МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт Математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

01.03.02 Прикладная математика и информатика
(код и наименование направления подготовки, специальности)

Компьютерные технологии и математическое моделирование
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Моделирование системы контроля удалённого доступа при подключениях SSH, RDP и VPN»

Обучающийся О.А. Иванов
(И.О. Фамилия) (личная подпись)

Руководитель Г.А. Тырыгина
(ученая степень, звание, И.О. Фамилия)

Консультант О.А. Головач
(ученая степень, звание, И.О. Фамилия)

Тольятти 2023

Аннотация

Тема бакалаврской работы: «Контроль удалённого доступа при подключениях SSH, RDP и VPN».

Бакалаврская работа посвящена контролю удалённого доступа при подключениях SSH, RDP и VPN.

В ходе выполнения исследований по бакалаврской работе была поставлена задача на исследование, описаны протоколы SSH, RDP и VPN и проведен сравнительный анализ. Так же спроектирован удаленный доступ и реализован удаленный доступ.

Во введении прописывается актуальность темы, написаны цель и задачи.

В первой главе описаны задачи на исследование, был рассмотрен удаленный доступ, а так же подробно описан каждый протокол: SSH, RDP, VPN и проводится анализ аналогов.

Вторая глава ВКР посвящена описанию архитектуры и моделированию контроля удалённого доступа. Также были описаны физическая и логическая модель. И была создана диаграмма компонентов.

Третья глава была посвящена реализации удаленного доступа, мы подключились к удаленному компьютеру по протоколу RDP, а внутри тоннель SSH с помощью ключей, и установленный SSL VPN Plus для контроля.

В заключении представлены результаты выполнения выпускной квалификационной работы.

Бакалаврской работа состоит из введения, трёх глав, заключения и списка использованной литературы.

Бакалаврская работа состоит из 47 страниц, 30 рисунков, 1 таблиц и 25 источников.

Abstarst

The title of the bachelor’s thesis is “Remote access control for SSH, RDP and VPN connections”.

The research is devoted to remote access control for SSH, RDP and VPN connections.

When doing a research, task is set, SSH, RDP and VPN protocols are described and a comparative analysis is carried out. Remote access is also designed and remote access is implemented.

The introduction reveals the relevance of the research and gives a brief description of the work done.

The first chapter, the research tasks are described, remote access was considered, as well as each protocol is described in detail: SSH, RDP, VPN and an analysis of analogues is carried out.

The second chapter of the WRC is devoted to the description of the architecture and modeling of remote access control. The physical and logical model were also described. And a component diagram was created.

The third chapter was devoted to the implementation of remote access, we connected to a remote computer using the RDP protocol, and inside the SSH tunnel using keys, and installed SSL VPN Plus for control.

In conclusion, the conclusions of the entire work are drawn.

The bachelor’s thesis consists of an introduction, three chapters, a conclusion and list of used literature.

The volume of the bachelor's thesis is 47 pages, it also contains 30 figures, 1 table, and a list of 25 references.

Содержание

Введение 5
1. Теоретические основы удаленного доступа 7
1.1 Постановка задачи 7
1.2 Удаленный доступ 8
1.3 Протокол SSH 9
1.4 Протокол RDP 11
1.5 VPN 13
1.6 Сравнительный анализ аналогов 14
2. Проектирование удаленного доступа 18
2.1 Моделирование архитектуры системы 18
2.2 Модель данных 20
2.3 Диаграмма компонентов 22
2.4 Контроль удаленного доступа 23
3. Реализация удаленного доступа 25
Заключение 44
Список используемой литературы 45

Введение

Эпоха цифровых технологий повлияла на то, как люди работают и общаются друг с другом. Внедрение облачных вычислений, удаленного доступа и виртуальных частных сетей (VPN) позволило предприятиям работать более эффективно и безопасно, чем когда-либо прежде. Однако с такой повышенной эффективностью возникает повышенный риск несанкционированного доступа к конфиденциальной информации и данным. Таким образом, для предприятий важно внедрить безопасные меры контроля доступа, чтобы гарантировать, что только авторизованным пользователям разрешен доступ к корпоративным сетям, данным и приложениям [10].

Одним из наиболее распространенных методов, используемых для установления безопасного управления доступом, является использование протоколов управления удаленным доступом, таких как соединения SSH, RDP и VPN. SSH (SecureShell) – это сетевой протокол, который позволяет пользователям безопасно выполнять команды и передавать файлы по зашифрованному соединению. RDP (протокол удаленного рабочего стола) – это протокол удаленного доступа, который позволяет пользователю получать доступ к компьютеру и управлять им через Интернет. Наконец, VPN (виртуальная частная сеть) – это безопасный туннель, через который данные шифруются и отправляются через Интернет, что обеспечивает дополнительный уровень безопасности.

В сочетании эти протоколы управления доступом обеспечивают комплексный подход к безопасному удаленному доступу. Протоколы должны быть правильно настроены, чтобы обеспечить наивысший уровень безопасности и ограничить доступ только тем пользователям, которым предоставлено разрешение. Кроме того, необходимо регулярно контролировать протоколы, чтобы убедиться, что они работают должным образом и что неавторизованные пользователи не могут получить доступ к системе.

Актуальность данной темы заключается в том, что при подключениях SSH, RDP и VPN необходимо обеспечить безопасность при передаче данных и доступа к системам. В таких случаях необходимо использовать различные методы контроля удаленного доступа, которые обеспечат безопасность при передаче данных и доступа к системам.

Объектом является удалённый доступ при подключениях SSH, RDP и VPN.

Предметом является контроль системы удаленного доступа.

Цель работы: смоделировать систему контроля удаленного доступа при подключениях SSH, RDP и VPN.

Для решения данной цели, необходимо выполнить следующие задачи:

- описать теоретические основы удаленного доступа;
- спроектировать систему удаленного доступа;
- реализовать систему удаленного доступа.

1. Теоретические основы удаленного доступа

1.1 Постановка задачи

Для выполнения выпускной квалификационной работы необходимо разобраться, что же нужно сделать:

- определить уровень доступа, который мы хотим предоставить удаленным пользователям. В зависимости от требований безопасности организации нам может потребоваться ограничить доступ к определенным ресурсам или ограничить количество пользователей, которые могут подключаться удаленно;
- создать политику удаленного доступа, определяющую права и обязанности удаленных пользователей. Убедится, что политика соответствует всем нормативным требованиям или отраслевым стандартам;
- настроить для применения политики при подключении удаленных пользователей. Это может включать настройку фильтров или списков управления доступом для ограничения или разрешения доступа к определенным ресурсам;
- отслеживать активность удаленного доступа, чтобы видеть любой несанкционированный доступ или необычную активность. Рассмотреть возможность использования таких инструментов, как системы обнаружения вторжений (IDS) или программное обеспечение для управления информацией и событиями безопасности (SIEM), чтобы помочь в этом;
- регулярно проверять и обновлять политику и параметры по мере необходимости, чтобы убедиться, что они по-прежнему эффективны при управлении удаленным доступом.

1.2 Удаленный доступ

Удаленный доступ – это возможность доступа к компьютеру, сети или приложению из другого места с помощью сетевого подключения. Удаленный доступ обычно используется в современном деловом мире, чтобы позволить сотрудникам получать удаленный доступ к сети и приложениям своей компании, что позволяет им оставаться на связи и продуктивно работать, даже если они находятся за пределами физического офиса.

Существует множество различных методов предоставления удаленного доступа, каждый из которых имеет свои преимущества и недостатки. Наиболее распространенными методами удаленного доступа являются виртуальные частные сети (VPN), протокол удаленного рабочего стола (RDP) и средства удаленного администрирования.

Виртуальные частные сети (VPN) – это безопасное соединение между двумя или более компьютерами, позволяющее пользователям получать доступ к частной сети извне. Они используют расширенные протоколы безопасности для шифрования данных и обеспечения их безопасности во время передачи. Виртуальные частные сети также обеспечивают аутентификацию и авторизацию, позволяя пользователям получать доступ только к тем ресурсам, на которые они авторизованы.

Протокол удаленного рабочего стола (RDP) – это собственный протокол, разработанный Microsoft, который позволяет пользователям получать доступ к удаленному компьютеру через сетевое соединение. RDP использует шифрование и аутентификацию для защиты соединения и предоставления доступа к приложениям и данным, расположенным на удаленном компьютере.

Средства удаленного администрирования – это специализированные приложения, которые используются для удаленного управления и контроля за компьютером. Эти инструменты позволяют пользователям получать доступ к удаленному компьютеру, выполнять команды и управлять такими

функциями, как управление файлами, установка программного обеспечения и настройка системы.

В дополнение к упомянутым выше методам удаленный доступ также может быть обеспечен через web-приложения и облачные вычисления. Web-приложения позволяют пользователям получать доступ к приложениям и использовать их через web-браузер. Облачные вычисления обеспечивают удаленный доступ к приложениям и данным без необходимости их локальной установки на компьютер пользователя [14].

Независимо от того, какой метод удаленного доступа используется, самое главное – обеспечить безопасность подключения к удаленному компьютеру и правильность аутентификации и авторизации пользователя. Компании также должны обеспечить наличие надлежащих процедур для защиты своих данных и информации.

1.3 Протокол SSH

Протокол SecureShell (SSH) – это сетевой протокол, используемый для безопасной передачи данных между двумя компьютерами. Это безопасная альтернатива традиционному протоколу telnet.

Протокол SSH обеспечивает безопасный канал связи между двумя компьютерами с использованием зашифрованного соединения. Он используется для доступа к удаленным системам, передачи файлов и выполнения команд на удаленной машине [19].

Протокол SSH состоит из двух компонентов: клиента SSH и сервера SSH. Клиент – это программа, которая инициирует соединение, а сервер получает запрос. На рисунке 1 переадресация портов SSH.

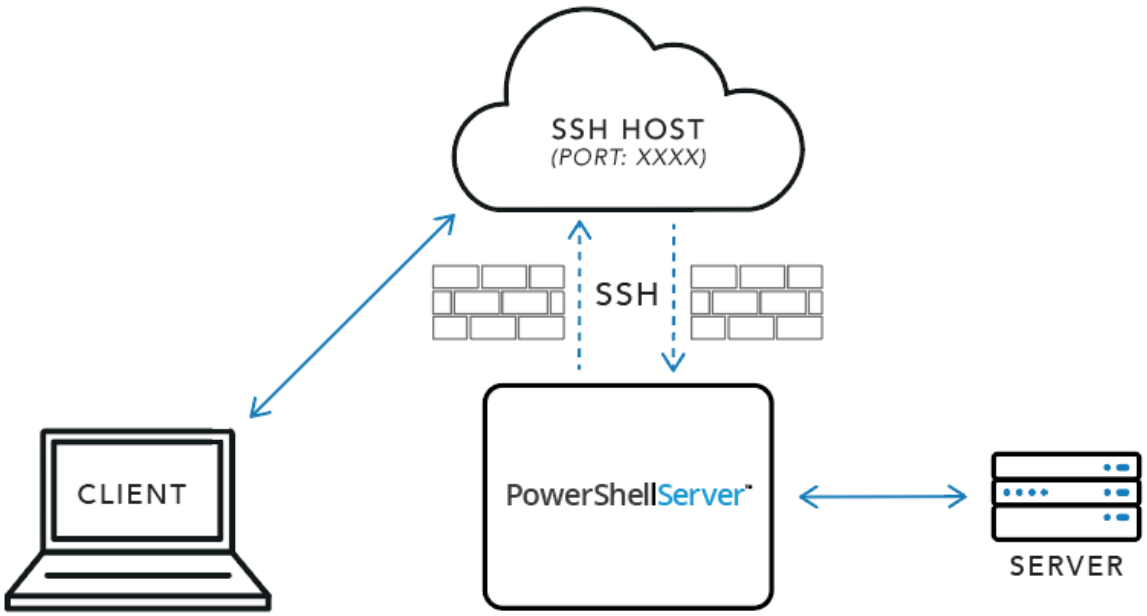

Рисунок 1 – Переадресация портов SSH

Протокол SSH использует порт 22 для начального подключения. После того, как начальное соединение установлено, протокол SSH согласовывает безопасный туннель для передачи данных.

Протокол SSH поддерживает различные методы аутентификации, такие как аутентификация с открытым ключом, аутентификация по паролю и аутентификация на основе хоста. Протокол SSH также поддерживает несколько методов шифрования, включая Advanced Encryption Standard (AES) и Triple Data Encryption Standard (3DES).

Протокол SSH поддерживает несколько функций, таких как переадресация портов, переадресация X11 и туннелирование. Протокол SSH также поддерживает передачу файлов, что позволяет пользователям безопасно передавать файлы между двумя компьютерами [25].

Протокол SSH также поддерживает мультиплексирование сеансов, позволяя устанавливать несколько сеансов через один и тот же безопасный туннель. Это позволяет пользователям запускать несколько команд и приложений по одному и тому же безопасному соединению.

Протокол SSH также поддерживает пересылку агента аутентификации, что позволяет клиенту пересылать аутентификационную информацию на удаленный сервер. Эта функция позволяет пользователям использовать один и тот же метод аутентификации на нескольких удаленных компьютерах без необходимости многократного ввода одних и тех же учетных данных.

Протокол SSH также поддерживает методы обмена ключами, что позволяет двум компьютерам безопасно обмениваться криптографическими ключами. Это позволяет шифровать и расшифровывать данные с использованием одного и того же ключа.

Протокол SSH также поддерживает сжатие, что позволяет сжимать данные перед передачей по сети. Это уменьшает объем сетевого трафика и ускоряет передачу данных [1], [9].

Протокол SSH поддерживает несколько других функций, таких как совместное использование соединений, протоколы туннелирования и выполнение прокси-команд. Протокол SSH также поддерживает запросы на подключение к данным, позволяя приложениям получать доступ к удаленным ресурсам через зашифрованное соединение.

В целом, протокол SSH – это безопасный и гибкий протокол, используемый для удаленного доступа и безопасной передачи файлов. Благодаря своим различным функциям и поддержке нескольких методов аутентификации это важный инструмент для безопасного удаленного доступа.

1.4 Протокол RDP

Протокол удаленного рабочего стола (RDP) – это собственный протокол, разработанный Microsoft, который предоставляет пользователю графический интерфейс для подключения к другому компьютеру через сетевое соединение. Он основан на протоколе T.120 и используется в основном для предоставления графического интерфейса удаленному

компьютеру. RDP используется многими организациями для предоставления удаленной поддержки и доступа к системам, приложениям и данным. На рисунке 2 представлена настройка безопасности RDP.

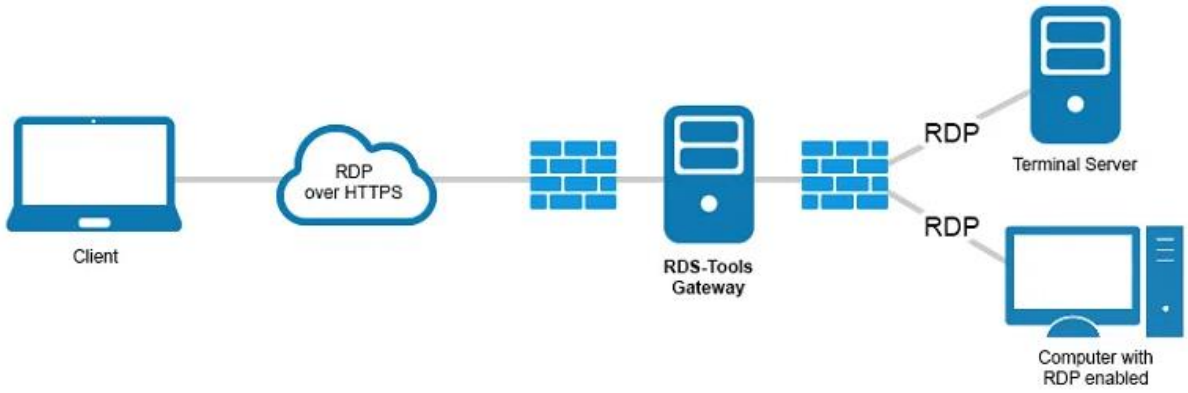

Рисунок 2 – Настройка безопасности протокола RDP

RDP предоставляет широкий набор функций, которые позволяют пользователям удаленно выполнять задачи, такие как совместное использование файлов и принтеров, воспроизведение аудио и предоставление удаленной поддержки. Он также обеспечивает зашифрованное соединение, помогающее защитить конфиденциальность данных и сообщений по сети. Он также предоставляет возможность передавать файлы между компьютерами, а также копировать и вставлять текст и изображения с одного компьютера на другой.

RDP – это безопасный протокол, предлагающий аутентификацию, шифрование, целостность и конфиденциальность данных. Он также включает алгоритмы сжатия трафика и дифференциального сжатия, которые повышают производительность передачи данных. Кроме того, RDP можно использовать для доступа к приложениям и службам на разных платформах, что позволяет пользователю работать с приложениями из разных операционных систем [5], [15].

1.5 VPN

Технология виртуальной частной сети (VPN) – это безопасное и зашифрованное соединение между двумя или более компьютерами или устройствами через Интернет. Он обеспечивает доступ к ресурсам, которые обычно доступны только через локальную сеть (LAN) или интернет. VPN используются для безопасного подключения удаленных офисов и отдельных лиц друг к другу, а также для безопасного доступа к приложениям и ресурсам, расположенным в удаленной сети [2], [7], [24].

Когда пользователь подключается к VPN, соединение устанавливается с использованием специального протокола, называемого протоколом туннелирования. Этот протокол шифрует все данные, передаваемые между двумя компьютерами, используя защищенный туннель. Этот туннель устанавливается с использованием технологий шифрования и аутентификации. Шифрование гарантирует, что данные защищены от любого несанкционированного доступа или модификации, а аутентификация гарантирует, что только авторизованные пользователи могут получить доступ к данным. На рисунке 3 можно увидеть принцип работы VPN.

Рисунок 3 – Принцип работы VPN

Одним из основных преимуществ использования VPN является его способность маскировать online-активность пользователя от интернет-

провайдера или любого другого стороннего наблюдателя. Это связано с тем, что все данные, отправляемые через VPN-туннель, шифруются и отправляются безопасным способом. Это предотвращает отслеживание сторонними лицами online-активности пользователя или идентификацию реального IP-адреса пользователя. Кроме того, виртуальные частные сети также защищают пользователей от вредоносных Web-сайтов, поскольку они не смогут получить доступ к информации, отправляемой на компьютер пользователя или с него.

Помимо обеспечения безопасного соединения, виртуальные частные сети также предлагают ряд других преимуществ, включая повышенную скорость и надежность. Используя VPN, пользователи могут испытывать меньшую задержку и более высокую скорость загрузки. Направляя трафик через безопасный туннель, виртуальные частные сети также могут помочь сократить количество обрывов соединений.

В целом, VPN – это универсальный и безопасный способ доступа к удаленным сетям и приложениям. Они обеспечивают пользователям безопасное соединение, повышенную скорость и надежность, а также защиту от вредоносных Web-сайтов [3].

1.6 Сравнительный анализ аналогов

По мере того как компании расширяют свою IT-инфраструктуру, они часто сталкиваются с проблемой управления привилегированными учетными записями. Возможным решением этой проблемы является внедрение системы управления привилегированным доступом (PAM). Хотя Indeed PAM 2.0 является относительно новым продуктом, он эффективно выполняет основные функции, необходимые для систем PAM, и имеет удобный интерфейс. Несмотря на то, что он может не предлагать такой же уровень функциональности и поддержки определенных устройств и протоколов, как некоторые из его конкурентов. Indeed PAM может завоевать популярность на

внутреннем рынке, поскольку это продукт, разработанный в России, и компания открыта для сотрудничество с клиентами для усовершенствования продукта в соответствии с их индивидуальными потребностями.

IT BASTION – компания, предлагающая на отечественном рынке ряд программных продуктов, в том числе СКДПУ (Система мониторинга действий поставщиков IT-услуг). Первоначально система была дистрибьютором Wallix, но с тех пор была разработана собственная система управления привилегированными пользователями. Система СКДПУ сертифицирована Минкомсвязи РФ, имеет допуски НДВ-4 ФСТЭК России и НДВ-2 Минобороны РФ [17], [22].

Система СКДПУ имеет несколько функций, в том числе логирование сеансов удаленного доступа пользователей по SSH, SCP/SFTP, RDP, VNC, Telnet, Rlogin, а также RS-242 и RS-485 – запись операций с клавиатуры, запись видео, методы OCR. Пользователи могут использовать стандартные средства подключения консоли SSH или RDP, такие как Putty и mstsc. Система также имеет единую точку входа и управление паролями для привилегированных пользователей с возможностью прозрачной аутентификации на целевых устройствах.

Система СКДПУ является масштабируемой и может использоваться в географически распределенных установках. Он отслеживает введенные команды текстовых сеансов, ввод с клавиатуры, запуск приложений и анализ изображений с помощью методов OCR. Он также поддерживает черные списки действий и команд и может интегрироваться с внешними каталогами, такими как Active Directory и LDAP. Система может работать с брокером фермы RDP серверов Windows версии 2012 и выше и может интегрироваться с внешними системами через свой API. Система СКДПУ работает без использования агентов и доступна в форматах Virtual Appliance и PACK [8].

Российская компания Zecurion предлагает гибкую систему управления привилегированным доступом (PAM), которую можно настроить под нужды любой организации. Разработанная как для малых предприятий, так и для

крупных учреждений, программа может быть интегрирована в существующую IT-инфраструктуру организации на уровне протокола, что делает ее гибкой для настройки. Решение обеспечивает централизованное хранение учетных записей с исчерпывающим набором прав, что позволяет изолировать критические объекты сети для сохранения строгого контроля над доступом к ним. Он также поддерживает безопасный архив сеансов и регистрирует действия привилегированных пользователей. Система имеет усовершенствованный механизм отчетности, который обеспечивает детальный подход к удаленному доступу, ограничивая сеансы RDP на уровне приложений. Zecurion PAM использует учетные записи Active Directory для авторизации привилегированных пользователей. Он включен в реестр российского программного обеспечения, не содержит иностранного кода и может использоваться госкомпаниями в рамках программы импортозамещения.

На основании описании аналогов, сделаем их сравнение, где опишем преимущества и недостатки каждой из перечисленных программ (Таблица 1).

Таблица 1 – Сравнение аналогов

	Преимущества	Недостатки
Indeed PAM	Экспертное руководство, индивидуальные решения, проактивная поддержка, экономия времени.	Стоимость, ограниченный контроль, зависимость от третьих лиц, возможность недопонимания.
СКДПУ	Повышение самодостаточности, расширение прав и возможностей, устойчивое развитие.	Ограниченные ресурсы, зависимость от государственной поддержки, культурная нечувствительность
Zecurion PAM	Улучшенная безопасность, сниженный риск внутренних угроз, повышение соответствия, оптимизированное управление.	Сложное развертывание, высокая стоимость, требуется обучение, ограниченная поддержка сторонних систем.

Таким образом, после проведения сравнительного анализа аналогов, видно, что каждая программа в разных областях уступает другим двум программа, поэтому было принято решение делать свой метод для контроля удаленного доступа. Который мог бы конкурировать и даже превзойти описанные выше аналоги.

Выводы по главе

В начале первой главы выпускной квалификационной работы описали задачи, которые нужно реализовать для выполнения цели.

Далее был рассмотрен удаленный доступ, а так же подробно описан каждый протокол: SSH, RDP, VPN.

После описания каждого протокола был произведен сравнительный анализ аналогов, а именно: Indeed PAM, СКДПУ, Zecurion PAM. После проведения сравнительного анализа, было принято решение, что каждое из этих приложений не идеально и не превосходит другие приложения. Поэтому было принято решение создать свой метод, который мог бы конкурировать и даже превзойти описанные выше.

2. Проектирование удаленного доступа

2.1 Моделирование архитектуры системы

Чтобы спроектировать архитектуру системы для управления удаленным доступом к соединениям SSH, RDP и VPN, необходимо учитывать следующие компоненты [11], [18]:

- аутентификация и авторизация: это процесс проверки личности пользователя, вошедшего в систему, и определения его уровня доступа. Система должна поддерживать многофакторную аутентификацию, такую как пароли, биометрические данные и смарт-карты, чтобы обеспечить доступ к системе только авторизованным пользователям;
- контроль доступа. Этот компонент отвечает за контроль доступа к системе на основе ролей и разрешений пользователей. Он включает в себя настройку политик для тех, кто может входить в систему, разрешенного типа подключения, к каким ресурсам они могут получить доступ и какие действия они могут предпринимать;
- сетевая инфраструктура: сюда входят аппаратные и программные компоненты, которые позволяют системе обмениваться данными и обрабатывать данные. Он должен обеспечивать безопасную передачу данных, предотвращать утечку данных или несанкционированный доступ, а также поддерживать высокоскоростные соединения для минимизации задержки;
- мониторинг и отчетность. Этот компонент отвечает за отслеживание действий пользователей, производительности системы и событий безопасности. Он должен генерировать отчеты, оповещения и уведомления, чтобы предупреждать системных администраторов о любых проблемах или потенциальных угрозах;

– консоль управления: это основной интерфейс, используемый системными администраторами для управления системой, настройки параметров и мониторинга производительности. Он должен быть удобным и интуитивно понятным, позволяя администраторам легко получать доступ к системным журналам, отчетам и оповещениям.

В целом, архитектура должна быть разработана с учетом безопасности, гарантируя, что все соединения зашифрованы, аутентификация надежна, а политики контроля доступа строги. Таким образом, риск несанкционированного доступа или утечки данных может быть сведен к минимуму, а система может работать бесперебойно и эффективно. На рисунке 4 представлена архитектура протоколов SSH, RDP и VPN.

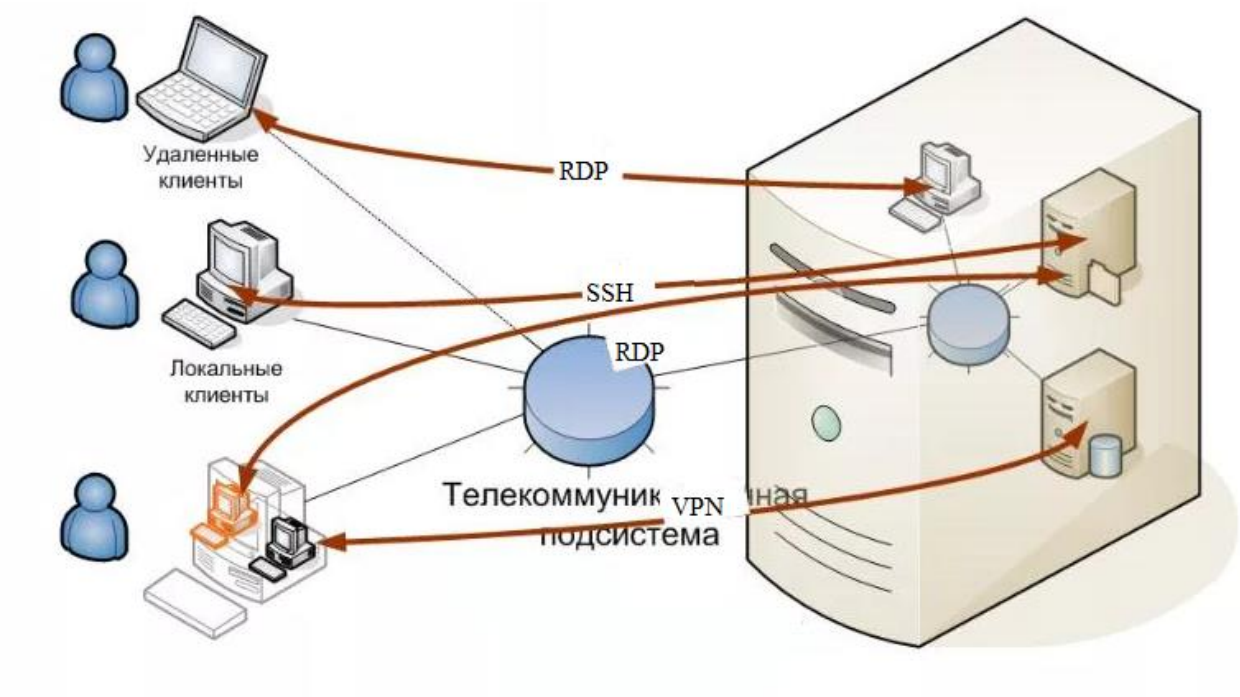

Рисунок 4 – Архитектура протоколов

2.2 Модель данных

Спроектируем логическую модель.

Объекты:

- пользователь;
- сервер удаленного доступа;
- брандмауэр;
- сервер аутентификации;
- политика контроля доступа.

Атрибуты:

- пользователь: имя пользователя, пароль, роль;
- сервер удаленного доступа: IP-адрес, тип (SSH, RDP или VPN);
- брандмауэр: IP-адрес, номер порта, разрешенные протоколы;
- сервер аутентификации: IP-адрес, метод аутентификации (например, LDAP, Active Directory);
- политика контроля доступа: список пользователей, разрешенные серверы удаленного доступа, разрешенные протоколы, временные ограничения.

Отношения:

- пользователь может аутентифицироваться на сервере аутентификации;
- пользователь может запросить доступ к серверу удаленного доступа;
- брандмауэр проверяет, соответствует ли запрос политике контроля доступа;
- если запрос одобрен сетевым экраном, пользователь может установить соединение с сервером удаленного доступа.

Ограничения:

- пользователь должен иметь действительные учетные данные для аутентификации на сервере аутентификации;

– пользователь должен иметь соответствующую роль для запроса доступа к серверу удаленного доступа;
– политика контроля доступа должна быть определена и регулярно обновляться;
– брандмауэр должен быть правильно настроен для обеспечения соблюдения политики контроля доступа;
– серверы удаленного доступа должны быть надлежащим образом защищены и обновлены для предотвращения несанкционированного доступа или уязвимостей.

Спроектированная логическая модель показана на рисунке 5.

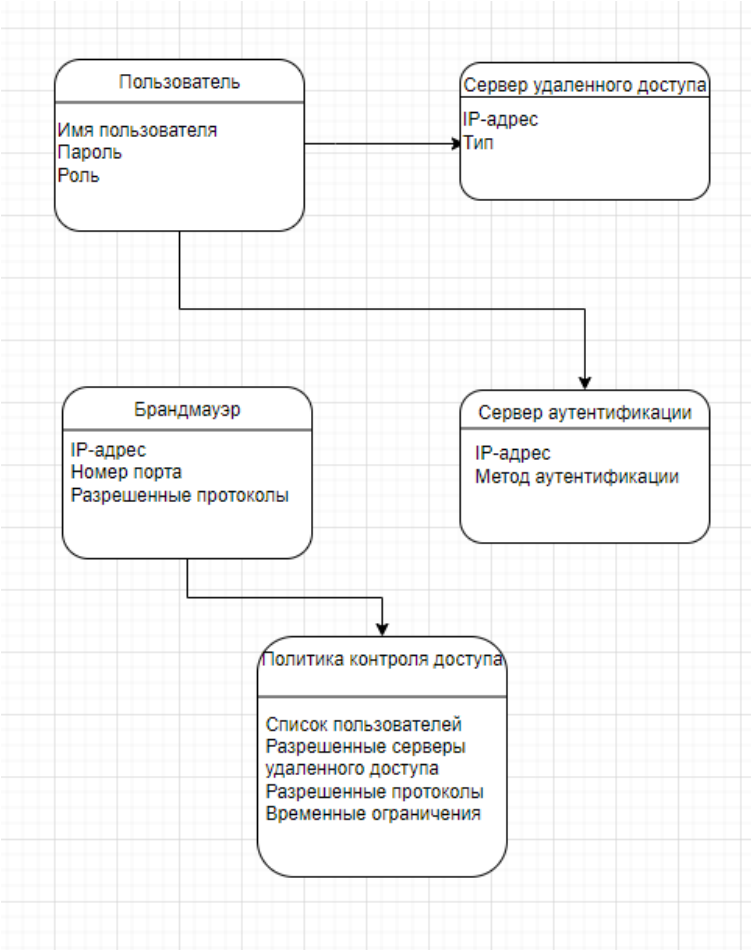

Рисунок 5 – Логическая модель данных

Физическая модель управления удаленным доступом для соединений SSH, RDP и VPN может быть устройство сетевой безопасности. Это устройство может быть выделенным аппаратным устройством или виртуальной машиной, работающей на сервере. Устройство будет действовать как шлюз между внутренней сетью и внешними пользователями или устройствами, пытающимися получить доступ к сети через протоколы SSH, RDP или VPN [20], [21].

Устройство будет включать в себя различные функции безопасности, такие как брандмауэры, системы обнаружения/предотвращения вторжений и сканеры вредоносных программ, для защиты сети от киберугроз. Он также будет включать функции аутентификации и контроля доступа, такие как многофакторная аутентификация, управление доступом на основе ролей и мониторинг активности пользователей.

Физическая модель также может включать дополнительные аппаратные компоненты, такие как сетевые коммутаторы и маршрутизаторы, для обеспечения связи между устройством, внутренней сетью и внешними устройствами. Модель также может включать в себя пользовательский интерфейс для администраторов, позволяющий управлять устройством и настраивать его, а также отслеживать сетевую активность.

2.3 Диаграмма компонентов

Схема, на которой показаны системные компоненты для управления удаленным доступом для соединений SSH, RDP и VPN (рисунок 6).

На этой схеме сервер удаленного доступа отвечает за управление удаленным доступом к сети. Этот сервер поддерживает соединения SSH, RDP и VPN.

Сервер аутентификации используется для проверки личности удаленных пользователей, пытающихся получить доступ к сети. Этот сервер

связывается с базой данных пользователей для проверки информации об имени пользователя и пароле.

Наконец, брандмауэр/маршрутизатор отвечает за контроль доступа к сети. Этот компонент блокирует попытки несанкционированного доступа, позволяя пользователям, прошедшим проверку подлинности, подключаться к серверу удаленного доступа.

Рисунок 6 – Диаграмма компонентов

2.4 Контроль удаленного доступа

В нашей стране существует два основных направления контроля удаленного подключения пользователей. Первый предполагает

использование IPsec VPN, для которого требуется предварительно установленный VPN-клиент и дополнительные меры безопасности, такие как полное шифрование диска, антивирусное программное обеспечение и средства аутентификации пользователей. Однако реализация всех этих механизмов в одном программном клиенте может привести к значительной экономии средств. Второй тренд – использование технологии SSL VPN, которой отдают предпочтение, когда нет возможности контролировать каждое удаленное рабочее место [12], [13]. Важно тщательно выбирать поставщика решения, поскольку в качестве рабочего места можно использовать любой компьютер или смартфон. Эффективным решением является возможность создания безопасной рабочей области при подключении к шлюзу SSL VPN на клиентской машине, которая гарантированно не содержит вредоносного программного обеспечения. Это избавляет от необходимости устанавливать антивирусное программное обеспечение, но производители таких решений используют метод «песочницы», чтобы предотвратить непосредственное взаимодействие прикладного программного обеспечения с ядром операционной системы.

Выводы по главе

Вторая глава ВКР посвящена описанию архитектуры и моделированию контроля удалённого доступа.

Архитектура должна быть разработана с учетом безопасности, гарантируя, что все соединения зашифрованы, аутентификация надежна, а политики контроля доступа строги

Учли компоненты чтобы спроектировать архитектуру системы для управления удаленным доступом к соединениям SSH, RDP и VPN,

Также были описаны физическая и логическая модель. И была создана схема, на которой показаны системные компоненты для управления удаленным доступом для соединений SSH, RDP и VPN.

3. Реализация удаленного доступа

Для реализации необходимо сначала установить PuTTY, для генерации ключа, как это показано на рисунке 7.

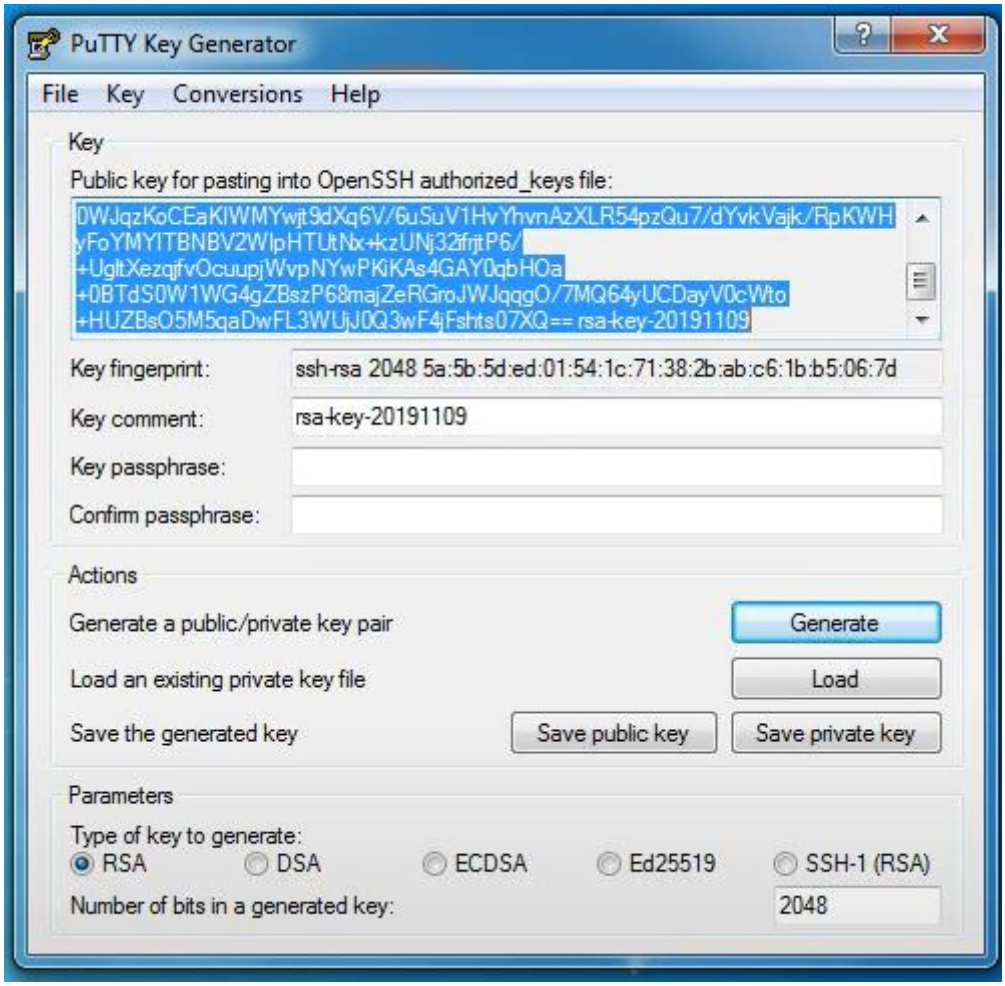

Рисунок 7 – Генерация ключа

После генерации ключа, нужно создать и сохранить приватный ключ пользователя, где нужно ввести и повторить пароль (рисунок 8).

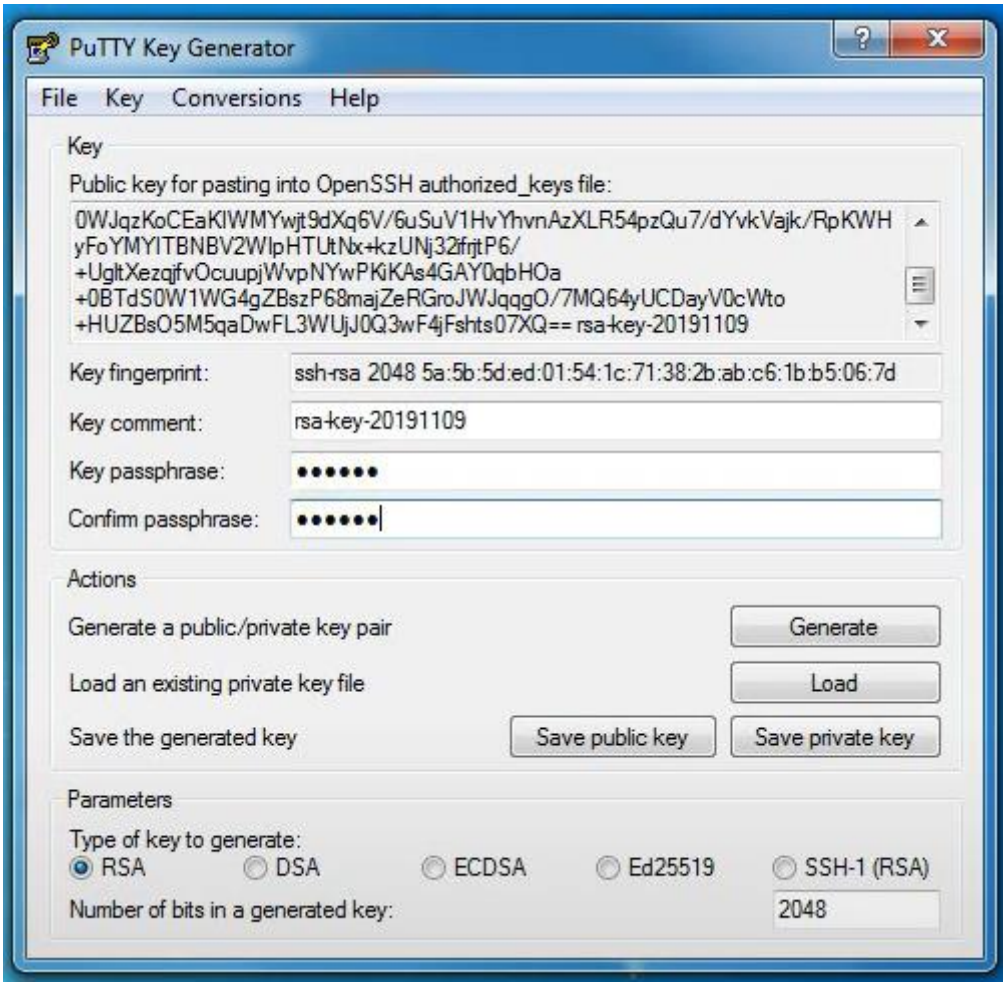

Рисунок 8 – Создание и сохранение приватного ключа пользователя

Переходим на удаленный компьютер с помощью удаленного доступа AnyDesk с использованием freeSSHd, как показано на рисунке 9.

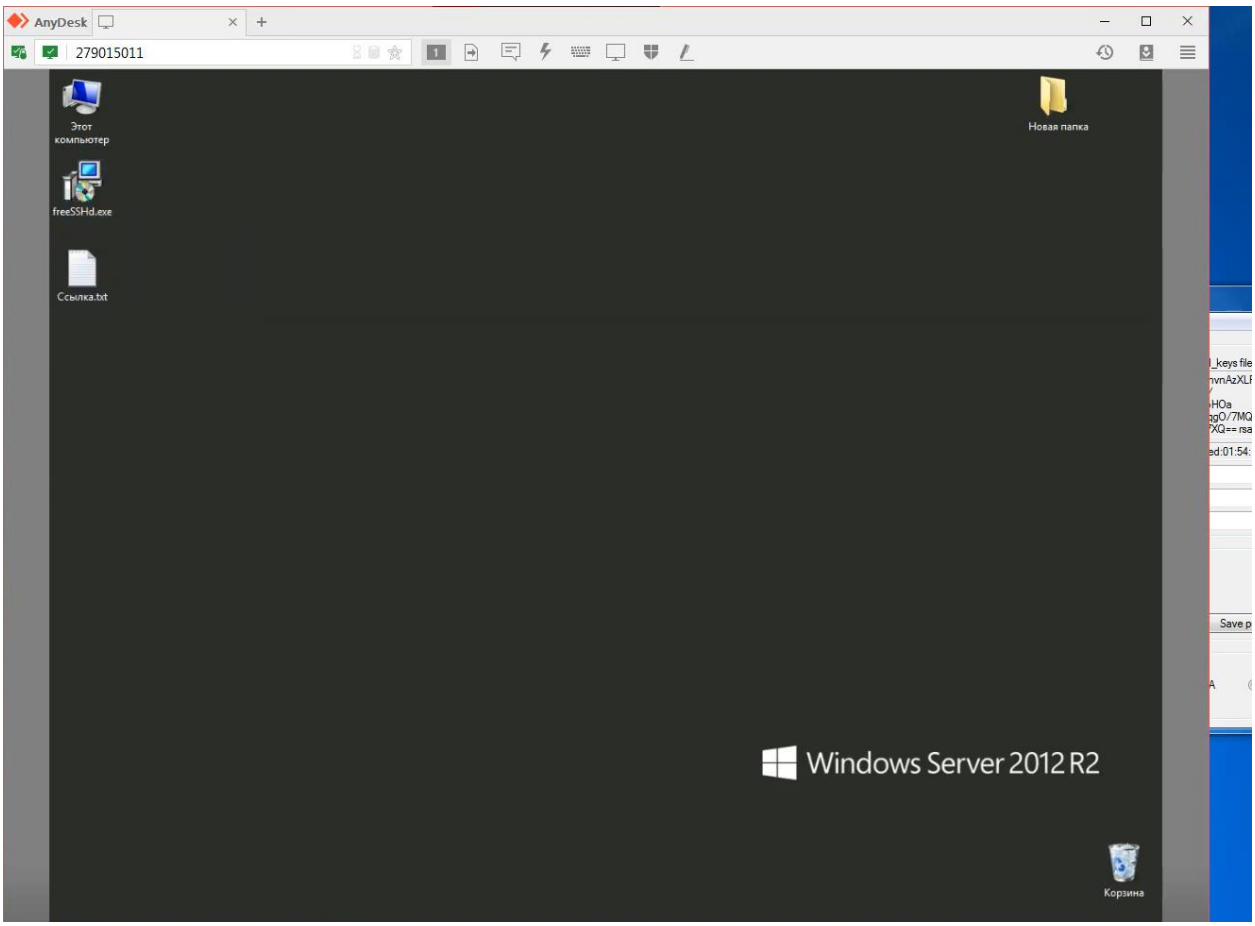

Рисунок 9 – Удаленный доступ AnyDesk с использованием freeSSHd

Запустим установку freeSSHd.exe, где везде выбираем далее, в конце подтверждаем создавание нового ключа сервера. У нас появился значок FreeSSHd, который в дальнейшем необходимо запускать от имени администратора (рисунок 10).

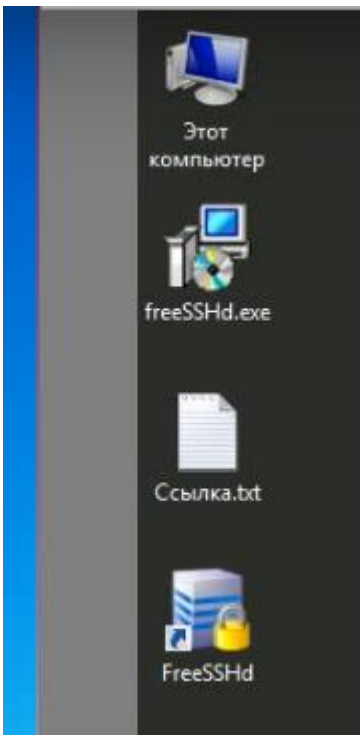

Рисунок 10 – Установленный FreeSSHd

При первом запуске программа приветствует и благодарит за использование программы (рисунок 11).

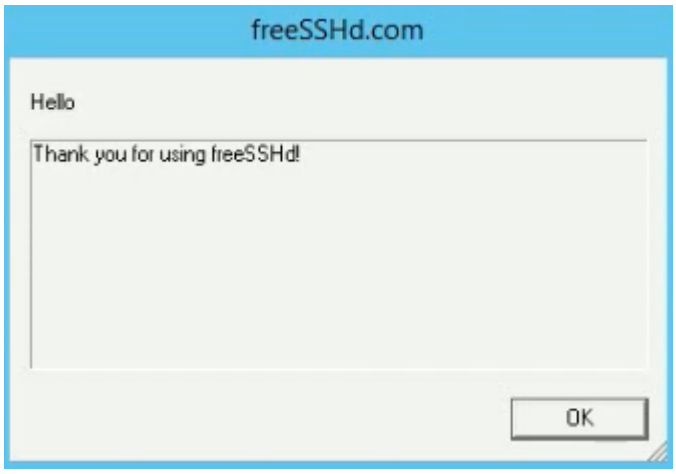

Рисунок 11 – Запуск FreeSSHd от имени администратора

В панели задач находим иконку FreeSSHd и нажимаем на нее. Вводим данные для авторизации, где вводим ключ (рисунок 12).

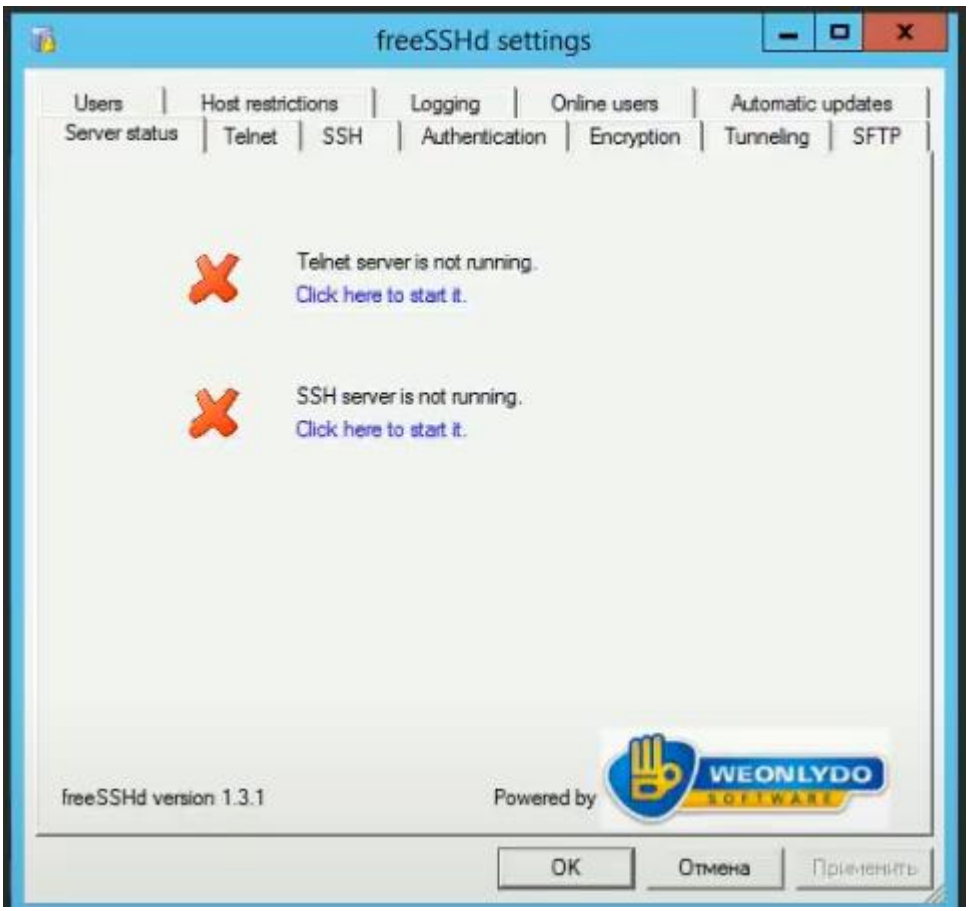

Рисунок 12 – Вход в программу FreeSSHd

Теперь переходим на вкладку SSH, выбираем IP-адерс, оставляем стандартный порт, ниже устанавливаем максимальное количество клиентов, одновременно подключенных к серверу и выбираем время, через которое программа закроет сессию, если она не активна [4]. Ниже можно сгенерировать SSH ключи, но это не обязательно (рисунок 13).

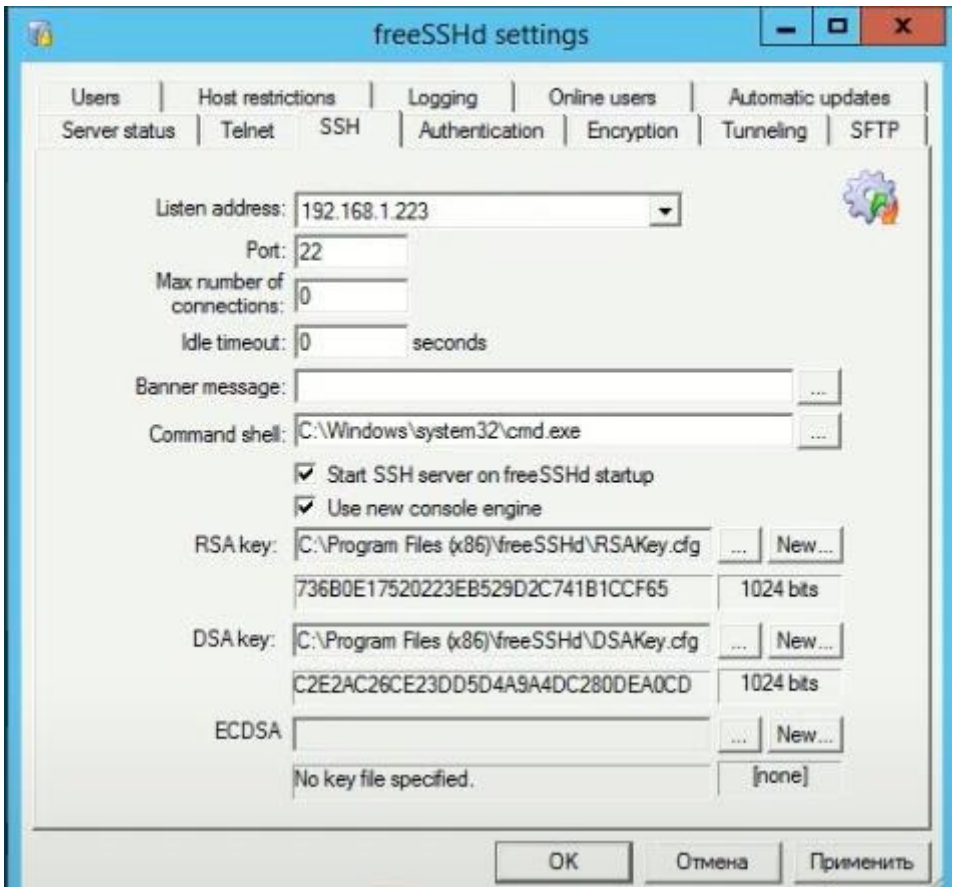

Рисунок 13 – Настройка адреса

Дальше переходим во вкладку аутентификация (рисунок 14), где ставим запрет авторизации по паролю и выбираем авторизацию по публичному ключу с проверкой.

Рисунок 14 – Вкладка аутентификация

Теперь переходим во вкладку автоматического обновления (рисунок 15), где убираем галочку, для дальнейшей корректной работы программы.

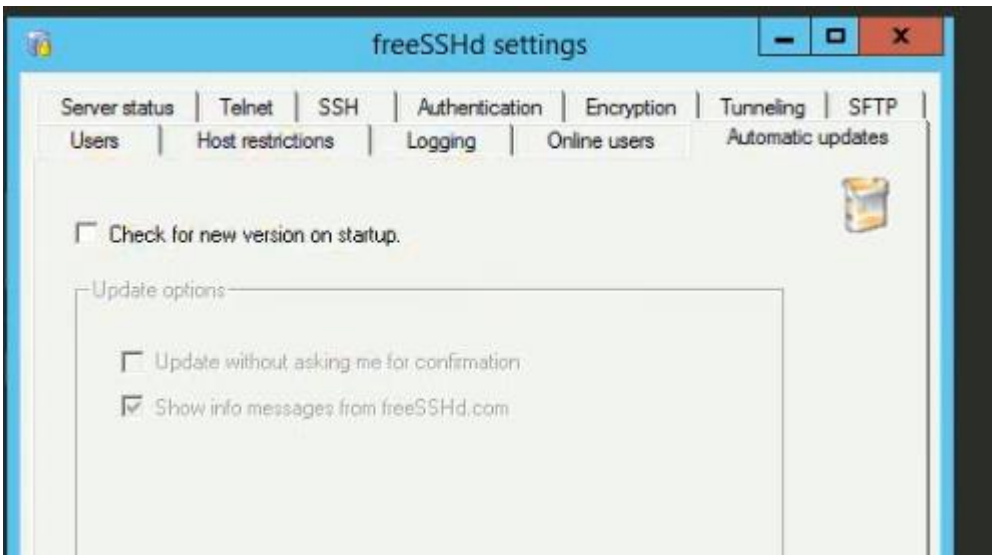

Рисунок 15 – Отключение автоматического обновления

На этом основная настройка сервера закончена.

Теперь нужно зайти в управление компьютером (рисунок 16), службы и перезапустить службы SSHD Service [6]. Сделали мы это для того, чтобы те изменения в настройках, которые мы сделали, они применились.

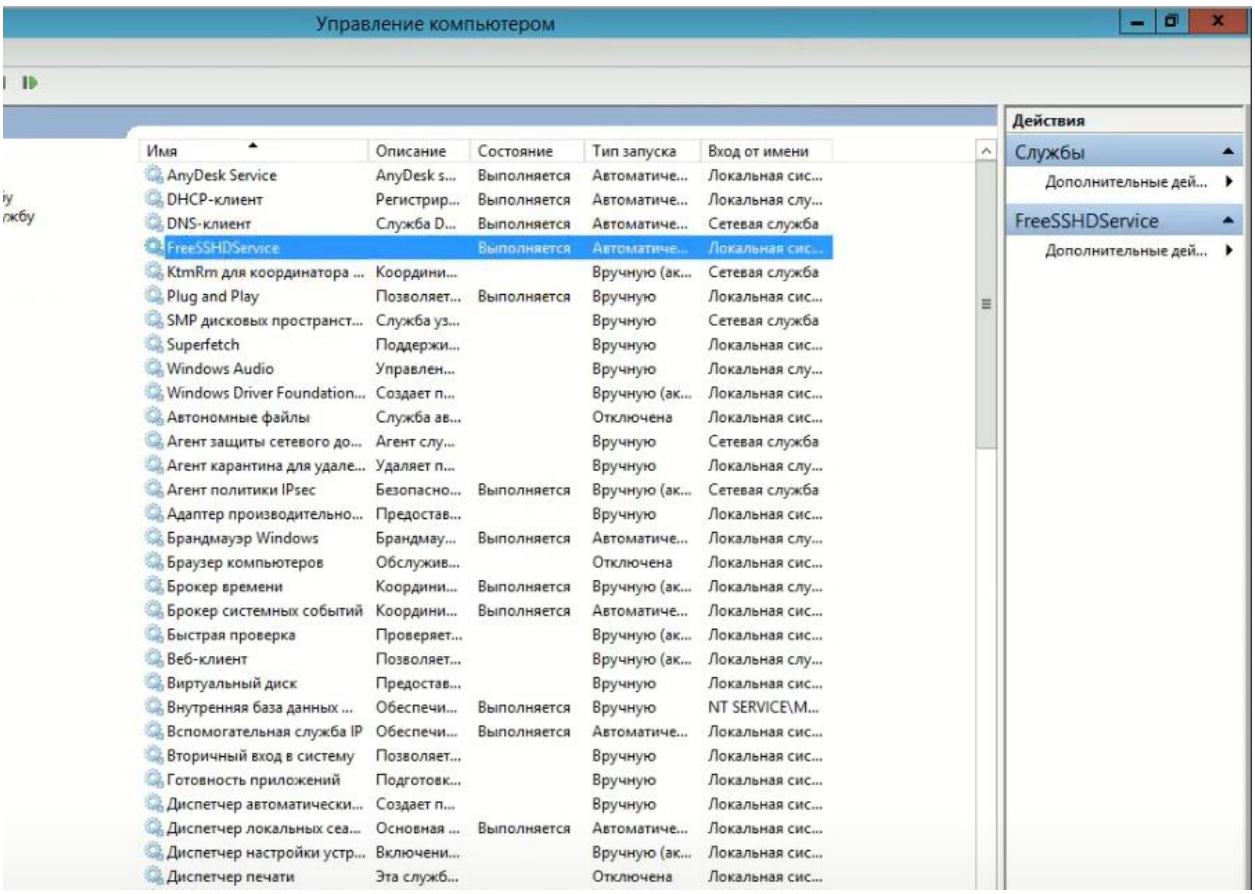

Рисунок 16 – Перезапуск службы FreeSSHD Service

Дальше нужно зайти в брандмауэр Windows (рисунок 17), где во вкладке правила для входящих подключений, нажимаем создать правило (рисунок 19). Правила, мы будем создавать для входящих подключений(рисунок 20), для порта (рисунок 18).

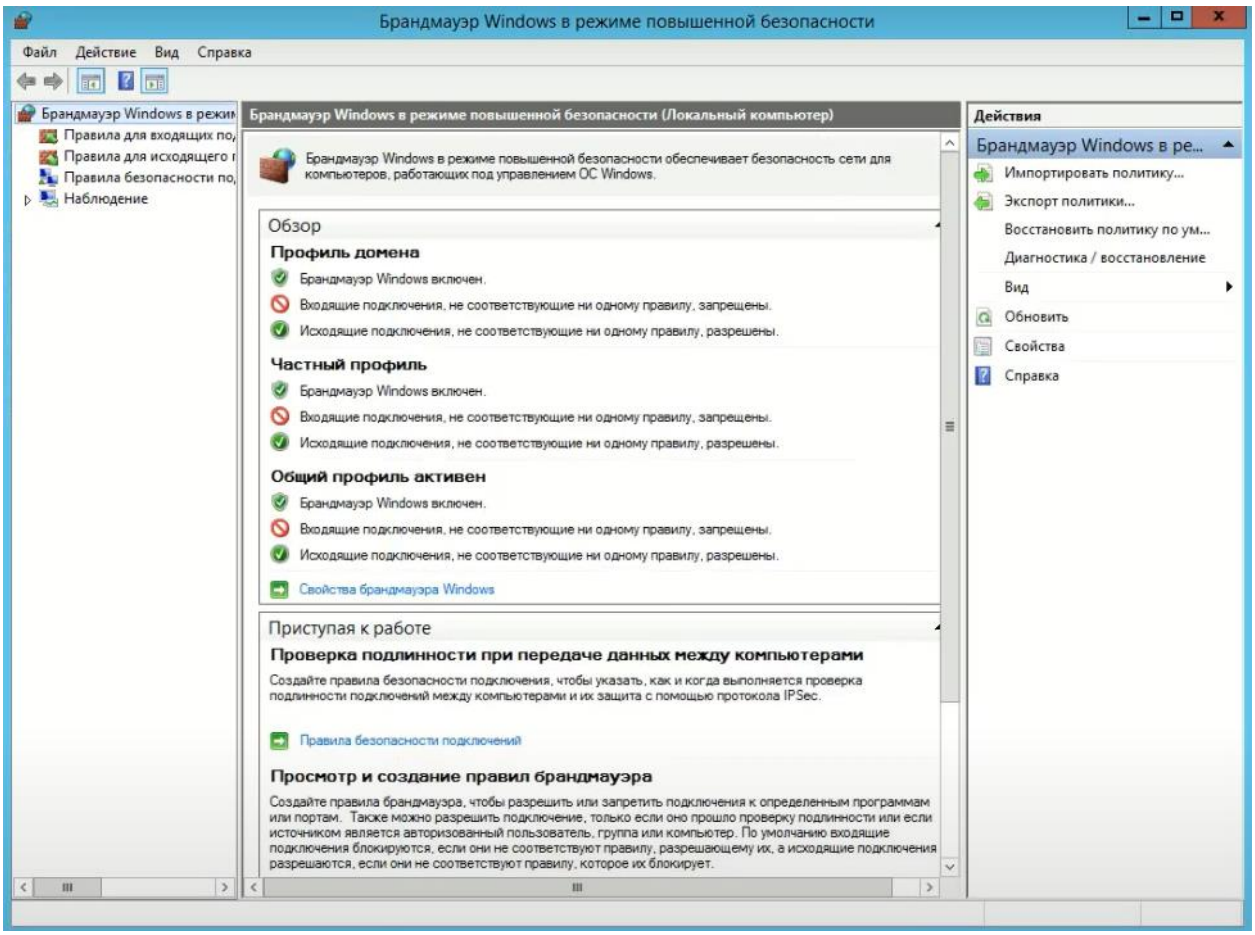

Рисунок 17 – Окно брандмауэр Windows

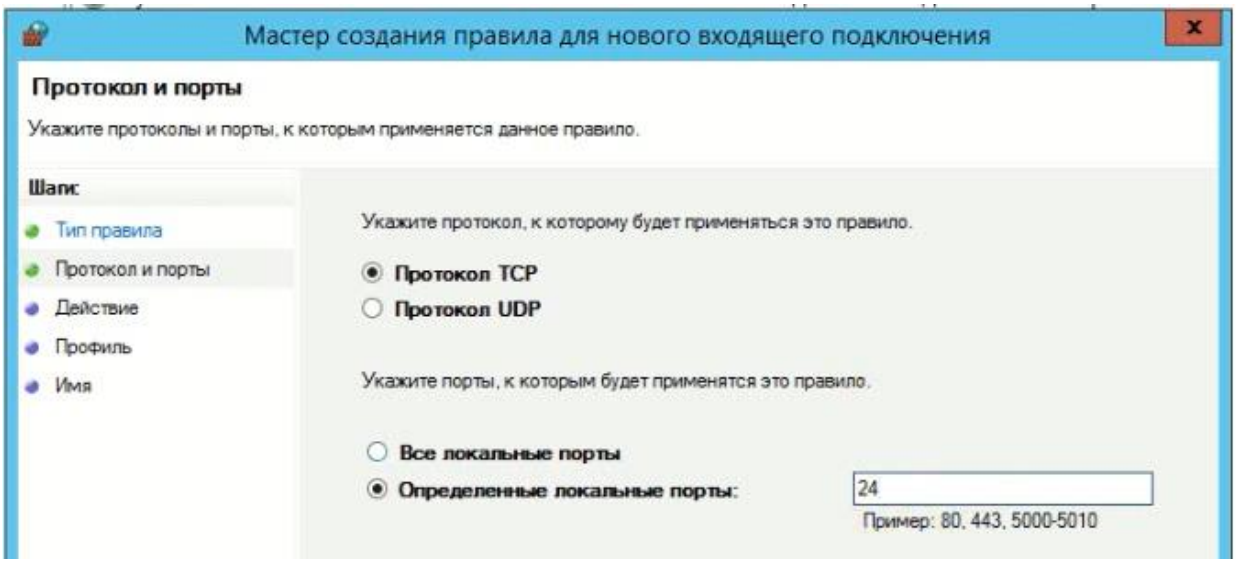

Рисунок 18 – Настройка новых подключений

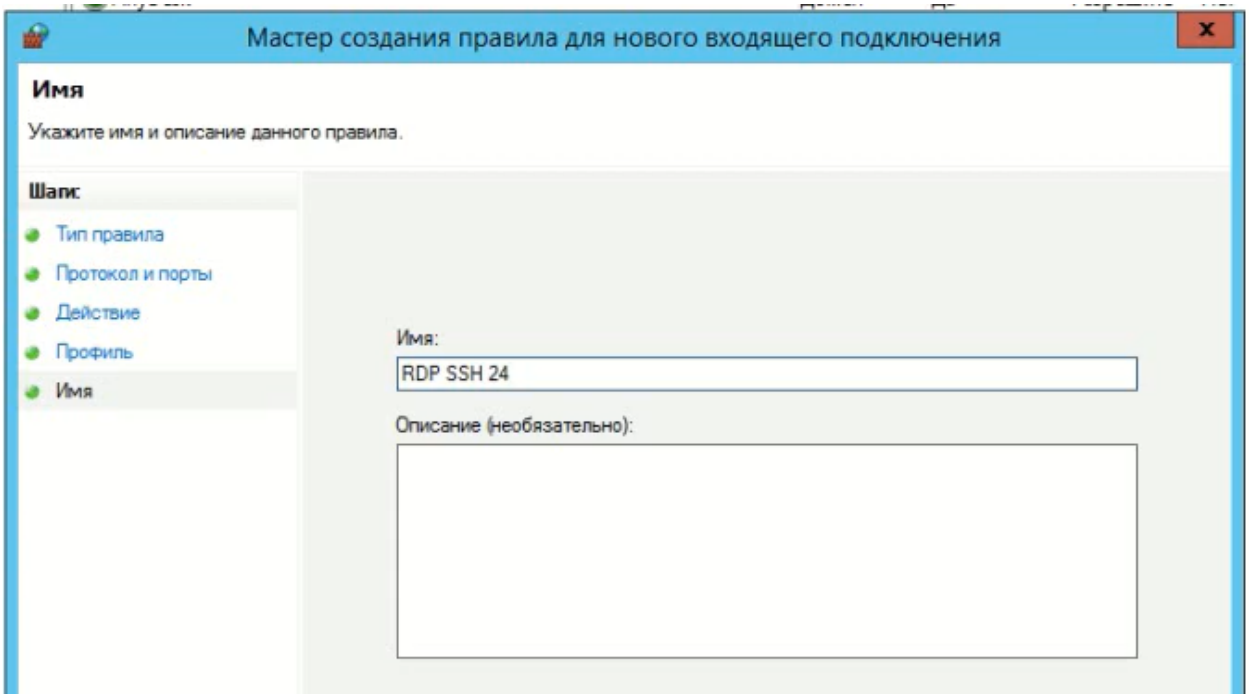

Рисунок 19 – Создание правила

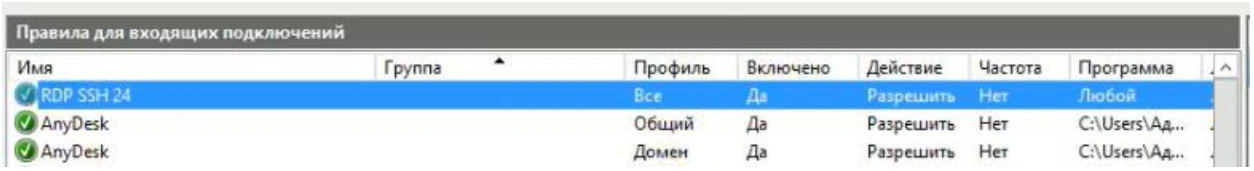

Рисунок 20 – Разрешающее правило

Теперь необходимо запретить стандартный порт RDP, по протоколам TCP и UDP, как это показано на рисунке 21.

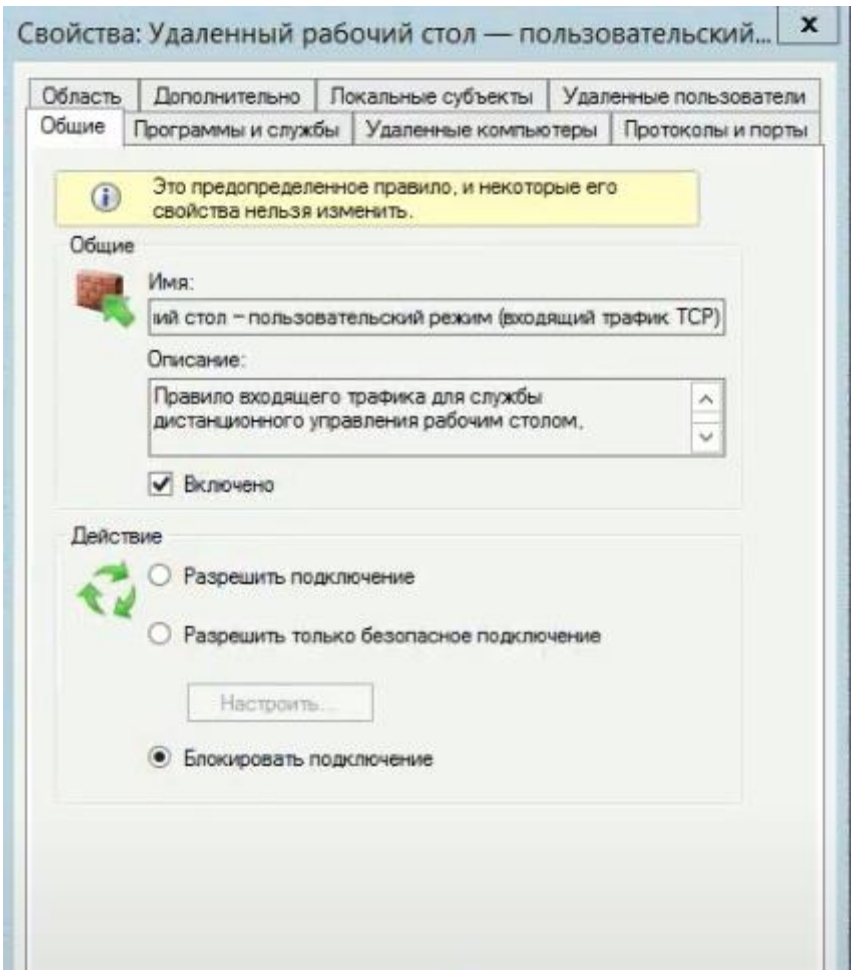

Рисунок 21 – Блокировка подключения

Теперь на рабочем компьютере запускаем программу PuTTY (рисунок 22). Где вводим IP-адрес и порт [23]. Далее вводим название подключения и сохраняем.

Рисунок 22 – Настройка программы PuTTY

В появившимся окне вводим логин и пароль от приватного ключа пользователя. Если нижняя строчка появилась «This service is prohibited», значит пользователь успешно авторизовался, рисунок 23.

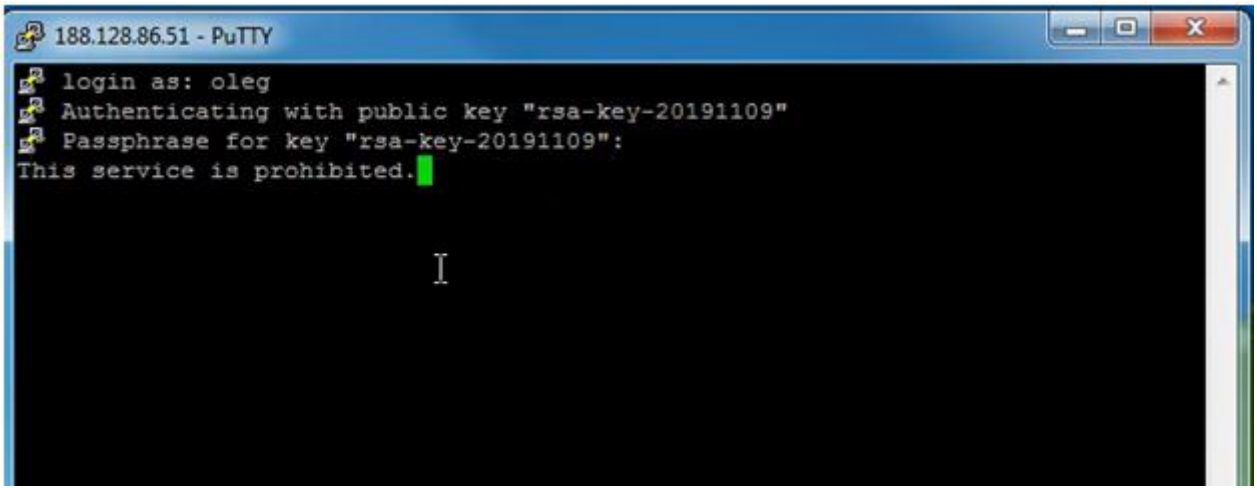

Рисунок 23 – Авторизация пользователя

Запускаем удаленный рабочий стол, как это показано на рисунке 24, вводим localhost: 3391, это порт, который мы выбрали в настройках PuTTY.

Дальше вводим логин и пароль учетной записи Windows удаленного компьютера [16].

Мы подключились к удаленному компьютеру по протоколу RDP, а внутри тоннель SSH с помощью ключей (рисунок 25).

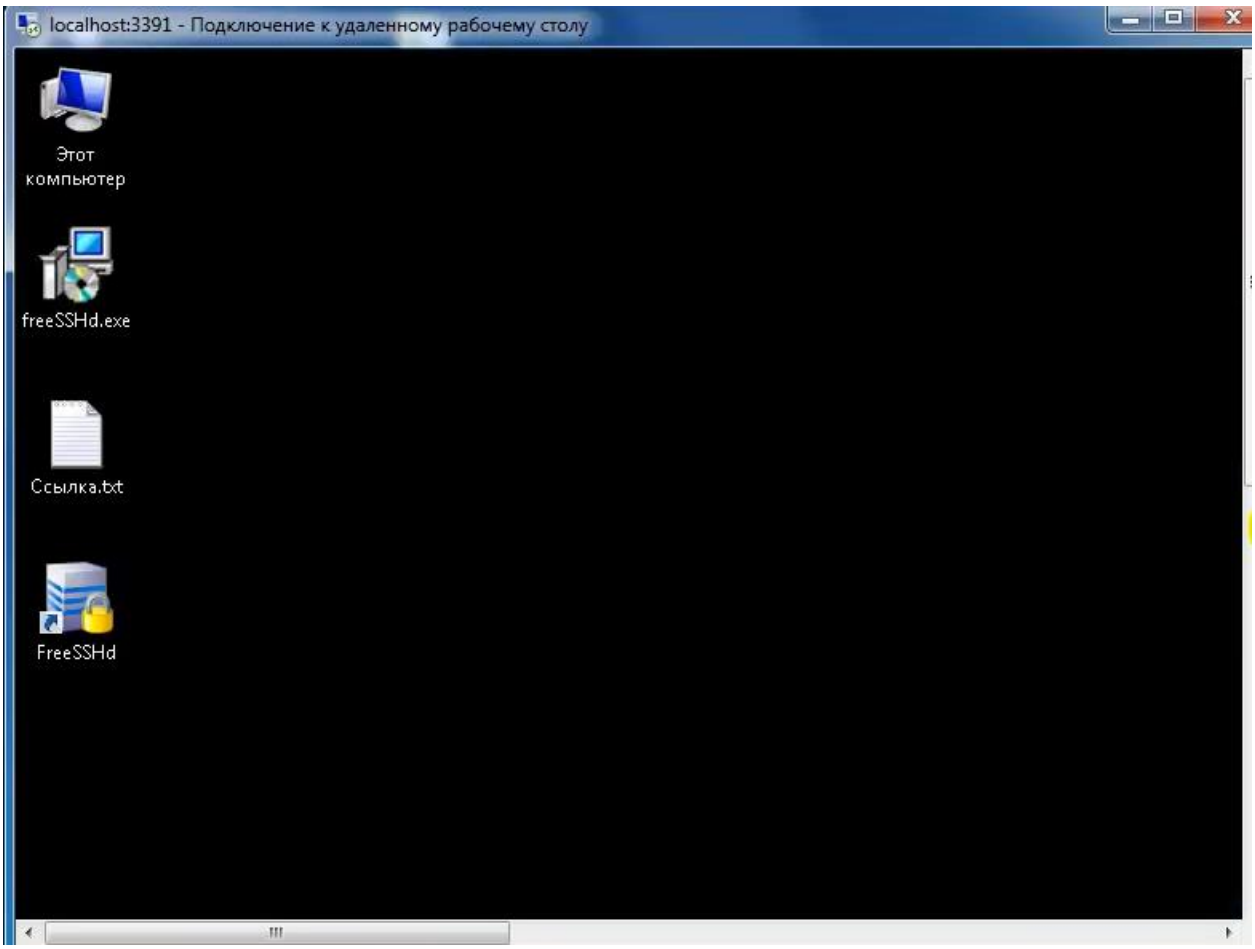

Рисунок 24 – Удаленный компьютер по протоколу RDP

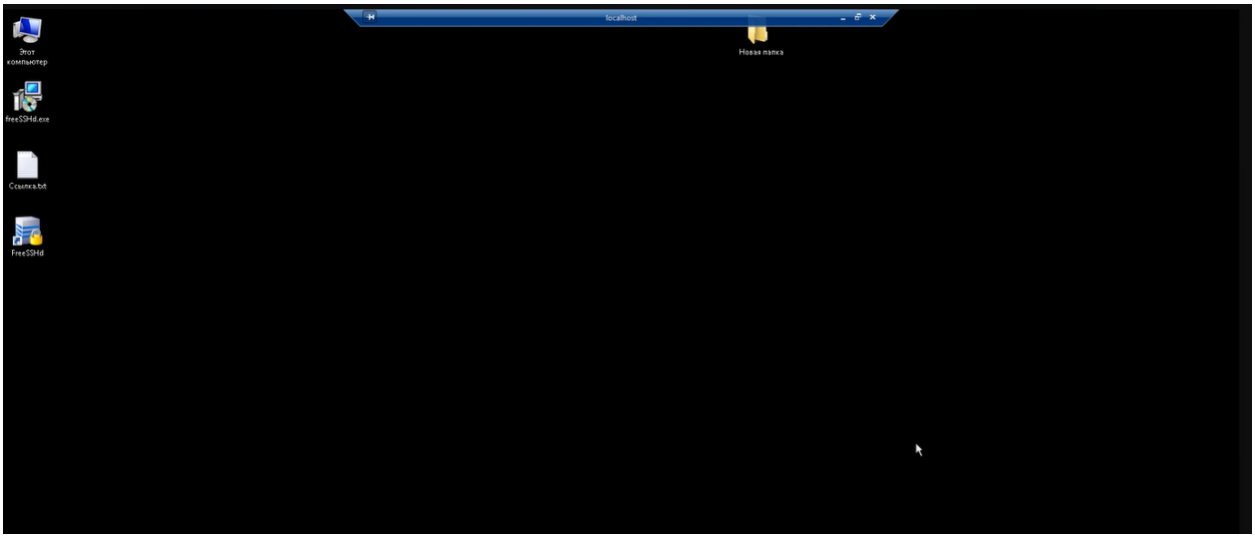

Рисунок 25 – Удаленный компьютер с помощью тоннеля SSH

Чтобы начать настройку SSL VPN Plus, перейдите на вкладку “Authentication” для включения и настройки сервера аутентификации (рисунок 26).

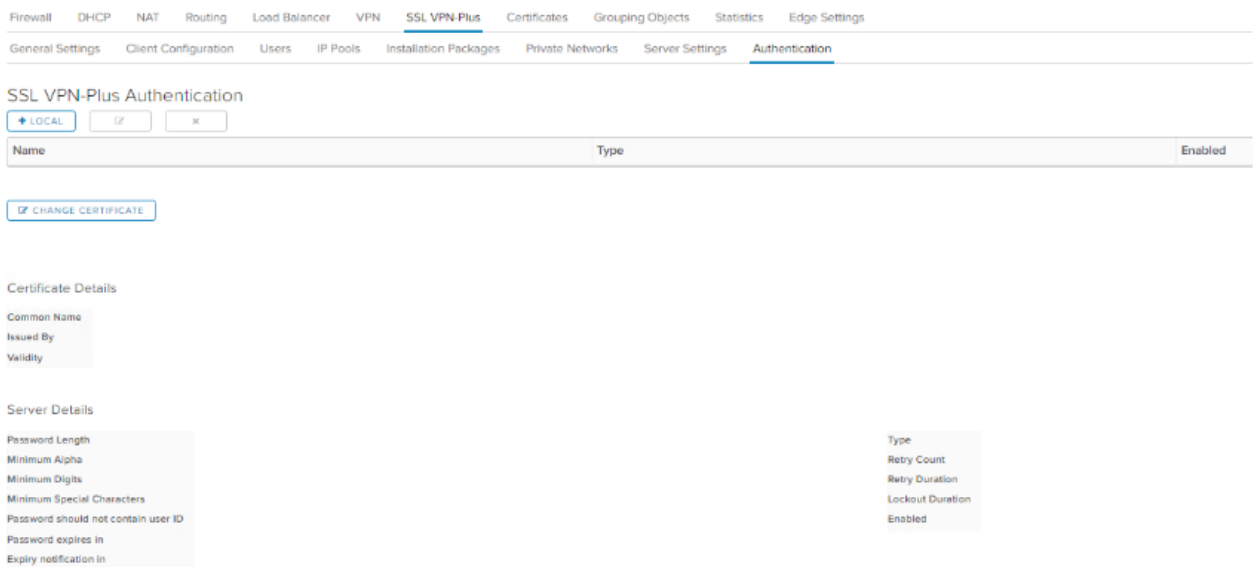

Рисунок 26 – Настройка SSL VPN Plus

На вкладке IP Pools мы задаем адреса выдаваемые подключаемым клиентам, как это показано на рисунке 27, эти IP-адреса должны находится в подсети, имеющей доступ к существующей среде. Эта подсеть пула не должна соответствовать сети vDC.

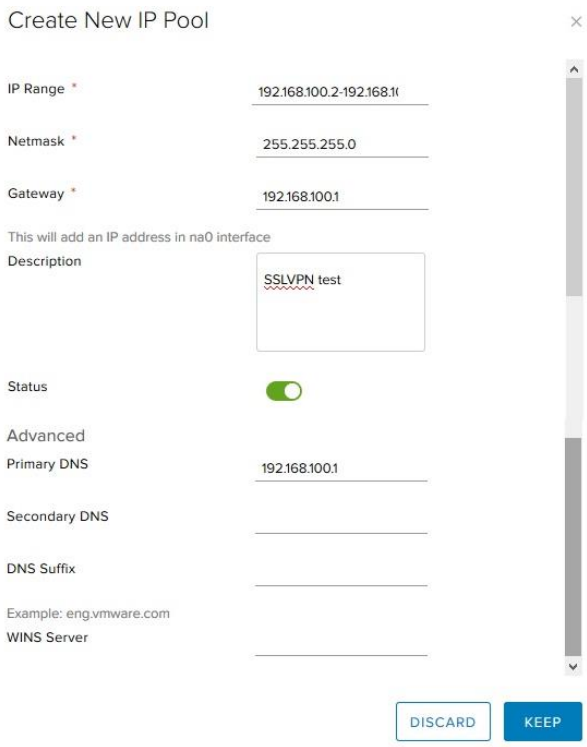

Рисунок 27 – Настройка IP Pools

Добавляем пользователя в ручную (рисунок 28).

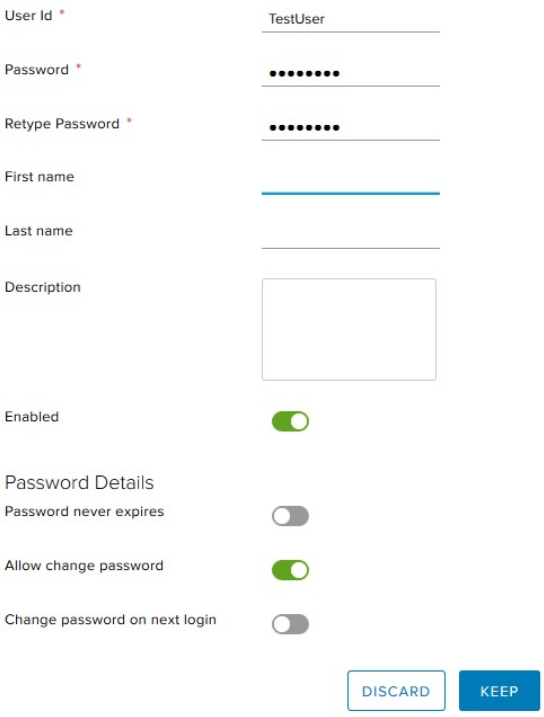

Рисунок 28 – Регистрация пользователя в системе

Установим пользователя SSL VPN под Windows (рисунок 29).

Рисунок 29 – Установка пользователя SSL VPN под Windows

Запустим установленный клиент, нажмем Login, и введем учетные данные пользователя (рисунок 30).

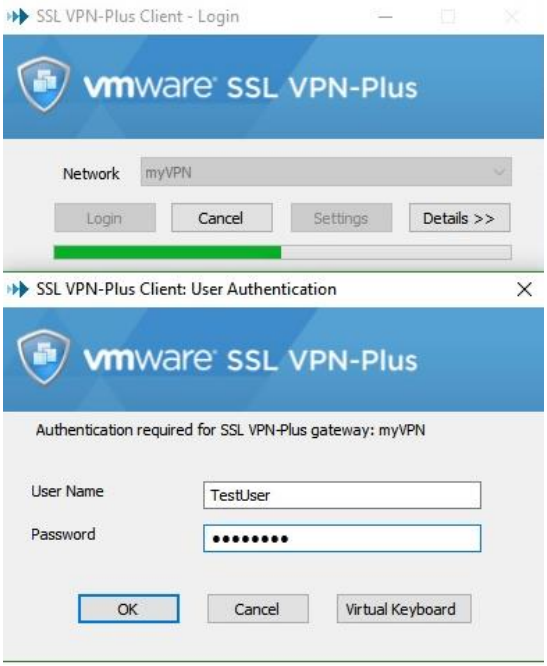

Рисунок 30 – Запуск клиента в систему

Выводы по главе

Третья глава ВКР была посвящена реализации удаленного доступа.

Для реализации сначала установили PuTTY, для генерации ключа.

Запустили установку freeSSHd.exe, где в конце подтверждаем создание нового ключа сервера. У нас появился значок FreeSSHd, который в дальнейшем необходимо запускать от имени администратора.

Дальше нужно было зайти в брандмауэр Windows, где во вкладке правила для входящих подключений, нажали создать правило. Правила, мы создали для входящих подключений, для порта.

Мы подключились к удаленному компьютеру по протоколу RDP, а внутри тоннель SSH с помощью ключей, а также контролировать мы сможем благодаря установленному и настроенному SSL VPN Plus.

Заключение

Бакалаврская работа посвящена контролю удалённого доступа при подключениях SSH, RDP и VPN.

В ходе выполнения ВКР был проведён анализ предметной области, выявлены проблемы, присущие исследуемой области.

В начале первой главы выпускной квалификационной работы были описаны задачи, которые нужно реализовать для выполнения цели.

Далее был рассмотрен удаленный доступ, а так же подробно описан каждый протокол: SSH, RDP, VPN.

После описания каждого протокола был произведен сравнительный анализ аналогов, а именно: Indeed PAM, СКДПУ, Zecurion PAM. После проведения сравнительного анализа, было принято решение, что каждое из этих приложений не идеально и не превосходит другие приложения. Поэтому было принято решение создать свой метод, который мог бы конкурировать и даже превзойти описанные выше.

Архитектура была разработана с учетом безопасности, гарантируя, что все соединения зашифрованы, аутентификация надежна, а политики контроля доступа строги.

Также были описаны физическая и логическая модели. И была создана схема, на которой показаны системные компоненты для управления удаленным доступом для соединений SSH, RDP и VPN.

Было подключение к удаленному компьютеру по протоколу RDP, а внутри тоннель SSH с помощью ключей, а также контроль с помощью установленного и настроенного SSL VPN Plus.

Задачи, определённые для достижения цели работы, были выполнены в полном объёме.

Цель бакалаврской работы была достигнута – создан контроль удалённого доступа при подключениях SSH, RDP и VPN.

Список используемой литературы

1. Алиев Т.И. Компьютерные сети и телекоммуникации: задания и тесты: Учебно-методическое пособие. / Алиев Т.И., Соснин В.В., Шинкарук Д.Н. – СПб.: ИТМО, 2018. – 112 с.
2. Бауткин М.С. Организация удаленного доступа на базе технологии VPN // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. / Бауткин М.С. – 2018. – № 3.– С.155–157.
3. Бондаренко Н.А. О корпоративной политике информационной безопасности предприятия // Актуальные вопросы обеспечения информационной безопасности. / Бондаренко Н.А., Буханцов А.Д., Лихолоб П.Г. – 2015. – № 3.– С.82–92.
4. Калистратов А.П. Анализ протоколов, используемых при организации удаленного доступа. // Молодежный научно-технический вестник. / Калистратов А.П. – 2016. – № 9.– С.42.
5. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний: утв. приказом от 17 декабря 2008 г. N 430-ст. URL: http://docs.cntd.ru/document/1200071688
6. Избачков Ю.С. Информационные системы 2-е издание. / Избачков Ю.С., Петров В.А. – Питер 2009.
7. Ишмухаметов Ш.Т., Математические основы защиты информации: учебное пособие / Ишмухаметов Ш.Т., Рубцов Р.Г. – Казань: Казанский федер. Ун-т, 2012. – 138 с.
8. Минаев В.А. Моделирование системы защиты информационно–телекоммуникационных объектов от угроз непосредственного и удаленного доступа. // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. / Минаев В.А., Журавлев В.С. 2013. № 4. С. 113-115. – 2013. – № 4.– С.113–115.

9. Новиков Ю.В. Основы локальных сетей. / Новиков Ю.В., Кондратенко С.В. Учебное пособие – М.: Интуит, 2014.– 360 с.

10. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / Олифер В.Г., Олифер Н.А. Учебник – СПб.: Питер, 2016.– 992 с.

11. Производитель RFID-меток и RFID-оборудования компания РСТИнвент [Электронный ресурс]: сайт компании. URL: http://www.rstinvent.ru/faq/

12. Савельева Т.С. Решения по обеспечению информационной безопасности при использовании удаленного доступа. // Инновационное развитие. / Савельева Т.С., Байрушин Ф.Т. – 2017. – № 4.– С.34–36.

13. Семененко В.А. Информатика и вычислительная техника / Семененко В.А., Скуратович Э.К. МГИУ, 2010.

14. СКУД компании BOLID [Электронный ресурс]: сайт компании. URL: https://bolid.ru/projects/iso-orion/access-control/

15. СКУД компании PERCo [Электронный ресурс]: сайт компании. URL:https://www.perco.ru/products/sistema-kontrolya-dostupa-perco-web/

16. Система безопасности для образовательных учреждении PERCO [Электронный ресурс]: сайт компании. URL: https://www.perco.ru/ products/sistema-bezopasnosti-perco-s-20-shkola/

17. Столингс В.Д. Компьютерные сети, протоколы и технологии Интернета. С.-Пб. БХВ, Петербург, 2005.

18. Таненбаум Э. Компьютерные сети. 5–е изд. / Таненбаум Э. , Уэзеролл Д. – СПб.: Питер, 2017.– 960 с.

19. Хабрейкен Д.М. Сетевые технологии за 24 часа. 3-е издание / Хабрейкен Д.М., Хайден М.К. Издательский дом Вильямс. Питер, 2008.

20. Ярмак Д.А. Удаленный доступ к корпоративной сети с помощью VPN. // Наука, техника и образование. / Ярмак Д.А. – 2017. – № 4.– С.69–72.

21. Adrian D.A. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. 2014. [Электронный ресурс]. Режим доступа: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

22. Paul J. Jackson, Jos M. van der Wielen Teleworking: International Perspectives. – New York: Routledge, 2012. – 369 c.

23. Pinsonneault A. The Impacts of Telecommuting on Organizations and Individuals: A Reviewof the Literature. – Montreal: University McGill, 2009. – 27 c.

24. Qingcang, Y. Web based control system design and analysis [Text] / Yu Qingcang, Chen Bo, H. H. Cheng // IEEE Control Systems Magazine. – 2014. – Vol. 24, no. 3. -P. 45-57.

25. Sullivan, D. Proven Portals: Best Practices for Planning, Designing, and Developing Enterprise Portals [Text] / Dan Sullivan. – [S. 1.] : Addison Wesley Professional, 2013. – 224 p.-ISBN: 0321125207