Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Система віддаленого адміністрування комп'ютеризованого робочого місця з захищеним доступом на основі з'єднань SSH, RDP та VPN*

Виконав: студент IV курсу, групи СІ-41
спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

(підпис) Глушко М.В. (прізвище та ініціали)

Керівник (підпис) Баран І.О. (прізвище та ініціали)

Нормоконтроль (підпис) Луцик Н.С.

Завідувач кафедри (підпис) Осухівська Г.М. (прізвище та ініціали)

Рецензент (підпис) Палка О.В. (прізвище та ініціали)

Тернопіль
2026

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«_25_» ____04____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 Комп'ютерна інженерія*
(шифр і назва спеціальності)

Студентці *Глушку Максиму Володимировичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Система віддаленого адміністрування комп'ютеризованого робочого місця з захищеним доступом на основі з'єднань SSH, RDP та VPN*

Керівник роботи *Баран Ігор Олегович., к.т.н., доц.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від *« 24 » 04 2026 року № 4/9-188*

2. Термін подання студентом завершеної роботи *19.06. 2026 р.*

3. Вихідні дані до роботи *Технічне завдання*

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ.
1. Аналіз технічного завдання.
2. Проектна частина.
3. Практична частина.
4. Безпека життєдіяльності, основи охорони праці.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Принцип роботи SSH_RDP_VPN
2. Логічна модель даних системи
3. Скріншоти вікон налаштування сервера
4. Скріншоти вікон реалізація віддаленого доступу до АРМ

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання 25.04.2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Розробка технічного завдання*	*26.01 – 02.02*	*Виконано*
2.	*Підбір джерел про системи віддаленого керування із*		
	захищеним доступом (на основі SSH, RDP та VPN)	*03.02 – 06.04*	*Виконано*
3.	*Опрацювання літературних джерел*	*05.04 – 10.05*	*Виконано*
4.	*Виконання дослідження щодо моделювання системи*		
	віддаленого адміністрування комп'ютеризованого		
	робочого місця з захищеним доступом	*11.05 – 13.05*	*Виконано*
5.	*Втілення практичної складової в частині реалізації*		
	системи	*14.05 – 18.05*	*Виконано*
6.	*Оформлення розділу «Аналіз технічного завдання»*	*19.05 – 22.05*	*Виконано*
7.	*Оформлення розділу «Проектна частина»*	*23.05 – 26.05*	*Виконано*
8.	*Оформлення розділу «Практична частина»*	*27.05 – 28.05*	*Виконано*
9.	*Виконання завдання до підрозділу «Безпека*		
	життєдіяльності, основи охорони праці»	*26.05 – 30.05*	*Виконано*
10.	*Оформлення пояснювальної записки і графічного матеріалу*	*01.06 – 03.06*	*Виконано*
11.	*Перевірка на академічний плагіат, перевірка керівником та консультантами*	*04.06 – 09.06*	*Виконано*
12.	*Попередній захист кваліфікаційної роботи бакалавра*	*11.06 – 17.06*	*Виконано*
13.	*Захист кваліфікаційної роботи*	*26.06*	

Студент _____ *Глушко М.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Баран І.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Глушко М.В. Система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN: робота на здобуття кваліфікаційного ступеня бакалавра: спец. 123 — комп’ютерна інженерія. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2026

Ключові слова: аутентифікація, віддалений доступ, керування доступом, передача даних, RDP, SSH, VPN

У першому розділі кваліфікаційної роботи чітко сформульовані завдачі, котрі необхідно втілити для виконання поставленої мети. Розглянуто поняття віддаленого доступу, детально описані можливості протоколів SSH, RDP та технології VPN.

У другому розділі роботи спроєктована та описана архітектура розроблюваної системи віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом із моделюванням контролю віддаленого доступу. Архітектура спроєктована із урахуванням політик безпеки, забезпечуючи шифрування усіх з'єднань, надійну аутентифікацію, та суворі правила контролю доступу. Враховані усі необхідні компоненти, забезпечення керування віддаленим доступом на основі з'єднань SSH, RDP і VPN. Описані фізична і логічна моделі системи. Побудована схема, на якій відображені системні компоненти для керування віддаленим доступом.

У третьому розділ роботи описано реалізацію віддаленого доступу із використанням програмних продуктів PuTTY, freeSSHd. В результаті покрокового виконання описаних дій вдалося під’єднатися до віддаленого комп'ютера за протоколом RDP, з тунелем SSH, а також контролювати доступ через інстальований та попередньо налагоджений SSL VPN Plus.

ANNOTATION

Hlushko Maksym. Remote Administration System for a Computerized Workplace with Secure Access Based on SSH, RDP, and VPN Connections: Bachelor's Graduation Thesis: speciality 123 — computer engineering. Ternopil: Ternopil Ivan Puluj National Technical University, 2026

Keywords: authentication, remote access, access control, data transfer, RDP, SSH, VPN

The first section of the Thesis clearly formulates the tasks that need to be implemented to achieve the set goal. The concept of remote access is considered, the capabilities of the SSH, RDP and VPN protocols are described in detail.

In the second section, the architecture of the developed remote administration system of a computerized workplace with secure access with remote access control modeling is designed and described. The architecture is designed taking into account security policies, ensuring encryption of all connections, reliable authentication, and strict access control rules. All necessary components are taken into account, ensuring remote access management based on SSH, RDP and VPN connections. The physical and logical models of the system are described. A diagram is built, which displays the system components for remote access management.

In the third section, the implementation of remote access using the PuTTY, freeSSHd software products is described. As a result of the step-by-step execution of the described actions, it was possible to connect to a remote computer via the RDP protocol, with an SSH tunnel, and also control access via the installed and pre-configured SSL VPN Plus.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

RDP (англ. Remote Desktop Protocol – протокол віддаленого робочого столу) – протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на котрому запущений сервіс термінальних з'єднань.

SSH (англ. Secure Shell – безпечна оболонка) – мережевий протокол прикладного рівня, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів).

VPN (англ. Virtual Private Network – віртуальна приватна мережа) – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри.

НСД – несанкціонований доступ.

ПЗ – програмне забезпечення.

ВСТУП

Епоха цифрових технологій вплинула на те, як люди працюють та спілкуються один з одним. Впровадження хмарних обчислень, віддаленого доступу та VPN дозволило підприємствам працювати більш ефективно та безпечніше, ніж будь-коли раніше. Однак з такою підвищеною ефективністю виникає підвищений ризик НСД до конфіденційної інформації та даних. Таким чином, для підприємств важливо впровадити безпечні заходи контролю доступу, щоб гарантувати, що лише авторизованим користувачам дозволено доступ до корпоративних мереж, даних та додатків [1].

Одним з найбільш поширених методів, котрі застосовуються з метою встановлення безпечного керування доступом, є використання протоколів керування віддаленим доступом, таких як з'єднання SSH, RDP та VPN. SSH є мережевим протоколом, котрий дає змогу користувачам безпечно реалізовувати команди та передавати файли із зашифрованого з'єднання. RDP є протоколом віддаленого доступу, який дозволяє користувачеві отримувати доступ до комп'ютера та управляти ним через Internet. Наостанку, VPN - це безпечний тунель, через який дані шифруються та відправляються через Інтернет, що забезпечує додатковий рівень безпеки.

У поєднанні ці протоколи керування доступом забезпечують комплексний підхід до безпечного віддаленого доступу. Протоколи повинні бути правильно налаштовані, щоб забезпечити найвищий рівень безпеки та обмежити доступ лише тим користувачам, яким надано дозвіл. Крім того, необхідно регулярно контролювати протоколи, щоб переконатися, що вони працюють належним чином, і що неавторизовані користувачі не можуть отримати доступ до системи.

Актуальність цієї теми полягає в тому, що при під’єднаннях SSH, RDP та VPN необхідно забезпечити безпеку при передачі даних та доступу до систем. У таких випадках необхідно використовувати різні методи контролю віддаленого доступу, які забезпечать безпеку під час передачі даних та доступу до систем.

Мета роботи - змоделювати систему контролю віддаленого доступу при

під’єднаннях SSH, RDP і VPN.

Завдання, необхідні для досягнення даної мети:

– описати теоретичні засади віддаленого доступу;

– провести порівняльний аналіз протоколів та технологій SSH, RDP та VPN;

– спроектувати систему віддаленого доступу;

– змоделювати її архітектуру;

– побудувати фізичну та логічну моделі віддаленого доступу;

– реалізувати систему віддаленого доступу.

.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Постановка завдання

Для виконання кваліфікаційної роботи необхідно розібратися із тими задачами, котрі потрібно зробити:

– визначити рівень доступу, який хочемо надати віддаленим користувачам. Залежно від вимог безпеки організації, може знадобитися застосування обмеження доступу до певних ресурсів або обмеження кількості користувачів, котрі можуть під’єднюватися віддалено;

– створити політику віддаленого доступу, що визначає права та обов'язки віддалених користувачів. Переконається, що політика відповідає всім нормативним вимогам чи галузевим стандартам;

– налаштувати для застосування політики під час під’єднання віддалених користувачів. Це може містити налаштування фільтрів або списків керування доступом для обмеження або дозволу доступу до певних ресурсів;

– відстежувати активність віддаленого доступу, щоб бачити будь-який НСД або незвичайну активність. Проаналізувати можливість застосування таких засобів, зокрема як системи виявлення вторгнень (IDS) або ПЗ для керування інформацією і безпековими подіями (SIEM), для допомоги у цьому;

– регулярно перевіряти та оновлювати політику та параметри за потреби, щоб переконатися, що вони, як і раніше, ефективні при керуванні віддаленим доступом.

1.2 Віддалений доступ

Віддалений доступ - це можливість доступу до комп'ютера, мережі або

програми з іншого місця за допомогою під’єднання до мережі. Віддалений доступ, зазвичай, використовується в сучасному діловому світі, щоб дозволити співробітникам отримувати віддалений доступ до мережі та застосунків своєї компанії, що дозволяє їм залишатися на зв'язку та продуктивно працювати, навіть якщо вони знаходяться за межами фізичного офісу.

Існує безліч різних методів надання віддаленого доступу, кожен з яких володіє певними перевагами і недоліками. Найбільш розповсюдженими методами віддаленого доступу є VPN, RDP та засоби віддаленого адміністрування.

VPN - це безпечне з'єднання між двома або більше комп'ютерами, що дозволяє користувачам отримувати доступ до приватної мережі ззовні. Вони використовують розширені протоколи безпеки для шифрування даних та забезпечення їхньої безпеки під час передачі. VPN також забезпечують автентифікацію та авторизацію, дозволяючи користувачам отримувати доступ лише до тих ресурсів, на які вони авторизовані. На рис. 1.1 представлено корисні можливості використання VPN.

Рисунок 1.1 – Корисні властивості VPN

RDP - це власний протокол, розроблений Microsoft, який дозволяє користувачам отримувати доступ до віддаленого комп'ютера через мережеве з'єднання. RDP використовує шифрування та автентифікацію для захисту з'єднання та надання доступу до додатків та даних, розміщених на віддаленому комп'ютері. На рис. 1.2 наведена схема роботи RDP.

Рисунок 1.2 – Як працює RDP

Засоби віддаленого адміністрування - це спеціалізовані програми, які використовуються для віддаленого керування та контролю за комп'ютером. Вони дають змогу користувачам одержувати доступ до віддаленого комп'ютера, виконувати команди та керувати такими функціями, як керування файлами, встановлення ПЗ та налаштування системи.

На додачу до згаданих вище методів віддалений доступ також може бути забезпечений через web -застосунки та хмарні обчислення. Web -програми дають змогу юзерам одержувати доступ до програм і використовувати їх через web - браузер. Хмарні обчислення [2] забезпечують віддалений доступ до застосунків та даних без необхідності їхньої локальної установки на комп'ютер користувача.

У будь якому разі, який би метод віддаленого доступу не використовується, найголовніше - забезпечити безпеку під’єднання до віддаленого комп'ютера та правильність автентифікації та авторизації користувача. Компанії також мають забезпечити належні процедури для захисту своїх даних та інформації.

1.3 Протокол SSH

SSH є безпечною альтернативою традиційному протоколу telnet.

Протокол SSH забезпечує безпечний канал зв'язку між двома комп'ютерами за допомогою зашифрованого з'єднання. Він використовується для доступу до віддалених систем, передавання файлів і виконання команд на віддаленій машині [3].

Протокол SSH складається із двох компонентів: клієнта SSH і сервера SSH. Клієнт – це програма, яка ініціює з'єднання, а сервер отримує запит. На рис. 1.3 відображена переадресація портів SSH.

Протокол SSH використовує порт 22 для початкового під’єднання. Після того, як початкове з'єднання встановлено, протокол SSH узгоджує безпечний тунель передачі даних.

SSH підтримує різні методи аутентифікації, такі як аутентифікація з відкритим ключем, аутентифікація паролем і аутентифікація на основі хоста. Протокол SSH також підтримує кілька методів шифрування, включаючи Advanced Encryption Standard (AES) та Triple Data Encryption Standard (3DES).

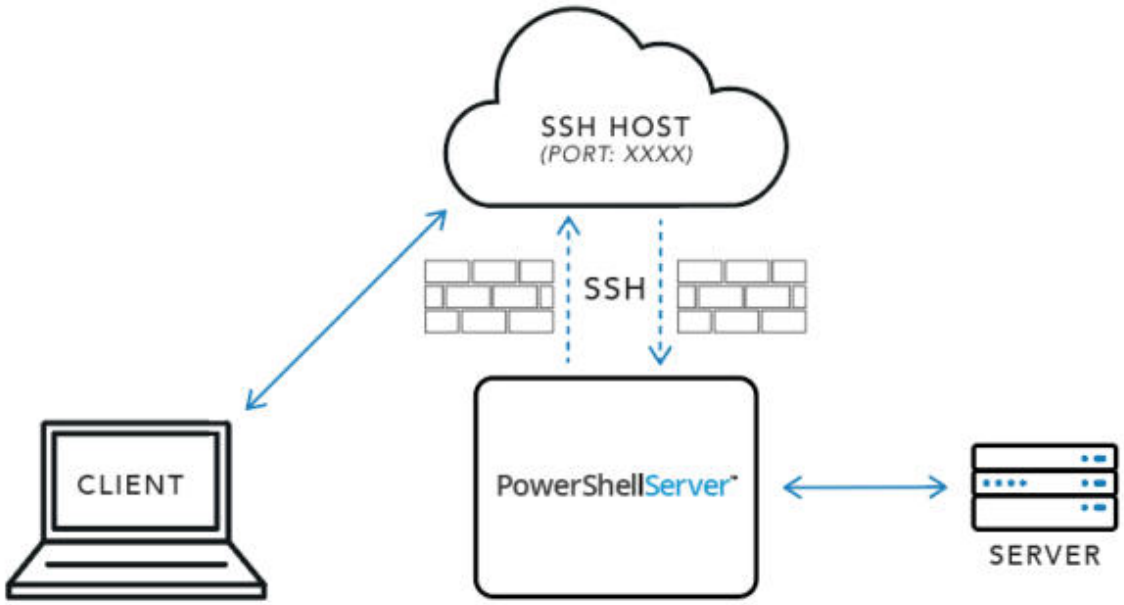

Рисунок 1.3 – Переадресація портів SSH

Протокол підтримує кілька функцій, таких як переадресація портів, переадресація X11 та тунелювання. SSH також підтримує передачу файлів, що дозволяє користувачам безпечно виконувати передавання файлів між двома комп'ютерами [4].

Протокол SSH також підтримує мультиплексування сеансів, дозволяючи встановлювати кілька сеансів через той самий безпечний тунель. Це дозволяє користувачам запускати кілька команд і програм по тому самому безпечному з'єднанню.

На додачу SSH підтримує пересилання агента аутентифікації, що дозволяє клієнту пересилати аутентифікаційну інформацію на віддалений сервер. Ця функція дозволяє користувачам застосовувати той самий метод аутентифікації на декількох віддалених комп'ютерах без необхідності багаторазового введення одних і тих самих облікових даних.

Водночас SSH підтримує методи обміну ключами, що дозволяє двом комп'ютерам безпечно обмінюватися криптографічними ключами. Це дозволяє шифрувати та розшифровувати дані з використанням одного і того ж ключа.

У протокола SSH наявна також підтримка стиснення, що дозволяє стискати дані перед передачею мережі. Це зменшує обсяг мережного трафіку та

прискорює передачу даних [5].

Протокол SSH підтримує кілька інших функцій, таких як спільне використання з'єднань, протоколи тунелювання та виконання проксі-команд. Підтримуються також запити на під’єднання до даних, дозволяючи програмам отримувати доступ до віддалених ресурсів через зашифроване з'єднання.

В цілому, протокол SSH - це безпечний та гнучкий протокол, який використовується для віддаленого доступу та безпечної передачі файлів. Завдяки своїм різним функціям та підтримці кількох методів аутентифікації, це важливий інструмент для безпечного віддаленого доступу.

1.4 Протокол RDP

RDP заснований на протоколі T.120 і використовується переважно для надання графічного інтерфейсу віддаленому комп'ютеру. RDP використовується багатьма організаціями для надання віддаленої підтримки та доступу до систем, застосунків та даних. На рис. 1.4 представлено налаштування безпеки RDP.

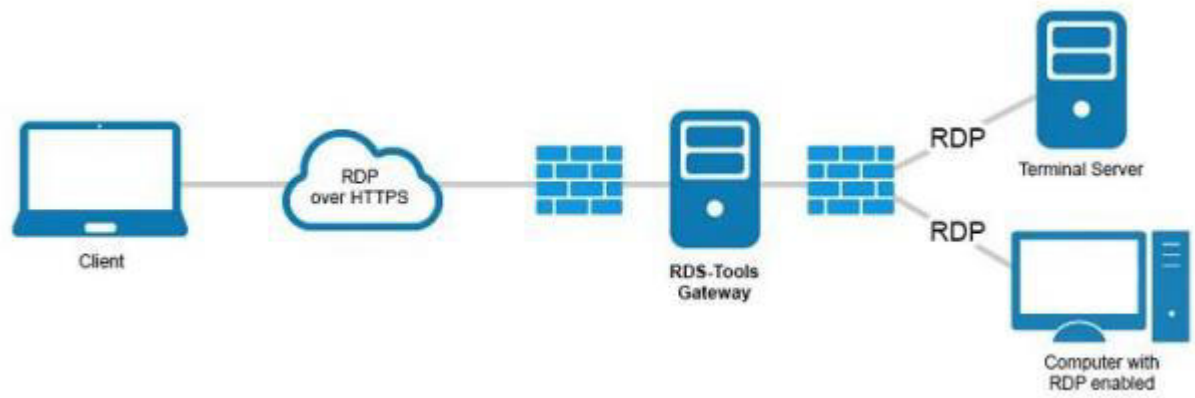

Рисунок 1.4 – Налаштування безпеки протоколу RDP

RDP надає широкий перелік функцій, котрі дозволяють користувачам віддалено виконувати завдання, такі як спільне використання файлів та принтерів, відтворення аудіо та надання віддаленої підтримки. Він також забезпечує зашифроване з'єднання, що допомагає захистити конфіденційність

даних та повідомлень через мережу. Він також надає можливість передавати файли між комп'ютерами, а також копіювати та вставляти текст та зображення з одного комп'ютера на інший.

RDP - це безпечний протокол, що пропонує автентифікацію, шифрування, цілісність та конфіденційність даних. Він також мітить алгоритми стиснення трафіку та диференціального стиснення, які підвищують продуктивність передачі даних. Крім того, RDP можна використовувати для доступу до програм та служб на різних платформах, що дозволяє користувачеві працювати з програмами з різних операційних систем [6].

1.5 VPN

VPN є безпечним та зашифрованим з'єднанням між двома або більше комп'ютерами або пристроями через Інтернет. Цей протокол забезпечує доступ до ресурсів, які зазвичай доступні лише через локальну мережу (LAN) чи Інтернет. VPN використовуються для безпечного під’єднання віддалених офісів та окремих осіб один до одного, а також для безпечного доступу до додатків та ресурсів, розміщених у віддаленій мережі [7].

Коли користувач під’єднується до VPN, з'єднання встановлюється за допомогою спеціального протоколу, званого протоколом тунелювання. Цей протокол шифрує всі дані, які передаються між двома комп'ютерами, використовуючи захищений тунель. Цей тунель встановлюється за допомогою технологій шифрування та аутентифікації. Шифрування гарантує, що дані захищені від будь-якого НСД або модифікації, а автентифікація гарантує, що тільки авторизовані користувачі здатні одержати доступ до даних. На рис. 1.5 можна побачити принцип роботи VPN.

Однією з основних переваг використання VPN є його здатність маскувати online -активність користувача від інтернет-провайдера чи будь-якого іншого стороннього спостерігача.

Рисунок 1.5 – Принцип роботи VPN

Це пов'язано з тим, що всі дані, що надсилаються через тунель VPN, шифруються і відправляються безпечним способом. Це запобігає відстеженню сторонніми особами онлайн -активності користувача або ідентифікації реальної IP- адреси користувача. Крім того, VPN також захищають користувачів від шкідливих Web -сайтів, оскільки вони не зможуть отримати доступ до інформації, що надсилається на комп'ютер або з нього.

Крім забезпечення безпечного з'єднання, VPN також пропонують низку інших переваг, як то підвищену швидкість та надійність. Використовуючи VPN, користувачі можуть відчувати меншу затримку та вищу швидкість завантаження. Спрямовуючи трафік через безпечний тунель, VPN також можуть допомогти скоротити обриви з'єднань.

В цілому, VPN - це універсальний та безпечний спосіб доступу до віддалених мереж та застосунків. Вони забезпечують користувачам безпечне з'єднання, підвищену швидкість та надійність, а також захист від шкідливих Web –сайтів [8].

1.6 Порівняння VPN та RDP

Тут варто зауважити, що VPN і RDP виконують різні задачі, хоча вони обидва забезпечують віддалений доступ [5].

VPN створює будує шифроване з’єднання між пристроєм користувача та мережею. Завдяки йому можна безпечно використовувати корпоративні ресурси, одержувати доступ до певних внутрішніх сервісів і служб чи оминати

блокування за географічним принципом. Водночас усі програми функціонують безпосередньо на користувацькому пристрої, а VPN тільки пересилає дані через захищений “тунель”.

Застосування ж RDP, на противагу до VPN, дає змогу повністю управляти у реальному часі віддаленим пристроєм. Ви бачите його екран, виконуєте програми, міняєте налаштування і працюєте так, наче перебуваєте за ним фізично. Всі обчислення здійснює віддалений комп’ютер, а ваш пристрій тільки відтворює картинку і передає вказівки мишки та клавіатури.

VPN краще використовувати, коли необхідно під'єднатися безпечно до мережі чи послуговуватися інтернетом, уникаючи ризику перехоплення даних. Властиво RDP більше годиться для адміністрування, техпідтримки або роботи із застосунками, котрі встановлені лише на віддаленому ПК. Фактично - це два схожих, проте все ж таки досить різних інструменти для власне роботи користувача в мережі інтернет, проте обидва вони гарантують надійну безпеку і захист від НСД.

У табл. 1.1 представлені основні особливості VPN та RDP

Таблиця 1.1 – Порівняння основних властивостей VPN та RDP

Критерій	VPN	RDP
Рівень безпеки	Високий (при шифруванні)	Залежить від конфігурації
Зручність використання	Потрібне окреме ПЗ, просте	Повний контроль, але складніше
Швидкість	Вища, якщо доступ лише до файлів	Дещо нижча (передача зображення)
Область застосування	Доступ до мережі та ресурсів	Робота з повним ПК
Вимоги до інфрастурктури	Сервер VPN	Віддалений ПК з RDP

1.7 Висновки до першого розділу

На початку першого розділу кваліфікаційної роботи були описані завдання, які необхідно реалізувати для виконання мети.

Далі було розглянуто віддалений доступ, а також детально описаний кожен протокол: SSH, RDP, VPN. Наведено порівняння основних можливостей VPN та RDP.

На підставі описаних переваг та недоліків розглянутих протоколів та технологій вирішено створити свій метод, який міг би конкурувати і навіть перевершити описані вище.

РОЗДІЛ 2 ПРОЄКТНА ЧАСТИНА

2.1 Моделювання архітектури системи віддаленого доступу

Щоб спроектувати архітектуру системи для керування віддаленим доступом до з'єднань SSH, RDP та VPN, необхідно враховувати такі моменти та компоненти [9]:

– автентифікація та авторизація: це процес перевірки особистості користувача, який увійшов до системи, та визначення рівня доступу. Система повинна підтримувати багатофакторну автентифікацію, таку як паролі, біометричні дані та смарт-картки, щоб забезпечити доступ до системи лише авторизованим користувачам;

– контроль доступу. Цей компонент відповідає за контроль доступу до системи на основі ролей та дозволів користувачів. Він мітить налаштування політик для тих, хто може входити в систему, дозволеного типу під'єднання, до яких ресурсів вони можуть отримати доступ і які дії вони можуть робити;

– мережна інфраструктура: сюди входять апаратні та програмні компоненти, які дозволяють системі обмінюватися даними та обробляти дані. Цей компонент повинен забезпечувати безпечну передачу даних, запобігати витоку даних або НСД, а також підтримувати високошвидкісні з'єднання для мінімізації затримки;

– моніторинг та звітність. Компонент відповідає за відстеження дій користувачів, продуктивності системи та подій безпеки. Він повинен генерувати звіти, оповіщення та повідомлення, щоб попереджати системних адміністраторів про будь-які проблеми чи потенційні загрози;

– консоль управління: це основний інтерфейс, який використовується системними адміністраторами для управління системою, як то налаштування

параметрів та моніторингу продуктивності. Він повинен бути зручним та інтуїтивно зрозумілим, дозволяючи адміністраторам легко отримувати доступ до системних журналів, звітів та оповіщень.

В загальному, архітектура повинна бути розроблена з урахуванням безпеки, гарантуючи, що всі з'єднання зашифровані, автентифікація надійна, а політики контролю доступу є суворими. Таким чином, ризик НСД або витоку даних може бути зведений до мінімуму, а система може працювати безперебійно та ефективно.

На рис. 2.1 представлена архітектура протоколів SSH, RDP та VPN.

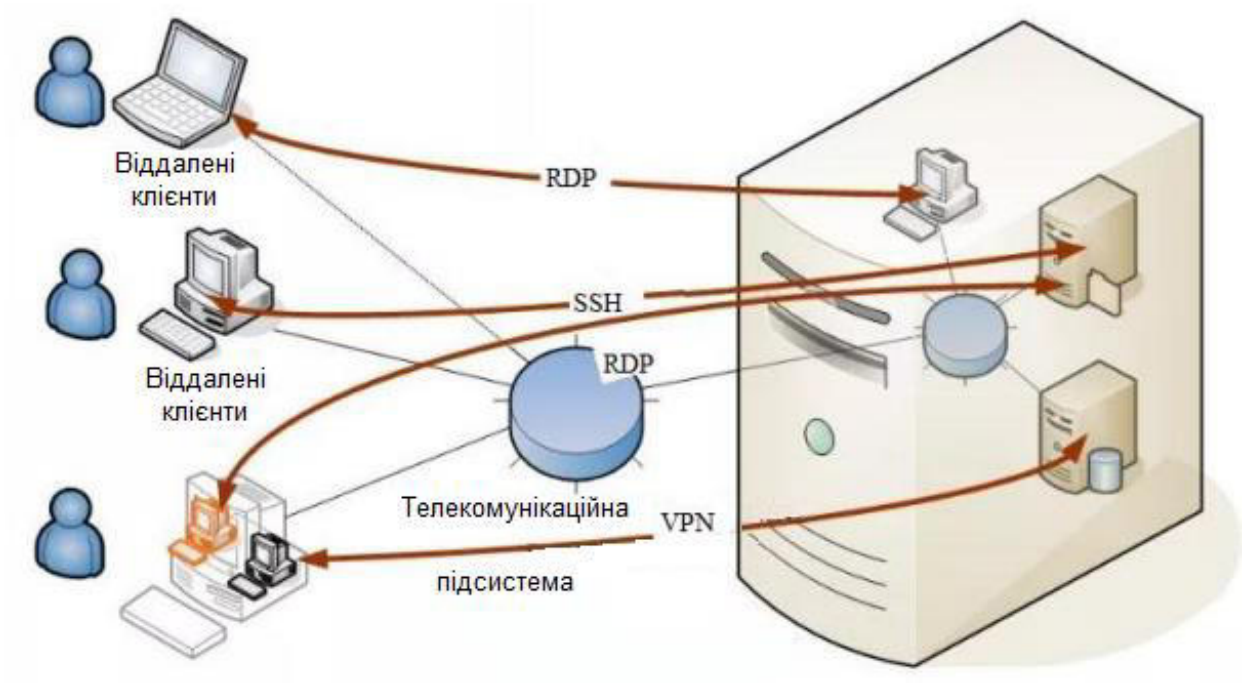

Рисунок 2.1 – Архітектура протоколів

2.2 Модель даних

Спроектуємо логічну модель.

Об'єкти:

– користувач;
– сервер віддаленого доступу;
– брандмауер;

– сервер аутентифікації;

– політика контролю доступу

Атрибути:

– користувач: Ім'я користувача, пароль, роль;

– сервер віддаленого доступу: IP- адреса, тип (SSH, RDP або VPN);

– брандмауер: IP- адреса, номер порту, дозволені протоколи;

– сервер аутентифікації: IP- адреса, метод аутентифікації (наприклад, LDAP, Active Directory);

– політика контролю доступу: список користувачів, дозволені сервери віддаленого доступу, дозволені протоколи, часові обмеження.

Відносини:

– користувач може аутентифікуватись на сервері аутентифікації;

– користувач може запросити доступ до сервера віддаленого доступу;

– брандмауер перевіряє, чи відповідає запит політиці контролю доступу;

– якщо запит схвалений мережевим екраном, користувач може встановити з'єднання із сервером віддаленого доступу.

Обмеження:

– користувач повинен мати дійсні облікові дані для автентифікації на сервері автентифікації;

– користувач повинен мати відповідну роль для запиту доступу до віддаленого сервера;

– політика контролю доступу має бути визначена та регулярно оновлюватися;

– брандмауер має бути правильно налаштований для забезпечення дотримання політики контролю доступу;

– сервери віддаленого доступу повинні бути належним чином захищені та оновлені для запобігання НСД або вразливості.

Спроектована логічна модель показана на рис. 2.2.

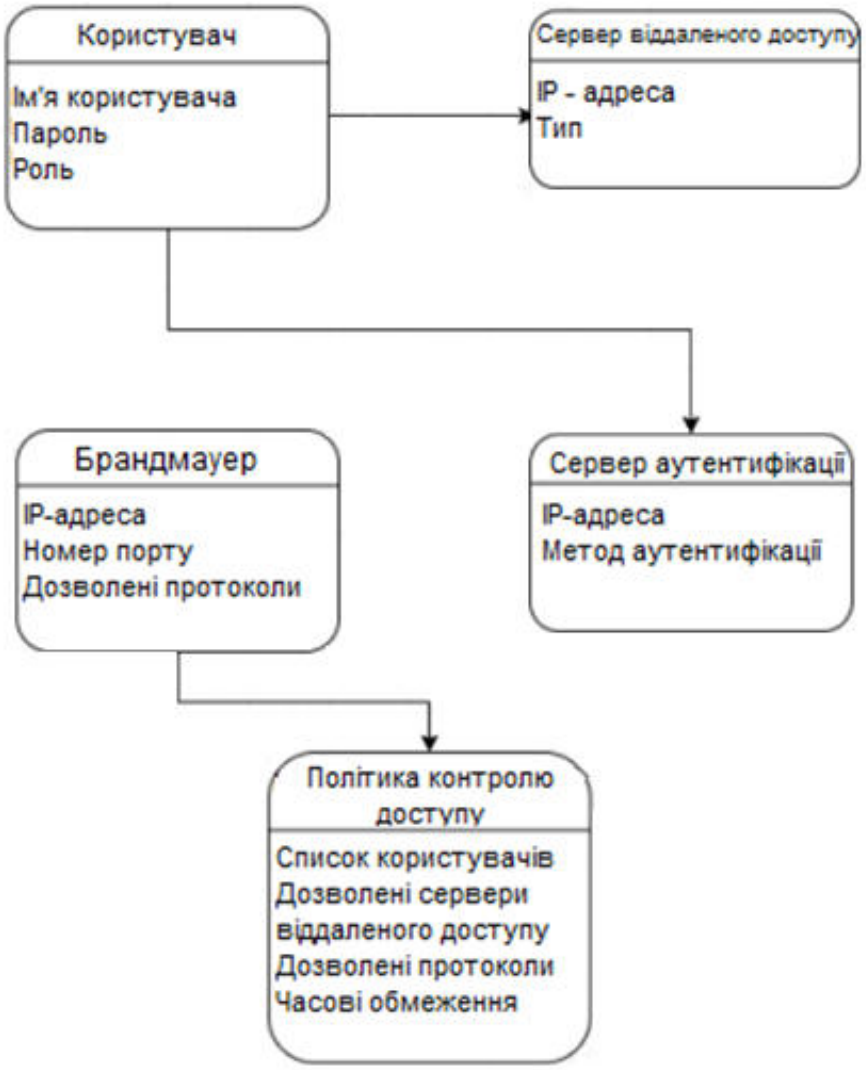

Рисунок 2.2 – Логічна модель даних

Фізична модель керування віддаленим доступом для з'єднань SSH, RDP і VPN може бути пристроєм мережевої безпеки. Цей пристрій може бути виділеним апаратним пристроєм або віртуальною машиною, яка працює на сервері. Пристрій діятиме як шлюз між внутрішньою мережею та зовнішніми користувачами або пристроями, які намагаються отримати доступ до мережі через протоколи SSH, RDP або VPN [10].

Пристрій буде володіти різними функціями безпеки, такі як брандмауери, системи виявлення / запобігання вторгнень і сканери шкідливих програм, для захисту мережі від кіберзагроз. Він також мітитиме функції аутентифікації та контролю доступу, такі як багатофакторна автентифікація, управління доступом

на основі ролей та моніторинг активності користувачів.

Фізична модель також може мати додаткові апаратні компоненти, такі як мережеві комутатори та маршрутизатори, для забезпечення зв'язку між пристроєм, внутрішньою мережею та зовнішніми пристроями. Модель також може мітити в своєму складі інтерфейс для адміністраторів, що дозволяє керувати пристроєм і налаштовувати його, а також відстежувати мережну активність.

2.3 Діаграма компонентів

Схема, на якій показані системні компоненти керування віддаленим доступом для з'єднань SSH, RDP і VPN, продемонстрована на рис. 2.3.

На цій схемі сервер віддаленого доступу відповідає за керування віддаленим доступом до мережі. Цей сервер підтримує з'єднання SSH, RDP та VPN.

Сервер аутентифікації використовується для перевірки особистості віддалених користувачів, які намагаються отримати доступ до мережі. Цей сервер зв'язується з базою даних користувачів для перевірки інформації про ім'я користувача та пароль.

Нарешті брандмауер/маршрутизатор відповідає за контроль доступу до мережі. Цей компонент блокує спроби НСД, дозволяючи користувачам, які пройшли автентифікацію, під’єднуватися до сервера віддаленого доступу.

Рисунок 2.3 – Діаграма компонентів

2.4 Контроль віддаленого доступу

У нашій країні є два основних напрями контролю віддаленого під’єднання користувачів.

Перший передбачає використання IPsec VPN, для якого потрібно попередньо встановлений VPN -клієнт та додаткові заходи безпеки, такі як повне шифрування диска, антивірусне ПЗ та засоби автентифікації користувачів. Однак реалізація цих механізмів в одному програмному клієнті може призвести до значної економії коштів.

Другий тренд - використання технології SSL VPN, якій віддають перевагу, коли немає можливості контролювати кожне віддалене робоче місце [11]. Важливо ретельно вибирати постачальника рішення, оскільки як робоче місце можна використовувати будь-який комп'ютер або смартфон. Ефективним

рішенням є можливість створення безпечної робочої області за умови під’єднання до шлюзу SSL VPN на клієнтській машині, яка гарантовано не містить шкідливого ПЗ. Це позбавляє необхідності встановлювати антивірусне ПЗ, але виробники таких рішень використовують метод «пісочниці», щоб запобігти безпосередній взаємодії прикладного ПЗ з ядром операційної системи.

2.5 Висновки до другого розділу

Другий розділ роботи присвячений опису архітектури та моделювання контролю віддаленого доступу.

Архітектура має бути розроблена з урахуванням безпеки, гарантуючи, що всі з'єднання зашифровані, аутентифікація надійна, а політики контролю доступу суворі. Врахували компоненти, щоб спроектувати архітектуру системи для керування віддаленим доступом до з'єднань SSH, RDP і VPN,

Також були описані фізична та логічна модель. Була створена схема, на якій показано системні компоненти для керування віддаленим доступом для з'єднань SSH, RDP та VPN.

.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 РЕАЛІЗАЦІЯ ВІДДАЛЕНОГО ДОСТУПУ

Для реалізації необхідно спочатку встановити PuTTY, для генерації ключа, як це показано на рис. 3.1.

Рисунок 3.1 – Генерація ключа

Після генерації ключа, потрібно створити та зберегти приватний ключ користувача, де потрібно ввести та повторити пароль, відображено це на рис. 3.2.

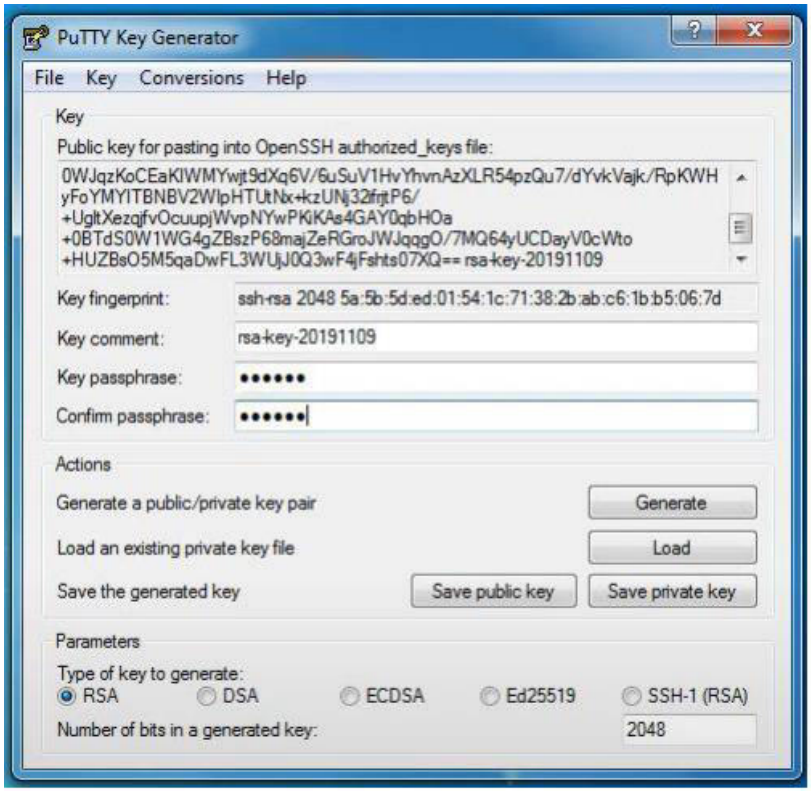

Рисунок 3.2 – Створення та збереження приватного ключа користувача

Переходимо на віддалений комп'ютер за допомогою віддаленого доступу AnyDesk із використанням freeSSHd, як показано на рис. 3.3.

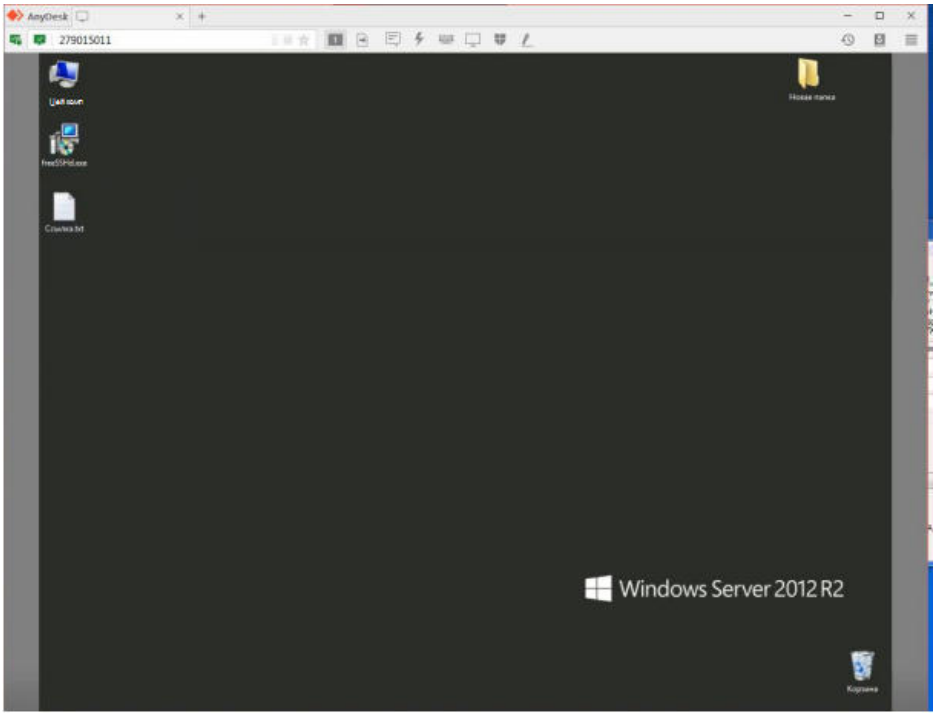

Рисунок 3.3 – Віддалений доступ AnyDesk з використанням freeSSHd

Запустимо встановлення freeSSHd.exe, де скрізь вибираємо «Далі», підтверджуємо створення нового ключа сервера. У нас з'явився значок FreeSSHd, який потрібно запускати від імені адміністратора, як це показано на рис. 3.4.

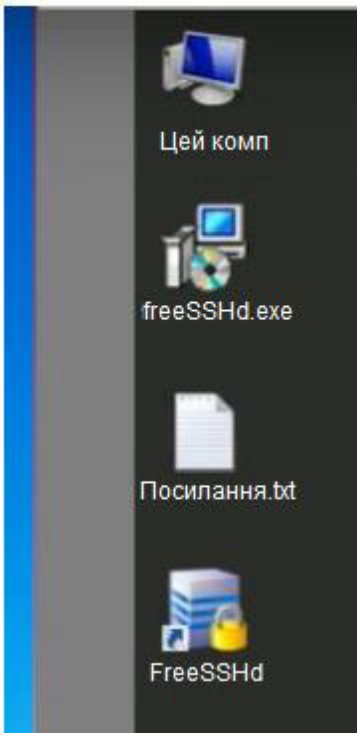

Рисунок 3.4 – Встановлений FreeSSHd

При першому запуску програма вітає та дякує за використання програми, це відображено на рис. 3.5.

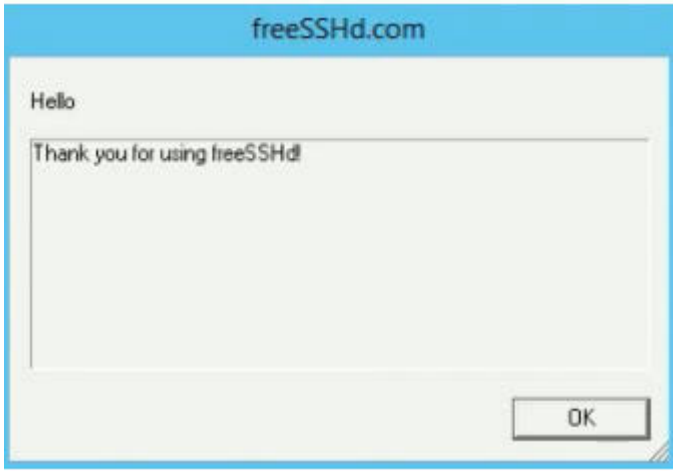

Рисунок 3.5 – Запуск FreeSSHd від імені адміністратора

У панелі задач знаходимо значок FreeSSHd та натискаємо на нього. Вводимо дані для авторизації, де вводимо ключ (рис. 3.6).

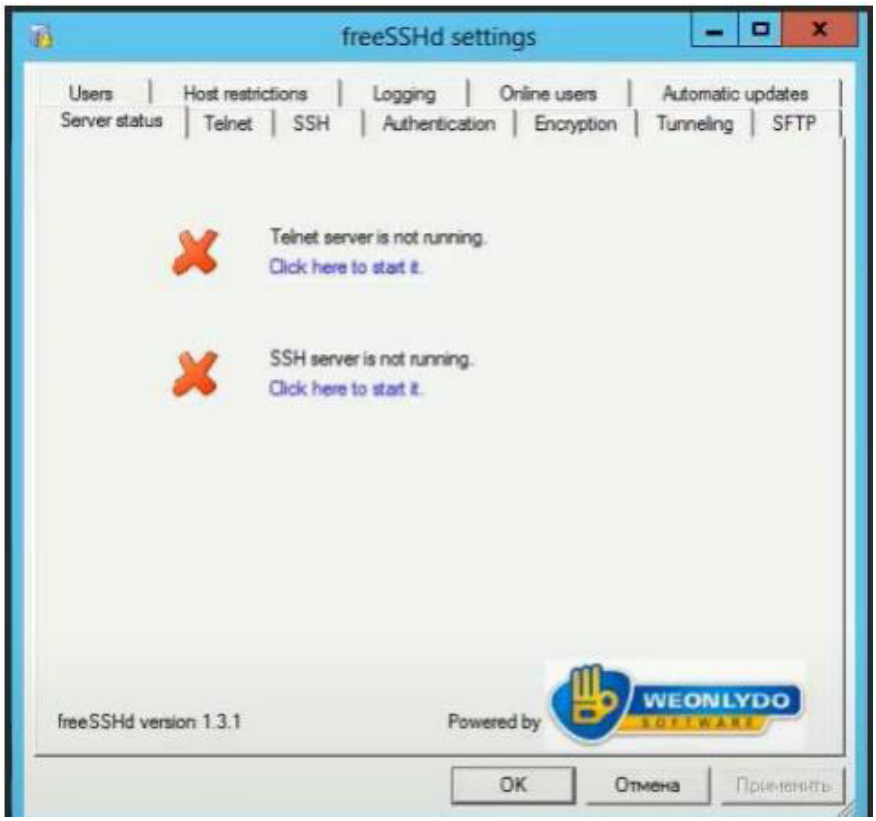

Рисунок 3.6 – Вхід у програму FreeSSHd

Тепер переходимо на вкладку SSH, вибираємо IP-алресу, залишаємо стандартний порт, нижче встановлюємо максимальну кількість клієнтів, одночасно під’єднаних до сервера та вибираємо час, через який програма закриє сесію, якщо вона не активна [12]. Нижче можна згенерувати ключі SSH, але це не є обов'язковим (рис. 3.7).

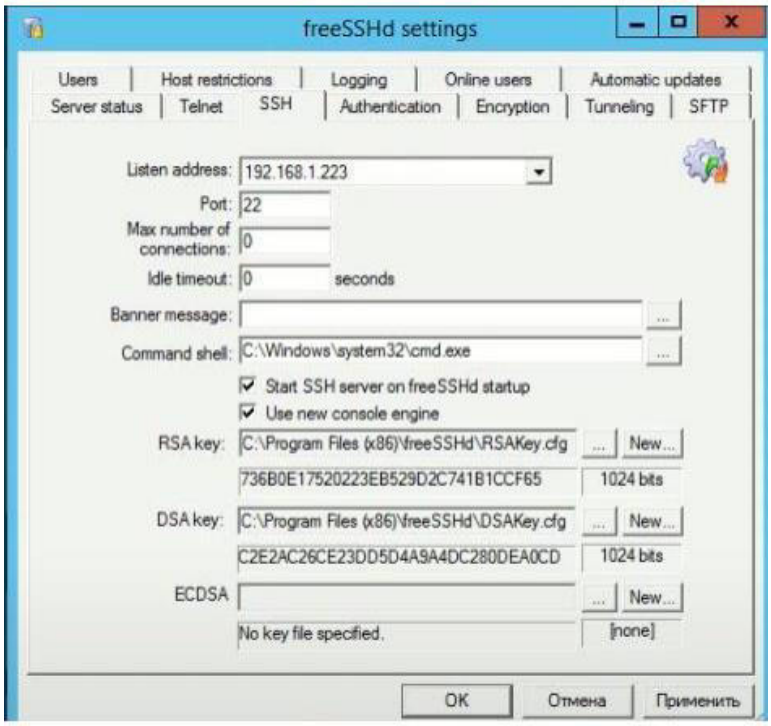

Рисунок 3.7 – Налаштування адреси

Далі переходимо у вкладку «Автентифікація» (рис. 3.8), де ставимо заборону авторизації паролем і вибираємо авторизацію за публічним ключем з перевіркою

Рисунок 3.8 –Вкладка «Автентифікація»

Тепер переходимо у вкладку автоматичного оновлення (рис. 3.9), де забираємо прапорець, для подальшої коректної роботи програми.

Рисунок 3.9 – Вимкнення автоматичного оновлення

На цьому основне налаштування сервера закінчено.

Тепер потрібно зайти в керування комп'ютером (рис. 3.10), у служби та перезапустити служби SSHD Service [6]. Зробили ми це для того, щоб зміни в налаштуваннях, які ми зробили, вони застосувалися.

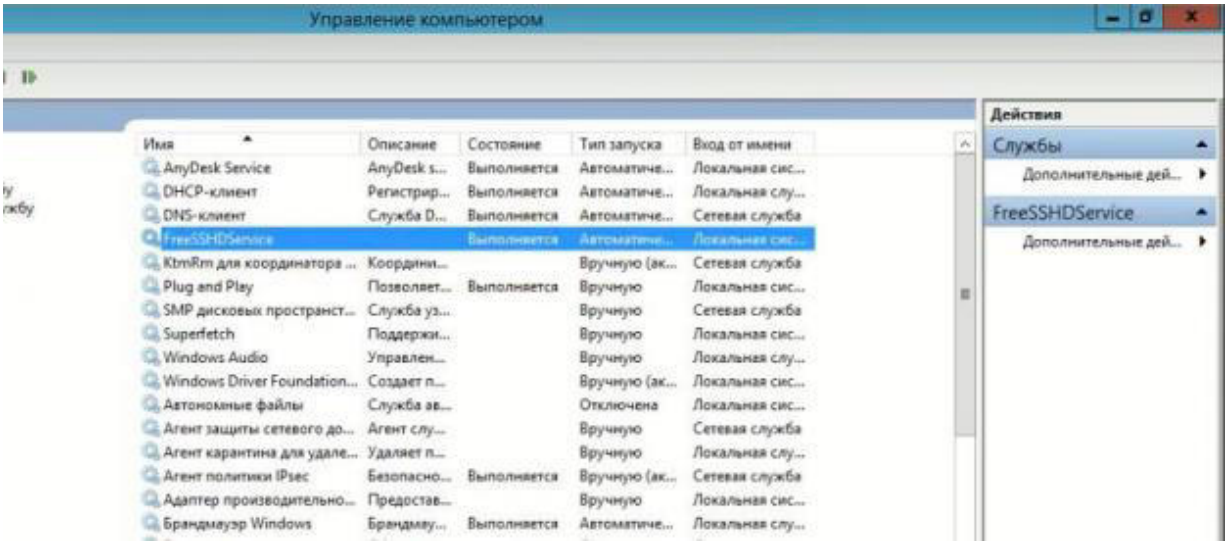

Рисунок 3.10 – Перезапуск служби FreeSSHD Service

Далі потрібно зайти в брандмауер Windows (рис. 3.11), де у вкладці «Правила для під'єднання», натискаємо «Створити правило» (рис. 3.12). Правила, ми будемо створювати для вхідних під'єднань (рис. 3.13), для порту (рис. 3.14).

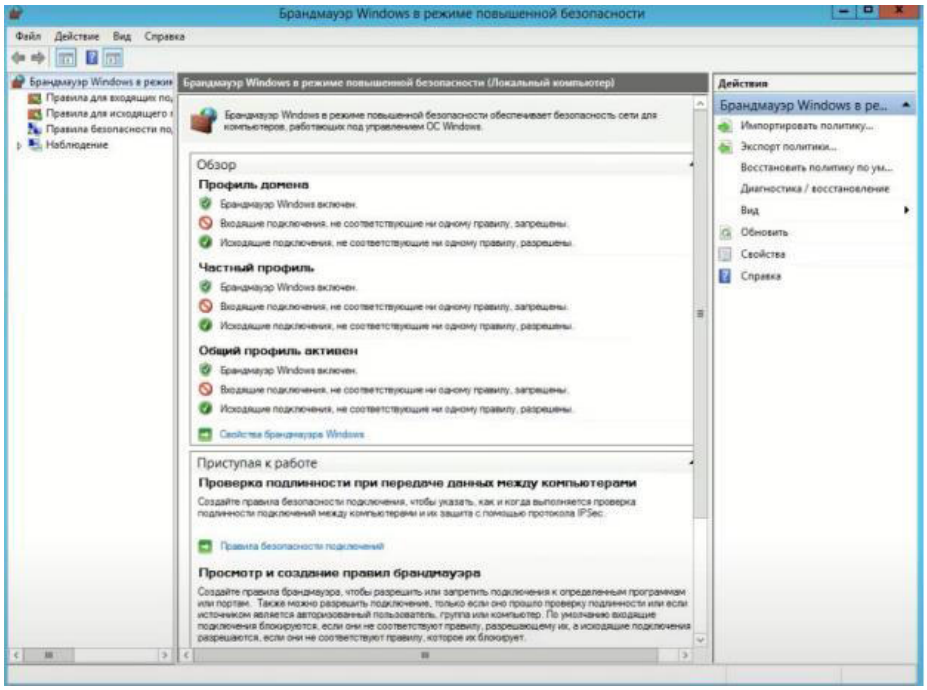

Рисунок 3.11 – Вікно брандмауер Windows

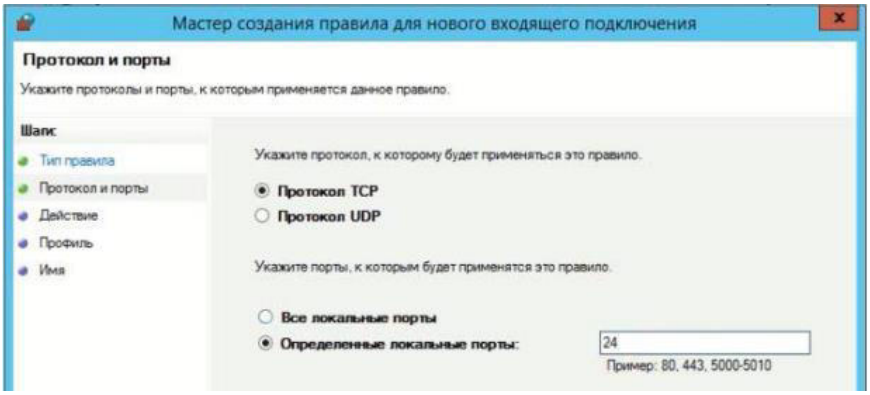

Рисунок 3.12 – Налаштування нових під'єднань

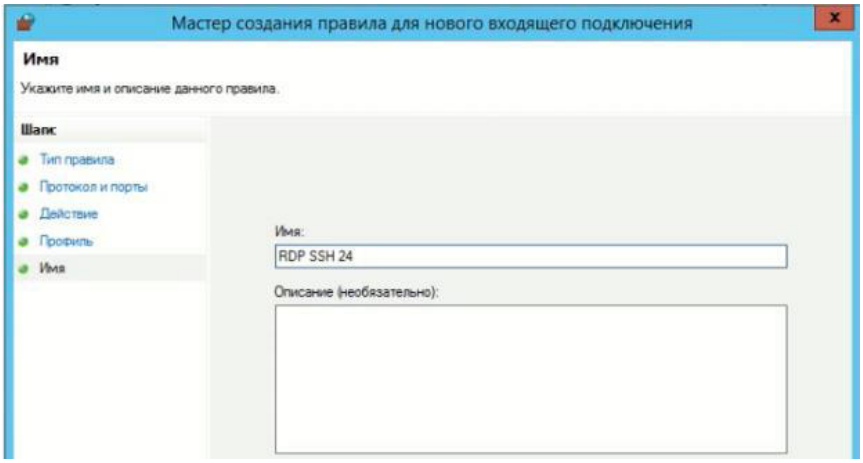

Рисунок 3.13 – Створення правил

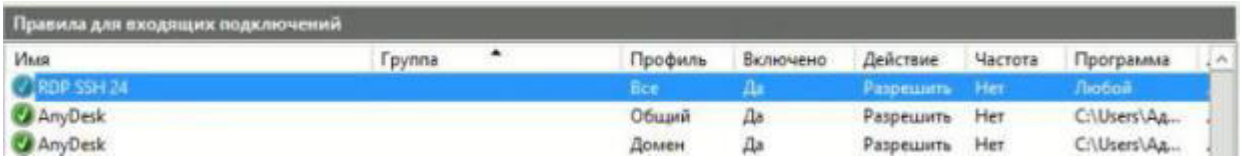

Рисунок 3.14 – Дозвільне правило

Тепер необхідно заборонити стандартний порт RDP, за протоколами TCP та UDP, як це показано на рис. 3.15.

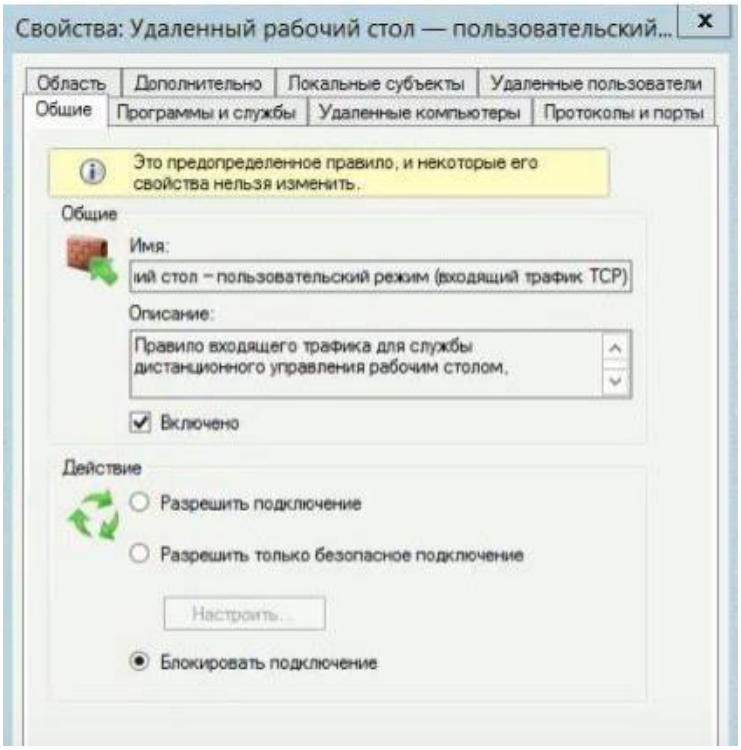

Рисунок 3.15 – Блокування під’єднання

Тепер на робочому комп'ютері запускаємо програму PuTTY (рис. 3.16). Де вводимо IP-адресу і порт [14]. Далі вводимо назву під’єднання та зберігаємо.

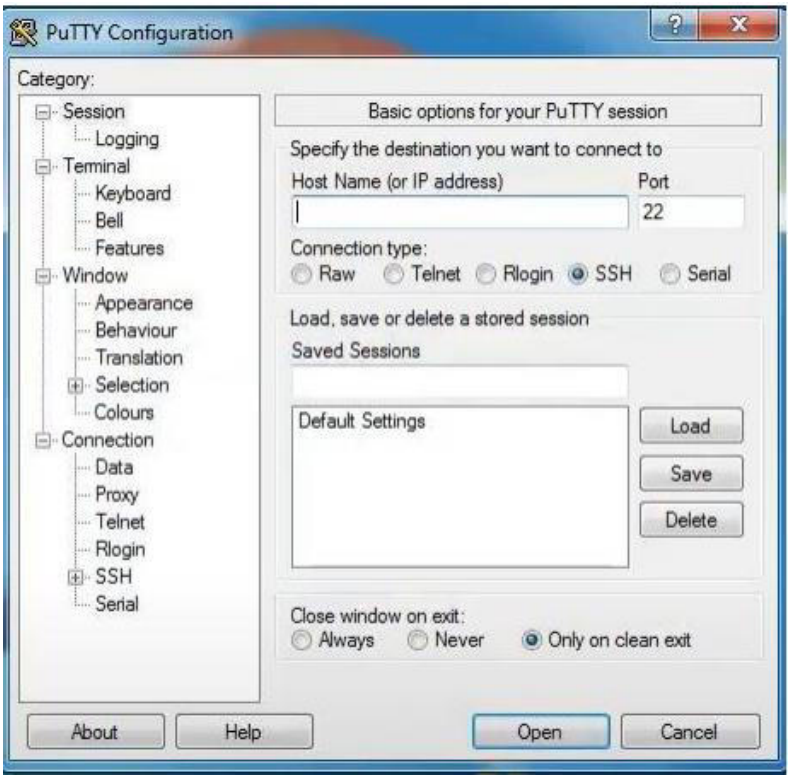

Рисунок 3.16 – Налаштування програми PuTTY

У вікні вводимо логін і пароль від приватного ключа користувача. Якщо нижній рядок виглядає так - "This service is prohibited", то користувач успішно авторизувався. Це продемонстровано на рис. 3.17.

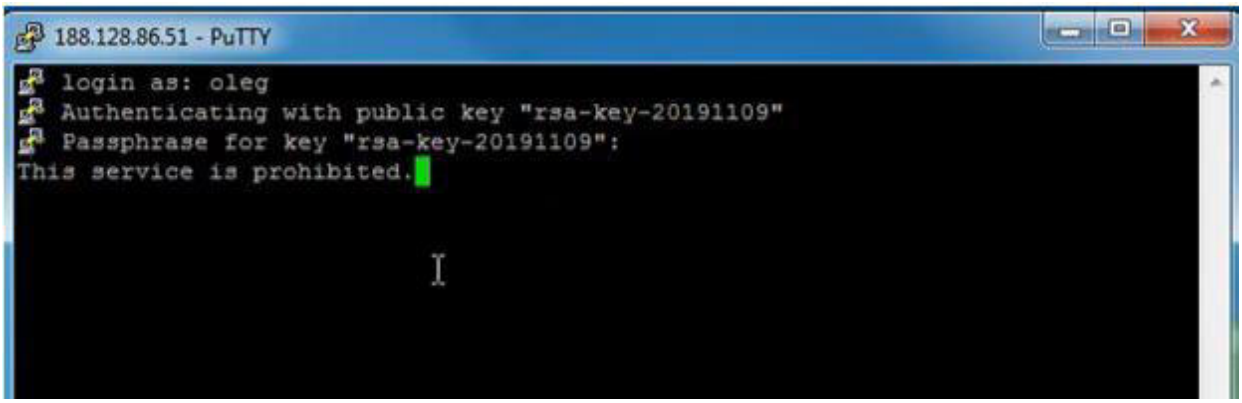

Рисунок 3.17 – Авторизація користувача

Запускаємо віддалений робочий стіл, як показано на рис. 3.18, вводимо localhost: 3391, це порт, який ми вибрали в налаштуваннях PuTTY.

Далі вводимо логін та пароль облікового запису Windows віддаленого комп'ютера.

Ми під’єдналися до віддаленого комп'ютера за протоколом RDP, а всередині тунель SSH за допомогою ключів (рис. 3.18).

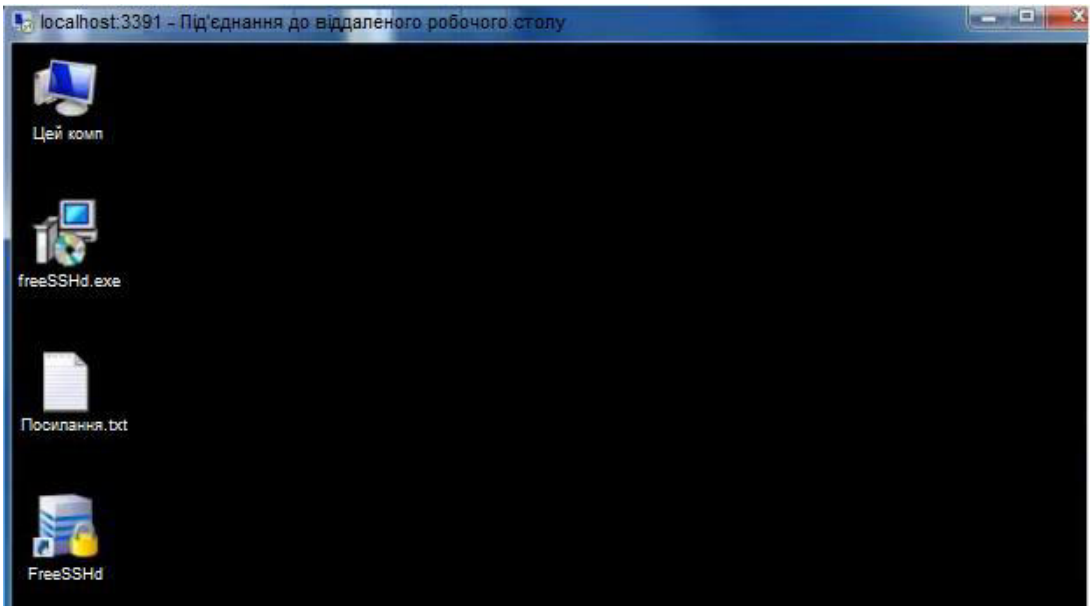

Рисунок 3.18 – Віддалений комп'ютер за протоколом RDP

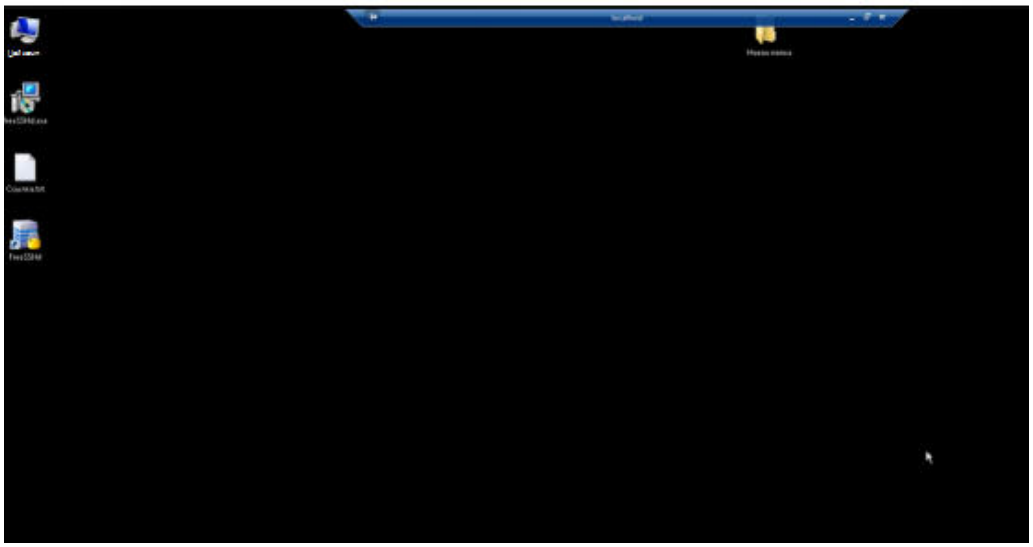

Рисунок 3.19 – Віддалений комп'ютер за допомогою тунелю SSH

Щоб розпочати налаштування SSL VPN Plus, перейдіть на вкладку

“Authentication”, щоб увімкнути та налаштувати сервер аутентифікації (рис. 3.20).

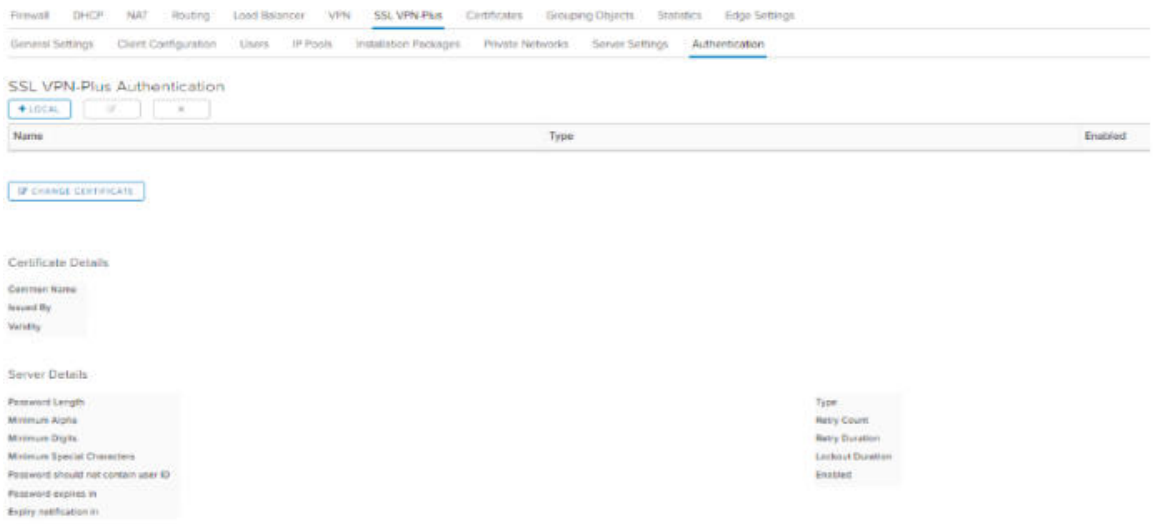

Рисунок 3.20 – Налаштування SSL VPN Plus

На вкладці IP Pools ми задаємо адреси, що видаються клієнтам, котрі під’єднуються, як це показано на рис. 3.21 27,. Ці IP -адреси повинні знаходитися в підмережі, що має доступ до існуючого середовища. Ця підмережа пула не повинна відповідати мережі vDC

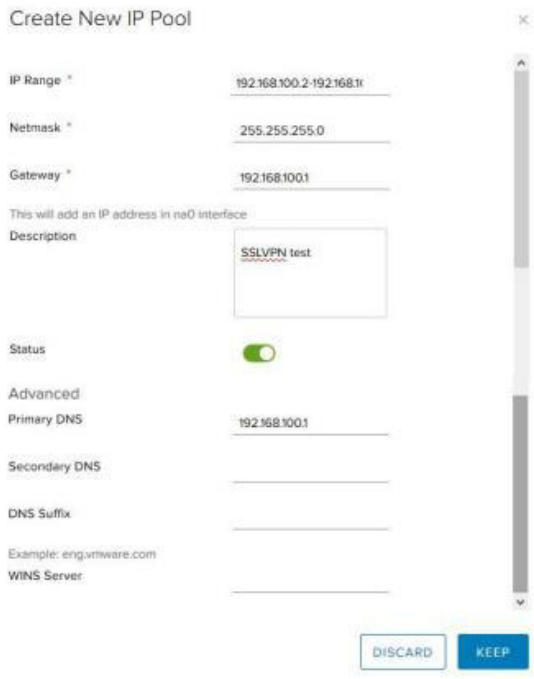

Рисунок 3.21 – Налаштування IP Pools

Додаємо користувача вручну (рис. 3.22).

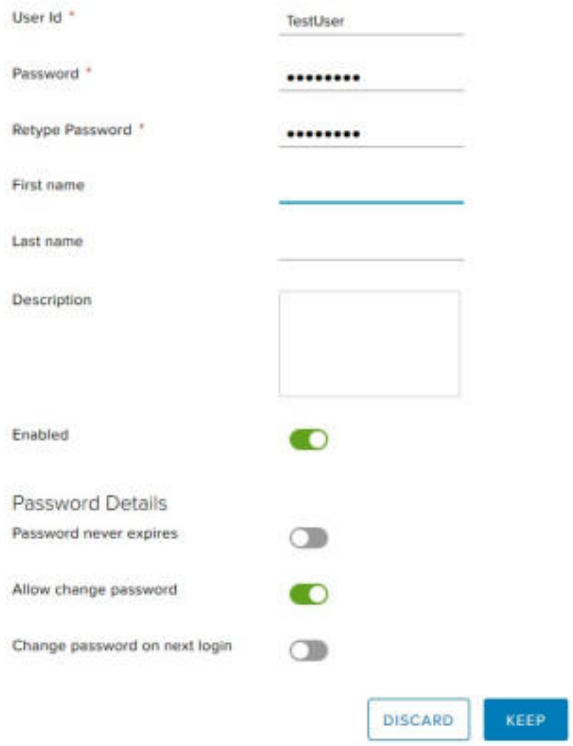

Рисунок 3.22 – Реєстрація користувача в системі

Встановимо користувача SSL VPN під Windows (рис. 3.23).

Рисунок 3.23 – Налаштування користувача SSL VPN під Windows

Запустимо встановлений клієнт, натиснемо Login, та введемо облікові дані користувача (рис. 3.24).

Рисунок 3.24 – Запуск клієнта до системи

3.2 Висновки до третього розділу

Третій розділ роботи присвячено реалізації віддаленого доступу.

Для реалізації спочатку встановили PuTTY для генерації ключа.

Запустили інсталяцію freeSSHd.exe, де наприкінці підтверджуємо створення нового ключа сервера. У нас з'явився значок FreeSSHd, який потрібно запускати від імені адміністратора.

Далі потрібно було зайти до брандмауера Windows, де у вкладці правила для вхідних під’єднань натиснули «Створити правило». Правила ми створили для вхідних під’єднань, для порту.

Ми під’єдналися до віддаленого комп'ютера за протоколом RDP, а всередині тунель SSH за допомогою ключів, а також контролювати ми зможемо завдяки встановленому та налаштованому SSL VPN Plus.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Соціальне значення охорони праці

Соціальне значення охорони праці полягає в сприянні росту ефективності суспільного виробництва шляхом безперервного вдосконалення і поліпшення умов праці, підвищення їх безпеки, зниження виробничого травматизму і профзахворювань [19]. Соціальне значення охорони праці проявляється в зростанні продуктивності праці, збереженні трудових ресурсів і збільшенні сукупного національного продукту.

Охорона праці полягає в сприянні росту ефективності виробництва, яке досягається шляхом безперервного вдосконалення і поліпшення умов праці, підвищення їх безпеки, зниження виробничого травматизму і профзахворювань.

Зростання продуктивності праці відбувається в результаті збільшення фонду робочого часу завдяки скороченню внутрішньо-змінних простоїв шляхом ліквідації мікротравм або зниження їх кількості, а також завдяки запобіганню передчасного стомлення шляхом раціоналізації і покращення умов праці та введенню оптимальних режимів праці і відпочинку та інших заходів, які сприяють підвищенню ефективності використання робочого часу.

Важливим питанням є зростання продуктивності праці, яка відбувається в результаті збільшення фонду робочого часу завдяки скороченню внутрішньозмінних простоїв шляхом ліквідації мікротравм або зниження їх кількості, а також завдяки запобіганню передчасного стомлення шляхом раціоналізації і покращення умов праці та введенню оптимальних режимів праці і відпочинку та інших заходів, які сприяють підвищенню ефективності використання робочого часу [19].

Особливої уваги заслуговує те, що збереження трудових ресурсів і підвищення професійної активності працюючих відбувається завдяки покращенню стану здоров’я і подовженню середньої тривалості життя шляхом покращення умов праці, що супроводжується високою трудовою активністю і підвищенням виробничого стажу. Підвищується професійний рівень також завдяки зростанню кваліфікації і майстерності. Відповідно і збільшення сукупного національного продукту відбувається завдяки покращенню вищеперелічених показників та їх складових компонентів. Збереження трудових ресурсів і підвищення професійної активності працюючих відбувається завдяки покращенню стану здоров'я і подовженню середньої тривалості життя шляхом покращення умов праці, що супроводжується високою трудовою активністю і підвищенням виробничого стажу. Підвищується професійний рівень також завдяки зростанню кваліфікації і майстерності. Збільшення сукупного національного продукту відбувається завдяки покращенню вищеперелічених показників та їх складових компонентів. Крім того, соціальне значення охорони праці проявляється в зростанні продуктивності праці, збереженні трудових ресурсів.

Комплекс заходів з поліпшення умов праці може забезпечити приріст продуктивності праці на 15-20%. Так, нормалізація освітлення робочих місць збільшує продуктивність на 6-13% та скорочує брак на 25%. Раціональна організація робочого місця підвищує продуктивність праці на 21%, раціональне фарбування робочих приміщень – на 25% [20]. Збільшення ефективного фонду робочого часу може бути досягнуто за рахунок скорочення тимчасової непрацездатності працівників внаслідок хвороб та виробничого травматизму.

4.2 Методи боротьби з монотонністю праці на виробництві

У перекладі з грецької монотонність означає одноманітність. Монотонною вважається робота, яка відповідає таким ознакам: невелика кількість виконуваних дій, простота дій, часта повторюваність дій. Таким чином робота з

розроблюваною комп'ютерною системою є монотонною, оскільки оператор повинен лише перемикатись між давачами, слідкувати за їхніми показами і фіксувати їх, а також час від часу вносити поправки в налаштування [20].

В залежності від виду роботи і навантаження на організм людини виділяють два типи монотонності:

– рухова монотонність – характерна для робіт, де основне навантаження припадає на опорно – руховий апарат. Така робота характеризується одноманітними рухами і діями, а основне навантаження припадає на якусь обмежену групу м'язів. Прикладом таких робіт є прості верстатні роботи, робота на конвеєрі, ручні допоміжні роботи, тощо;

– сенсорна монотонність – характерна для робіт, пов'язаних з обробкою інформації. В них вимагається постійне напруження сенсорних органів, уваги, пам'яті. Прикладом таких робіт є тривале пасивне спостереження.

При тривалому виконанні монотонних робіт у працівників виникає втома, зменшується увага, погіршується якість виконаної роботи. Це все може призвести до помилкових дій і аварійних ситуацій. В довго строковій перспективі монотонна роботи може мати такі наслідки:

– швидкий розвиток втоми в зв'язку з локалізацією м'язових і нервових навантажень;

– гіподинамія;

– розвиток неврозів;

– незадоволення роботою і зниження творчої активності працівника;

– підвищена плинність кадрів.

Для боротьби з монотонністю існують два підходи:

– зробити роботу менш одноманітною. Для цього робочий процес потрібно переробити так, щоб кількість окремих робіт зменшилась, але вони стали більш складними, наприклад об'єднати кілька простих процесів в один складний. Також, можна регулювати навантаження в залежності від стану робітників, наприклад, при роботі за конвеєром можна пускати його швидше чи повільніше;

– додати сторонні подразники. Оскільки однією з причин монотонності є мала кількість подразників, то можна збільшити їх штучно, наприклад ввімкнувши на робочому місці музику. Звісно додавати додаткові подразники можна лише за умови, якщо вони не будуть відволікати працівників від основної роботи.

При роботі з розроблюваною системою перший метод не підходить, оскільки слідкувати за виміряними параметрами потрібно з певною частотою, яку не можна змінити.

Також потрібно чергувати монотонну працю з якоюсь іншою [20]. При зміні діяльності потрібно враховувати наступне:

– операції, що підбираються для чергування, не повинні завантажувати ті самі органи й системи організму. Доцільно чергувати фізичну роботу з розумовою, навантаження на орган зору з роботою, де беруть участь інші аналізатори (слухові, дотикальні й ін.), роботу з керування механізмами — з ручною працею;

– при зміні форм діяльності необхідно враховувати вік працівників, тому що в молодих людей цей метод дає більший ефект, чим у людей похилого віку;

– систематичне чергування видів праці можна вводити лише тоді, коли працівники повністю опановують кожною з виконуваних операцій;

– робота, що сполучається, повинна бути помірною або легшою, порівняно з основною; – при сполученні робіт найкращого результату можна досягти коли більш інтенсивна робота заміняється менш інтенсивною, важча й складніша — простішою;

– чергуючі роботи повинні відрізнятися за характером робочої пози, навантаженням на різні ланки рухового апарата, забезпечувати перемикання діяльності з одних м’язових груп на інші. Статична напруга м’язів у відомих межах є стимулятором динамічної роботи. Це необхідно враховувати при сполученні робіт;

– залежно від швидкості перебудови робочого динамічного стереотипу (це залежить від складності робіт) чергування виконуваних робіт у часі може

здійснюватися протягом робочої зміни, тижня або більше тривалих відрізків часу;

– на ділянках з несприятливими умовами праці сполучення операцій застосовується з метою скорочення часу впливу несприятливих факторів на організм людини.

4.3 Висновки до четвертого розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки в надзвичайних ситуаціях, зокрема висвітлені питання соціального значення охорони праці та методи боротьби з монотонністю праці на виробництві.

ВИСНОВКИ

Кваліфікаційна робота присвячена контролю дистанційного доступу при під’єднаннях SSH, RDP та VPN.

У ході виконання було проведено аналіз предметної галузі, виявлено проблеми, властиві досліджуваній галузі.

На початку першого розділу кваліфікаційної роботи було описано завдання, які необхідно реалізувати до виконання мети.

Далі було розглянуто віддалений доступ, а також детально описаний кожен протокол: SSH, RDP, VPN.

Було вирішено створити свій метод віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом.

Архітектура була розроблена з урахуванням безпеки, гарантуючи, що всі з'єднання зашифровані, автентифікація надійна, а політики контролю доступу є суворими.

Також були описані фізична та логічна моделі. І була створена схема, на якій показано системні компоненти для керування віддаленим доступом для з'єднань SSH, RDP та VPN.

Під’єднання до віддаленого комп'ютера виконано за протоколом RDP, а всередині тунель SSH за допомогою ключів, а також контроль за допомогою встановленого та налаштованого SSL VPN Plus.

Завдання, визначені задля досягнення мети роботи, було виконано повному обсязі.

Таким чином мета бакалаврської роботи було досягнуто – створено контроль віддаленого доступу при під’єднаннях SSH, RDP та VPN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 1 [навчальний посібник]. Львів : «Магнолія 2006», 2013. 256 с.
2. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. Ч. 2. 372 с.
3. SSH. Що це і для чого? URL: https://hyperhost.ua/info/uk/ssh-shcho-tse-i-dlya-chogo (дата звертання: 10.05.2026).
4. Sullivan, D. Proven Portals: Best Practices for Planning, Designing, and Developing Enterprise Portals: Addison Wesley Professional, 2013. 224 p.
5. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с.
6. Захищений віддалений доступ: VPN чи RDP? URL: https://hyperhost.ua/info/uk/zaxishhenii-viddalenii-dostup-vpn-ci-rdp (дата звертання: 12.05.2026).
7. Кривий С.Л. Математичні основи захист інформації . Київ: ВПЦ «Київський університет». 2023. 352 с.
8. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.
9. Andrew S. Tanenbaum, David J. Wetherall. Computer networks. Prentice Hall. 2011. 960 p.
10. Adrian D.A. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. URL: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf (дата звертання: 20.05.2026).
11. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок та ін. Київ : КУБГ, 2019. 218 с.

12. SSH протокол. URL: https://itmaster.biz.ua/directory/standarts/ssh.html (дата звертання: 21.05.2026).

13. Литвин В.В., Пасічник В.В., Шаховська Н.Б. Проектування інформаційних систем. Київ: Магнолія 2006, 2024. 380 с.

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

15. Жаровський Р.О., Луцик Н.С., Осухівська Г.М., Паламар А.М., Тиш Є.В. Методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль: ТНТУ, 2024. 39 с.

16. Луцків А., Лупенко С., Пасічник В. Паралельні та розподільнені обчислення. Навчальний посібник. Львів: Видавництво «Магнолія 2006», 2024. 566 с.

17. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том другий. Львів: «Магнолія 2006», 2024. 333 с.

18. Voloshchuk A., Velychko D., Osukhivska H., Palamar A. Computer system for energy distribution in conditions of electricity shortage using artificial intelligence. CEUR Workshop Proceedings, 2nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024), Ternopil, Ukraine, June 12-14, 2024. Vol. 3742 P. 66-75.

19. Толок А.О., Крюковська О.А. Безпека життєдіяльності: Навч. посібник. 2011. 215 с.

20. Основи охорони праці: Підручник.; 3-те видання, доповнене та перероблене / За ред. К. Н Ткачука. К.: Основа, 2011. 480 с.

Додаток А.

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп’ютерно-інформаційних систем і програмної інженерії

Кафедра комп’ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС

_____ Осухівська Г.М.

“___” _____2026 р

СИСТЕМА ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ КОМП’ЮТЕРИЗОВАНОГО РОБОЧОГО МІСЦЯ З ЗАХИЩЕНИМ ДОСТУПОМ НА ОСНОВІ З’ЄДНАНЬ SSH, RDP ТА VPN

ТЕХНІЧНЕ ЗАВДАННЯ

на _8_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІ-41
_____ к.т.н., доц. Баран І.О.	_____ Глушко М.В.
«____» _____ 2026 р.	«____» _____ 2026 р.

Тернопіль 2026

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.157.00.00

1.2 Виконавець

Студент групи СІ-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерної інженерії, Тернопільського національного технічного університету імені Івана Пулюя, Глушко Максим Володимирович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№ 4/9-188 від 24.04.2026 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 26.01.2026 р.

Плановий термін завершення виконання кваліфікаційної роботи – 18.06.2026 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ІСО, ЄСКД, ЄСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи.

Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN призначена для для керування віддаленим доступом ПК із використанням автентифікації, авторизації, шифрування, моніторингу та звітності.

До складу системи повинні входити як апаратна складова, так і програмна.

Доцільність створення системи зумовлена тим, що при під’єднаннях SSH, RDP та VPN необхідно забезпечити безпеку при передачі даних та доступу до систем. У таких випадках необхідно використовувати різні методи контролю віддаленого доступу, які забезпечать безпеку під час передачі даних та доступу.

2.2 Мета створення системи

Основна метою є змоделювати систему контролю віддаленого доступу при під’єднаннях SSH, RDP і VPN.

Для того, щоб досягти поставленої мети роботи, необхідно розв’язати наступні задачі:

– описати теоретичні засади віддаленого доступу;

– провести порівняльний аналіз протоколів та технологій SSH, RDP та VPN;

– спроектувати систему віддаленого доступу;

– змоделювати її архітектуру;

– побудувати фізичну та логічну моделі віддаленого доступу;

– реалізувати систему віддаленого доступу.

2.3 Характеристика системи

2.3.1 Основні задачі та функції системи

Передбачається розробити спеціалізовану систему віддаленого адміністрування із урахуванням безпеки, гарантуючи, що всі з'єднання зашифровані, автентифікація надійна, а політики контролю доступу є суворими. Ризик несанкціонованого доступу (НСД) або витоку даних може бути зведений до мінімуму, а система може працювати безперебійно та ефективно.

Основні функції, що вимагають реалізації в системі віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN:

– визначення рівня доступу, який може бути надано віддаленим користувачам;

– створення політики віддаленого доступу, що визначає права та обов'язки віддалених користувачів;

– налаштування для застосування політики під час під’єднання віддалених користувачів;

– відстеження активності віддаленого доступу, щоб бачити будь-який НСД або незвичайну активність;

– регулярна перевірка та оновлення політики та параметрів за потреби.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Система повинна бути спроектована так, щоб до її складу особливих зусиль можна інтегрувати різні елементи, не порушуючи при цьому структуру системи.

У проектованій системі повинні бути забезпечені:

– можливість застосування мережевої інфраструктури;

– можливість оцінювання ефективності використання комп'ютерних мереж;

– використання консолі управління: для керування системою, в т.ч. налаштування параметрів та моніторингу продуктивності;

– продуктивність роботи програмного забезпечення;
– часова ефективність та ефективність використання ресурсів системи.

3.1.1 Вимоги до структури та функціонування системи

До структури та функціонування система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN входять:

– ПК
– комп’ютерна мережа;
– сервер;
– брандмауер;
– маршрутизатор / комутатор.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Протокол SSH за замовчуванням використовує 22-й порт TCP. За замовчуванням RDP використовує TCP-порт 3389. При використанні технології SSL VPN з'єднання відбувається за протоколом HTTPS через 443 порт.

Для підвищення безпеки та захисту від автоматизованих атак адміністратор може змінити ці стандартні порти на інший у файлах конфігурації.

3.1.3 Вимоги по діагностуванню системи

Діагностика системи віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN відбувається у відповідності до затвердженого розкладу профілактичних заходів.

3.1.4 Перспективи розвитку, модернізація системи

Перспективами розвитку та модернізації розроблюваної системи є розширення функціонального наповнення.

3.1.5 Вимоги до надійності системи

Система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN повинна бути захищена на транспортному рівні моделі OSI.

Фізичний рівень захисту повинен забезпечувати надійність щодо доступу до апаратного забезпечення. Програмний рівень захисту повинен передбачати захист від сторонніх втручань і впливів.

3.1.6 Вимоги до функцій та задач, які виконує система

Функціональні вимоги та задачі, які повинна реалізовувати система віддаленого адміністрування комп’ютеризованого робочого місця з захищеним доступом на основі з’єднань SSH, RDP та VPN полягають в наступному:

- багатофакторна автентифікація та авторизація.
- контроль доступу до системи на основі ролей та дозволів користувачів;
- забезпечувати безпечну передачу даних, запобігати витоку даних або НСД, а також підтримувати високошвидкісні з'єднання для мінімізації затримки;
- відстеження дій користувачів, продуктивності системи та подій безпеки із формуванням звітів, оповіщень та повідомлень, щоб попереджати системних адміністраторів про будь-які проблеми чи потенційні загрози;
- забезпечення зручності використання програмної частини.

3.1.7 Вимоги до апаратного забезпечення

- клієнтський комп’ютер;
- сервер;
- пристрій мережевої безпеки (брандмауер);
- мережеві комутатори та маршрутизатори.

3.1.8 Вимоги до програмного забезпечення

- PuTTY;
- AnyDesk;
- freeSSHd;
- SSL VPN Plus.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

1 Принцип роботи SSH_RDP_VPN.

2 Логічна модель даних системи.

3 Скріншоти вікон налаштування сервера

4 Скріншоти вікон реалізація віддаленого доступу до АРМ.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Техніко-економічні показники

Планована собівартість системи віддаленого адміністрування комп'ютеризованого робочого місця з захищеним доступом на основі з'єднань SSH, RDP та VPN повинна становити не більше 3 000 грн.

*Примітка: собівартість системи може змінюватись під час розрахунку в процесі розробки.

6 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Розробка технічного завдання	26.01 – 02.02	Виконано
2.	Підбір джерел про системи віддаленого керування із захищеним доступом		
	(на основі SSH, RDP та VPN)	03.02 – 06.04	Виконано
3.	Опрацювання літературних джерел	05.04 – 10.05	Виконано
4.	Виконання дослідження щодо моделювання		
	системи віддаленого адміністрування		

	комп’ютеризованого робочого місця з		
	захищеним доступом	11.05 – 13.05	Виконано
5.	Втілення практичної складової в частині		
	реалізації системи	14.05 – 18.05	Виконано
6.	Оформлення розділу «Аналіз технічного		
	завдання»	19.05 – 22.05	Виконано
7.	Оформлення розділу «Проектна частина»	23.05 – 26.05	Виконано
8.	Оформлення розділу «Практична частина»	27.05 – 28.05	Виконано
9.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи охорони праці»	26.05 – 30.05	Виконано
10.	Оформлення пояснювальної записки і		
	графічного матеріалу	01.06 – 03.06	Виконано
11.	Перевірка на академічний плагіат, перевірка		
	керівником та консультантами	04.06 – 09.06	Виконано
12.	Попередній захист кваліфікаційної роботи		
	бакалавра	11.06 – 17.06	Виконано
13.	Захист кваліфікаційної роботи	26.06	

7 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.