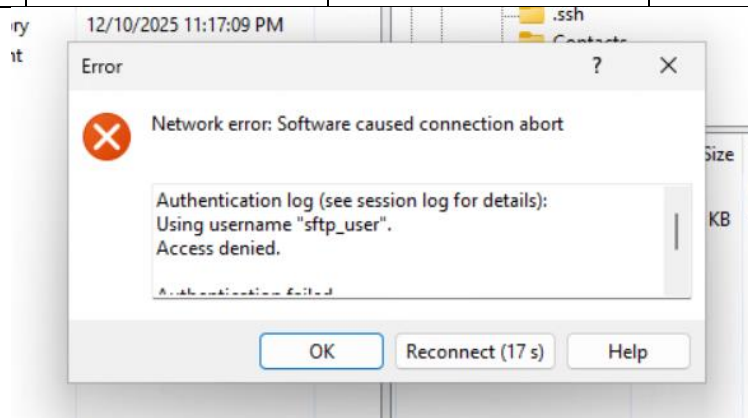


Рис. 12. Запрет доступа при переборе паролей (Brute-force)

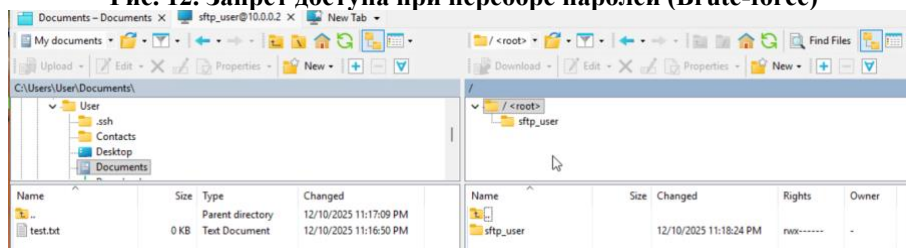


Рис. 13. Изоляция каталогов при попытке выхода за пределы chroot (Chroot Escape)

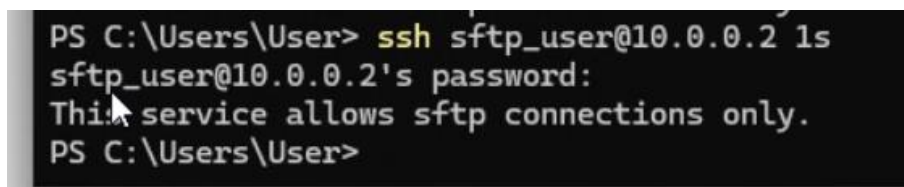


Рис. 14. Ошибка получения shell-доступа вместо SFTP

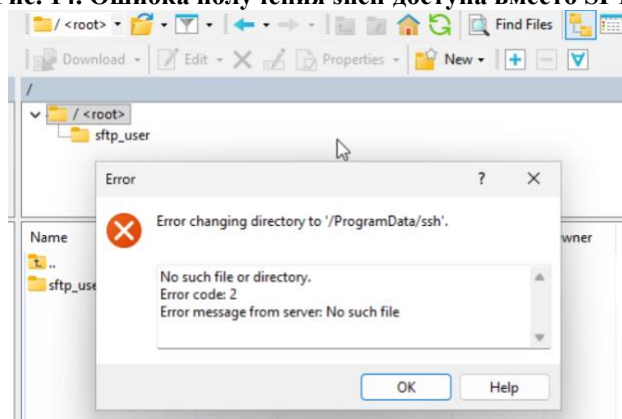


Рис. 15. Ошибка при попытке просмотра логов в каталоге ProgramData

Таблица 3 – Проверка устойчивости SFTP-сервера к угрозам

Угроза	Как проводилось тестирование	Результат
Brute-force	10 неверных попыток входа подряд	Учетная запись заблокирована
Попытка выхода за пределы chroot (Chroot Escape)	Попытка перейти выше корневой папки	Изоляция каталогов
Получение shell-доступа вместо SFTP	Попытка выполнить SSH-команду (ssh user@server ls)	Команда запрещена, сервер выдает ошибку
Перехват логов и сессий	Попытка зайти в C:\ProgramData\ssh из WinSCP	Полный отказ

Следует отметить, что блокировка учётной записи в Active Directory при неудачных попытках входа, будучи эффективной против Brute-force, несёт риск атаки типа «отказ в обслуживании» (DoS). Злоумышленник может намеренно вызвать блокировку аккаунта легитимного пользователя, лишив его доступа к SFTP и другим ресурсам. Для повышения отказоустойчивости рекомендуется дополнить защиту механизмами блокировки IP-адреса источника атаки, например, с помощью аналогов Fail2ban для Windows (IPBan, PowerShell-скрипты для анализа логов sshd) или настройки динамических правил в брандмауэре Windows. Это позволит сохранить доступ пользователям, изолируя только враждебные IP-адреса.

5. Сводная оценка защищенности. Настроенная конфигурация SFTP-сервера показала высокий уровень защищенности от основных угроз, связанных с несанкционированным доступом и перехватом данных. Ключевыми факторами, обеспечивающими этот результат, стали:
 2. Использование криптографически стойкого протокола SSH (SFTP) вместо FTP.
 3. Интеграция с централизованной системой аутентификации и политиками паролей Active Directory.
 4. Применение модели разграничения доступа на основе NTFS с принципом наименьших привилегий.
 5. Базовая настройка брандмауэра для ограничения сетевого доступа.

Заключение

Проведенное исследование было посвящено практической реализации защищенного протокола передачи файлов SFTP в корпоративной среде на базе инфраструктуры Windows Server с использованием доменных служб Active Directory. Основной целью работы являлась разработка, апробация и всестороннее тестирование методики развертывания такого решения. Все поставленные задачи были успешно выполнены, что позволяет сформулировать следующие выводы.

Основные достижения исследования:

1. Техническая реализуемость подтверждена. На базе контроллера домена Windows Server 2022 успешно развернут и интегрирован SFTP-сервер на основе открытого решения OpenSSH-Win64. Детально проработанная процедура установки, настройки файла конфигурации `sshd config` и интеграции с системой управления доступом Active Directory доказала свою эффективность и воспроизводимость.
2. Создана безопасная и управляемая архитектура. Ключевым результатом стала работоспособная модель безопасности, объединяющая централизованную доменную аутентификацию и детальное разграничение прав на уровне файловой системы NTFS. Созданный прототип системы продемонстрировал корректную работу принципа наименьших привилегий, эффективно изолируя пользовательские сессии в пределах назначенных каталогов и надежно защищая данные от несанкционированного доступа.
3. Функциональность и устойчивость верифицированы. Комплексное тестирование подтвердило полную работоспособность системы в штатных и нештатных сценариях. SFTP-сервер обеспечивает стабильное шифрованное соединение, надежную аутентификацию пользователей, корректную передачу файлов и адекватную реакцию на ошибочные или враждебные действия (неверные учетные данные, попытки выхода за границы разрешенной зоны доступа).

Разработанная методика обладает непосредственной практической ценностью для системных администраторов и специалистов по информационной безопасности. Она предоставляет готовый алгоритм для быстрого внедрения безопасного канала передачи файлов вместо устаревших и уязвимых протоколов в существующей Windows-инфраструктуре.

Важным результатом работы является не только пошаговая инструкция по настройке, но и проведенный анализ защищенности. Экспериментальное тестирование на устойчивость к основным классам угроз показало, что базовая конфигурация с использованием доменной аутентификации и NTFS-прав обеспечивает высокий уровень безопасности.

При этом важно отметить специфические ограничения реализации OpenSSH на Windows. В отличие от Linux-версии, где полноценно работает механизм `chroot` (`ChrootDirectory`) для изоляции пользователей в заданном каталоге, в Windows эта функция реализована ограниченно и опирается на комбинацию настроек SSH и прав NTFS. Это может приводить к особенностям управления доступом в гетерогенных средах, где требуются единые политики для Unix-подобных и Windows-систем. Кроме того, управление разрешениями на основе NTFS (в отличие от POSIX-прав в Linux) требует дополнительного внимания при настройке наследующих разрешений и аудите доступа. Эти особенности необходимо учитывать при планировании развертывания в смешанной инфраструктуре.

Направлениями для углубленного изучения могут стать:

- Реализация полноценного механизма ограничения корневого каталога (`ChrootDirectory`) в среде Windows для создания более строгих изолированных сред.
- Интеграция SFTP-сервера с системами многофакторной аутентификации на основе смарт-карт или TOTP-токенов.
- Разработка сценариев автоматизации управления жизненным циклом SFTP-аккаунтов (создание, ротация ключей, деактивация) с использованием PowerShell и возможностей Active Directory.
- Проведение нагрузочного тестирования и аудита безопасности (пентестинг) развернутой системы для оценки ее устойчивости в условиях реальной эксплуатации.

Таким образом, исследование подтвердило, что современные открытые технологии в синергии со стандартными платформенными службами Microsoft позволяют создавать в корпоративных сетях Windows надежные, безопасные и легко управляемые решения для защищенного обмена данными, полностью отвечающие актуальным требованиям кибербезопасности.

Библиографический список

1. Автайкин Р. А. ОСОБЕННОСТИ ПРОТОКОЛА FTP // Цифровые технологии в науке и образовании. – 2022. – С. 50–53.
2. Основы и применение протокола FTP // Skyeng. – 2025. – URL: <https://skyeng.ru/it-industry/it/kak-rabotaet-ftp-protokol-i-ego-primenenie/> (дата обращения: 02.12.2025).
3. Совкова О. И. ОПТИМИЗАЦИЯ ПЕРЕДАЧИ ФАЙЛОВ ДЛЯ ВЫСОКОСКОРОСТНОЙ ПЕРЕДАЧИ ДАННЫХ // Наука. Исследования. Практика. – 2019. – С. 161–164.
4. Орлов А. Г. АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ // Состав редакционной коллегии и организационного комитета. – 2025.
5. Win32-OpenSSH // GitHub. – 2025. – URL: <https://github.com/PowerShell/Win32-OpenSSH/releases> (дата обращения: 02.12.2025).
6. Настройка SFTP (SSH FTP) сервера в Windows // WINITPRO. – 2016. – URL: <https://winitpro.ru/index.php/2016/03/31/sftp-ssh-ftp-na-windows-server-2012-r2/> (дата обращения: 02.12.2025).
7. WinSCP 6.5.5 // WinSCP. – 2025. – URL: <https://winscp.net/eng/download.php> (дата обращения: 02.12.2025).

References

1. Avtaikin, R. A. (2022). Features of the FTP protocol. In Digital technologies in science and education (pp. 50–53).
2. Fundamentals and application of the FTP protocol. (2025). Skyeng. <https://skyeng.ru/it-industry/it/kak-rabotaet-ftp-protokol-i-ego-primenenie/>
3. Sovkova, O. I. (2019). File transfer optimization for high-speed data transmission. In Science. Research. Practice (pp. 161–164).
4. Orlov, A. G. (2025). Analysis of vulnerabilities of data transfer protocols. Composition of the editorial board and organizing committee.
5. PowerShell. (2025). Win32-OpenSSH [Computer software]. GitHub. <https://github.com/PowerShell/Win32-OpenSSH/releases>
6. Setting up an SFTP (SSH FTP) server in Windows. (2016). WINITPRO. <https://winitpro.ru/index.php/2016/03/31/sftp-ssh-ftp-na-windows-server-2012-r2/>
7. WinSCP. (2025). WinSCP 6.5.5 [Computer software]. <https://winscp.net/eng/download.php>

Информация об авторах

Ляхова Мария Владимировна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mariahlyahova@yanfex.ru

Сеникова Наталья Григорьевна — студентка, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: zraa2120@gmail.com

SETUP AND FUNCTIONAL TESTING OF SFTP (SSH FTP) ON WINDOWS SERVER. SECURITY CONSIDERATIONS

Lyahova M. V.¹, Senikova N. G.¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article addresses secure file transfer in corporate networks based on Windows Server. The study is motivated by the continued use of FTP, which can expose credentials and file contents to interception and unauthorized access. Its purpose is to develop and experimentally verify a methodology for deploying an SFTP server based on OpenSSH-Win64 in a Windows domain environment. The procedure includes preparing Active Directory security objects, configuring directories and NTFS permissions according to the principle of least privilege, setting up the sshd service and Windows Firewall, restricting user sessions to SFTP functionality, and connecting through WinSCP. The experiment was performed in an isolated Oracle VirtualBox environment with Windows Server 2022 and Windows 11. Functional testing confirmed domain authentication, file transfer, user isolation within the permitted directory, and correct handling of invalid credentials and network loss. Security-oriented scenarios included brute-force attempts, attempts to leave the permitted directory, attempts to obtain shell access, and attempts to access server-side log locations. The results show that the combined use of Active Directory, NTFS, and OpenSSH provides manageable access control. However, account

lockout during password guessing can be abused for denial-of-service attacks and should be supplemented by source-based blocking. The study also discusses Windows-specific OpenSSH isolation limitations compared with the Linux chroot mechanism.

Keywords: *SFTP, SSH, secure file transfer, OpenSSH for Windows, Active Directory, key-based authentication, user isolation.*

Information about the authors

Lyahova Mariya Vladimirovna — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: mariahlyahova@yanfex.ru

Senikova Natalya Grigoryevna — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: zraa2120@gmail.com