НАЦІОНАЛЬНИ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

ШТІЛЬМАН Павло Романович

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ДОСТУПУ ДО ВІДДАЛЕНОЇ ЛАБОРАТОРІЇ

Спеціальність 123 – Комп`ютерна інженерія

Спеціалізація – Комп'ютерні системи та мережі

Керівник: Шапорін Володимир Олегович,
кандидат технічних наук, доцент

Одеса – 2021

АНОТАЦІЯ

Штільман П.Р. Дослідження технології доступу до віддаленої лабораторії – Магістерська дипломна робота. Одеса, 2021: 65с. , 24 рис., 10 джерел.

Об'єкт дослідження – Існуюча лабораторія автоматизації.

Предмет дослідження – Технології доступу до віддаленої лабораторії.

Мета роботи - проведення дослідження технологій віддаленого доступу, для отримання даних, які дозволять виконати складання рекомендації стосовно використанню існуючих рішень віддаленого доступу до лабораторії. Це є необхідним для організації можливості студентам отримувати практичні навики праці з існуючим обладнанням та створення можливості виконувати роботу на лабораторному обладнані, на будь-якій машині та у зручному для студента місці, якщо виконання роботи при особистій присутності у лабораторії не є можливою.

У роботі був проведений аналіз існуючих рішень. Також було проведено моделювання підключення цих рішень з ціллю максимального наближення умов роботи існуючої лабораторії та отримання характеристик цих рішень при роботі в цих умовах для створення рекомендації щодо використання технології віддаленого доступу.

Також була проведена оцінка рішення, у якій було наглядно показано переваги лабораторії із віддаленим доступом над звичайною лабораторією, стосовно надання можливості студентам заробити якомога більше практичного досвіду.

ТЕХНОЛОГІЇ ВІДДАЛЕНОГО ДОСТУПУ, ЗАХВАТ ЗОБРАЖЕННЯ, ВІРТУАЛЬНА СЕСІЯ, ВІДДАЛЕНА СЕСІЯ ПІДКЛЮЧЕННЯ, ЗАХИЩЕНИЙ КАНАЛ ЗВ’ЯЗКУ.

ANNOTATIOM

Shtilman P.R. Research of remote laboratory access technology - Master's thesis. Odessa, 2021: 65p., 24 figs., 10 sources.

Object of research - Existing automation laboratory.

Subject of research - Technologies of access to a remote laboratory.

The purpose of the work - is to conduct a study of remote access technologies to obtain data that will make recommendations for the use of existing remote access solutions to the laboratory. This is necessary to enable students to gain practical skills with existing equipment and create opportunities to work on laboratory equipment, on any machine and in a convenient place for students, if the work in person in the laboratory is not possible.

The analysis of existing solutions was carried out in the work. It was also simulated to connect these solutions in order to approximate the operating conditions of the existing laboratory and obtain the characteristics of these solutions when working in these conditions to create a recommendation for the use of remote access technology.

An evaluation of the solution was also carried out, which clearly demonstrated the advantages of a remote access laboratory over a conventional laboratory in terms of enabling students to gain as much practical experience as possible.

REMOTE ACCESS TECHNOLOGIES, IMAGE CAPTURE, VIRTUAL SESSION, REMOTE CONNECTION SESSION, SECURED COMMUNICATION CHANNEL.

ЗМІСТ

Вступ 3
1 Тематичний огляд 7
1.1 Загальні відомості 7
1.2 Перелік існуючого обладнання лабораторії 11
1.3 Перелік існуючих технологій 13
1.4 Порівняння існуючих рішень 18
1.5 Висновок до розділу 1 20
2 Завдання на дослідження 22
2.1 Мета роботи 22
2.2 Завдання на дослідження 23
2.3 Вимоги до існуючих рішень 23
2.4 Вхідні та вихідні дані 24
2.5 Висновки до розділу 2 25
3 Дослідження технологій віддаленого доступу 26
3.1 Дослідження технологій віддаленого доступу 26
3.2 Модель підключення до віддаленої лабораторії 39
3.3 Моделі мережі віддаленої лабораторії 41
3.4 Висновки до розділу 3 49
4 Рекомендація щодо технології доступу до існуючої лабораторії 50
4.1 Розбір технологій віддаленого доступу на існуючій лабораторії 50
4.2 Методи підключення до віддаленої лабораторії 55
4.3 Кроки обробки запитів 59
4.4 Оцінка рішення 60
4.5 Висновок до розділу 4 62
Загальні висновки 63
Перелік джерел посилань 65

ВСТУП

У період значного розвитку мережевих технологій, доступ до віддаленої лабораторії є надзвичайно важливим інструментом для здобуття професійних практичних навичок вдома.

Віддалений робочій стіл пропонує студентам простий та зручний спосіб виконувати лабораторні та практичні заняття, використовуючи свій персональний пристрій для керування віддаленим середовищем.

Сервер віддаленого робочого столу дозволяє користувачам навчатися з будь-якого місця, будь-то вдома, в дорозі чи на роботі. Фізичне підключення до мережі не потрібне. Для підключення віддаленого користувача до серверу не потрібно додаткового обладнання. Все, що потрібне – це доступ до Інтернету та веб-браузер.

Таке рішення може спокійно підійти до сфери освіти, у якій хочуть зменшити капітальні витрати на обладнання та інше. Також це ідеально підходить університетам, студенти яких працюють вдома, або не мають можливості бути присутнім фізично у вищому навчальному закладі. Але це відноситься не тільки до студентів. Викладачі також мають свої значні переваги при використанні віддаленого робочого столу.

Віддалені настільні комп’ютери є цінним інструментом для освіти. Це економічно, ефективно, підвищує продуктивність і надає студентам ті самі практичні навички, які їм потрібні.

Основними інструментами реалізації лабораторії із віддаленим доступом є технології віддаленого доступу. Ці технології можуть розрізнятися по принципам їх роботи, так і тим, для чого їх планують застосовувати. Через що вони по різному можуть відповідати вимогам, які можуть бути висунуті про складанні рекомендації щодо технології віддаленого доступу до існуючої лабораторії.

Через це можливо зробити висновок, що об’єктом дослідження даної кваліфікаційної роботи є існуюча лабораторія автоматизації. Предметом дослідження виступають технології віддаленого доступу.

Метою даної роботи є проведення дослідження технологій віддаленого доступу, для отримання даних, які дозволять виконати складання рекомендації стосовно використанню існуючих рішень віддаленого доступу до лабораторії. Це є необхідним для організації можливості студентам отримувати практичні навики праці з існуючим обладнанням та створення можливості виконувати роботу на лабораторному обладнані, на будь-якій машині та у зручному для студента місці, якщо виконання роботи при особистій присутності у лабораторії не є можливою.

Завданнями даної роботи є:

- Проведення аналізу існуючих технологій віддаленого доступу та рішень які побудовані на їх основі. Виявлення переваг та недоліків цих рішень.
- Виконати порівняння існуючих рішень між собою, задля виявлення необхідних характеристик для створіння майбутнього рішення на їх основі, або складанню рекомендації щодо використанню існуючих рішень технології віддаленого доступу до лабораторії.
- Створення моделей мережі та проведення теоретичних досліджень на їх основі. Задля виявлення особливостей використання кожного із проаналізованих технологій та виявлення більш придатного рішення до його майбутнього використання у лабораторії із віддаленим доступом.

У якості вихідних даних виступають:

- Дані необхідні для складання рекомендації стосовно використанню технологій віддаленого доступу
- Вимоги до майбутнього рішення віддаленого доступу до лабораторії

В першому розділі був проведений аналіз існуючих рішень та проведення порівняння між цими рішеннями.

- Були виділені 4 основних категорії технологій віддаленого доступу до існуючої лабораторії:
- Технології віддаленої сесії.

- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Була створена модель підключення існуючої лабораторії.

При більш детальному порівнянню цих технологій було висунуто ряд вимог до системи, які дозволяють організувати віддалений доступ до існуючої лабораторії:

- Безпека зв’язку.
- Кросплатформеність.
- Рівень передачі інформації між віддаленими абонентами.
- Рівень налаштування обмежень.
- Автономність.
- Інформованість.
- Можливість організації роботи у групах.
- Вимогу до потужності.

У третьому розділі було проведено детальне дослідження технологій віддаленого доступу, які у майбутньому можуть бути застосовані при складанні рекомендації щодо організації лабораторії із віддаленим доступом.

Були розглянуті наступні моделі підключення до віддаленої лабораторії:

- Підключення від віддаленого абонента до локальної робочої станції.
- Пряме підключення від віддаленого абонента до локального обладнання.
- Підключення від віддаленого абонента до віртуального робочого столу.
- Підключення від віддаленого абонента до локальної робочої станції по WEB інтерфейсу.
- Підключення від віддаленого абонента до локального обладнання по WEB інтерфейсу.

Усі ці моделі були створені при максимально наближенні до реальної лабораторії із віддаленим доступом моделі підключення. Завдяки цьому отримані

дані, які в майбутньому допоможуть розробити пропозицію організації лабораторії із віддаленим доступом.

У четвертому розділі була проведена робота по складанню рекомендації щодо технології доступу до існуючої лабораторії. В ході її складання були виділені три технічних рішення, які розрізнялися між собою принципами роботи:

- Remote desktop services (RDS).
- Virtual private Network (VPN).
- Virtual desktop infrastructure (VDI).

Після проведення порівняння цих рішень із вимогами, які висувалися у зв’язку з особливістю технічного оснащення лабораторії, вибір для подальшого використання в складенні рекомендації пав на RDS.

Був розібраний сценарій процесу підключення та наступного виконання віддаленого управління при використанні RDS. Крім цього була проведена оцінка рішення, у якій було наглядно показано переваги лабораторії із віддаленим доступом над звичайною лабораторією, стосовно надання можливості студентам заробити якомога більше практичного досвіду.

1 ТЕМАТИЧНИЙ ОГЛЯД

1.1 Загальні відомості

На сьогоднішній момент, у період глобальної цифровізація та розвитку засобів зв’язку/інтернету назріває питання про надання учбової інформації у режимі онлайн, тоді коли це може буди зручно для студентів, які не можуть бути присутні в університеті з різних причин. І йдеться не лише про лекційний матеріал, але і про надання можливості отримати практичні навички, особисто річ ідеться про навички роботи з обладнанням, яке знаходиться у лабораторіях. Вирішення подібної проблеми можливо декількома шляхами:

- Створення програм, які будуть моделювати роботу лабораторного обладнання.
- Використання технологій, які дозволять утворити зв’язок між обладнанням, яке знаходиться у лабораторії та пристроями студентів.

Перше категорія представляє собою рішення у вигляді симуляторів. Вони можуть гарно замінити станки чи стенди на яких проводяться практичні дослідження. Для цих цілей можливо спокійно використовувати програмуємо логічний контролер. Але коли питання доходить до надання можливості набивати практичні навички саме із цим обладнанням одними симуляторами проблему не вирішити. Через що потрібно прибігати до інших рішень.

До другої категорії можливо сміливо віднести технології віддаленого доступу. Вони дозволяють користувачам отримати доступ до мережи, а також пристроїв які знаходяться в неї, сама мережа до якої ми підключаємося знаходиться у місці фізичної недосяжності.

Якщо порівнювати симулятори та технології віддаленого доступу, можливо зробити висновки, перші дуже складні у реалізації та потребують багато часу на розробку. Другі насамперед мають ряд переваг:

- Студент будь де та будь коли має можливість підключитися до реального обладнання.
- Окрім навичок праці з реальним обладнанням студент має можливість отримати навички праці з мережею.

Технології віддаленого доступу можливо поділити за типами:

- Технології віддаленої сесії.
- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Для розуміння різниці між кожним типом , роз’яснимо кожну з них та почнемо з технологій віртуальної сесії. Цей тип дозволяє виконувати віддалене підключення між сервером та клієнтом, управління виконується за допомогою відправки команд від клієнта до сервера. Таким чином є можливість використання не тільки програмного забезпечення, яке встановлене на сервер, а і використання обладнання підключеного зі сторони сервера на програмному забезпечені клієнта. Дуже часто технології даного типу не мають своєї системи захисту зв’язку та даних, через що треба про це подбати. Схема роботи подібних технології наведена нижче, на рисунку 1.1:

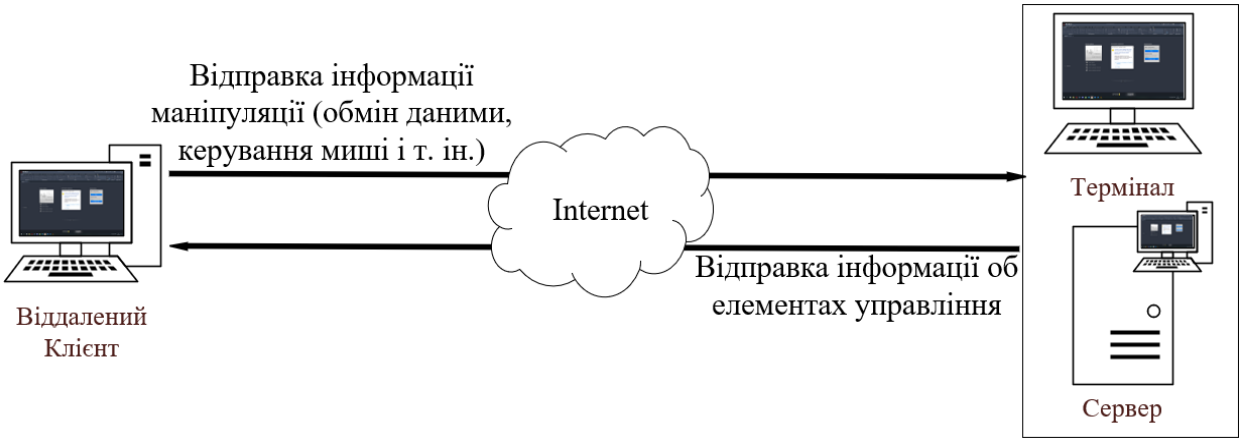

Рисунок 1.1 - Схема роботи технологій віддаленої сесії

Наступними до розглядання є технології захвату зображення. Зміст та принцип роботи такого типу технологій можливо зрозуміти із назви, воно захоплює

зображення, яке відображається на хості, транслює його на клієнті та надає можливості управління. Нижче, на рисунку 1.2 зазначена схема роботи такого типу технології віддаленого доступу:

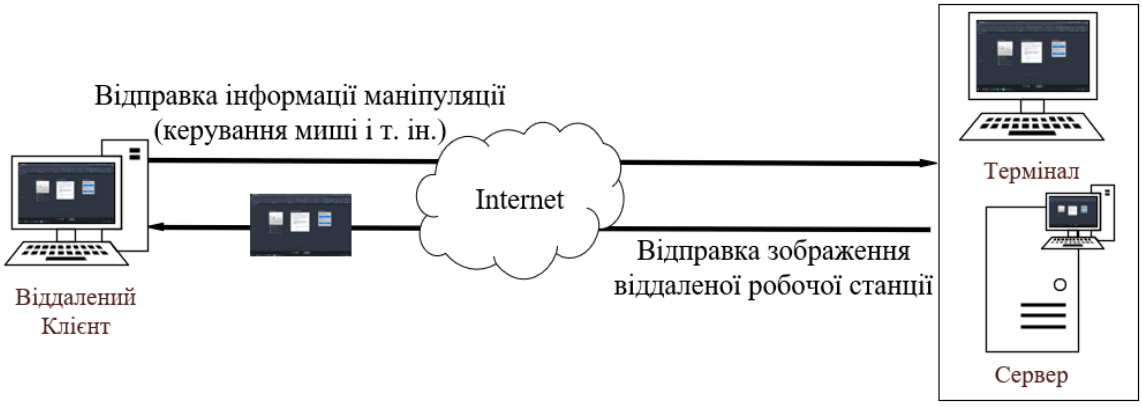

Рисунок 1.2 - Схема роботи технології захвату зображення

Через принцип роботи таких технологій, різницею цього типу від попереднього є можливість маніпулювати виключно програмним забезпеченням яке встановлено на сервері. Також через це такі рішення не дозволяють виконувати передачу ваших файлів для виконання практичних, все потрібно буде збирати спочатку на віддаленому пристрої. Цей тип технологій є доволі простим у використанні, але потребує великі потужності самого сервера. Також, дуже часто технології цього тупи не створюють безпечного з’єднання між сервером та клієнтом, через що треба окремо подбати.

Іншим представником віддаленого доступу є технології віртуальної сесії. Згідно із назви користувач підключається до сервера та виконує роботу на віртуальній машині. Рішення такого типу дуже легко масштабуються, через те, що уся екосистема знаходиться на сервері. Це дозволяє вирішити проблему із кількістю систем до яких студенти мають можливість підключитися. Але хоч таке рішення і не потребує великий парк систем з якими ми організуємо зв’язок, вона потребує великої потужності від самого сервера, через то що від нього залежить скільки систем ми зможемо одночасно підключити. Нижче, на рисунку 1.3 зазначена схема роботи технології віртуальної сесії:

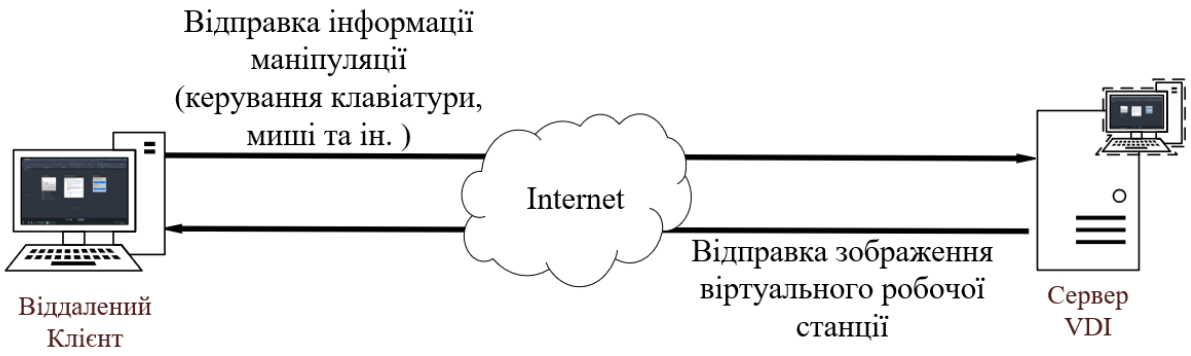

Рисунок 1.3 – Схема роботи технології віддаленої сесії

Останнім типом є технології віддаленого об’єднання у мережи. Технології цього типу дозволяють створити об’єднану мережи із комп’ютерів які знаходяться у різних куточках місцевості (будівель, міст, країн і т.д.). Для створення подібного зв’язку можливо як використання програмного забезпечення так і за допомогою спеціалізованих апаратних рішень. Плюсом використання такого типу технологій є створення окремого безпечного каналу зв’язку. Виконується це шляхом шифрування даних які йдуть до передачі даних. Також надається доступ до спільного використання обладнання підключеного у мережу між комп’ютерами самої мережи.

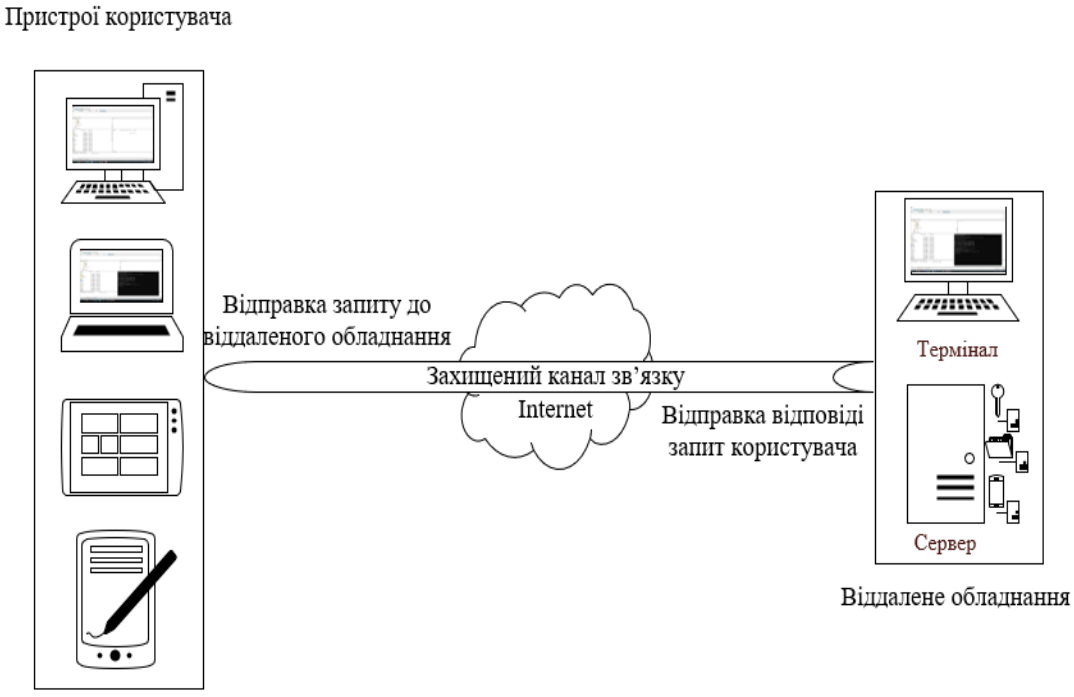

Рисунок 1.4 – Схема роботи віддаленого об’єднання у мережу

Але різницею технологій цього типу, від попередніх двох типів є те, що немає можливості напряму керувати віддаленим комп’ютером, тобто за допомогою графічного інтерфейсу, лише виконувати адміністративне управління за допомогою командної строки. Але ключовим моментом технологій цього типу є те, що їх використання можливо разом із двома попередніми для створення безпечного каналу зв’язку.

1.2 Перелік існуючого обладнання лабораторії

Спочатку, перед розгляданням існуючих технологій віддаленого доступу, потрібно роз`яснити яке лабораторне обладнання використовується та модель підключення даної лабораторії.

На сьогоднішній період часу лабораторія складається із наступного обладнання:

- Сервер DHCP, який використовується для генерації IP адресів усього обладнання лабораторії.
- Routing сервер, для коректної маршрутизації між обладнанням лабораторії.
- Сервер системи керування бази даних (СКБД) лабораторії, використовується для зберігання потрібної інформації, яка необхідна студентам для виконання практичних задач.
- Головний маршрутизатор лабораторії D-Link DIR-620, використовується для зв’язку лабораторії із зовнішнім світом.
- Головний комутатор на 24 портів FastEthernet (FE).
- Периферійні комутатори на 24 порта та на 16 портів.
- Комплекти програмованих логічних контролерів. До цього комплекту входить контролер з підтримкою інтерфейсу Ethernet, у кількості 15 штук. На боту модуль має вбудований блок живлення для всього комплекту, 8 цифрових входів і 4 цифрових виходів, які можливо використовувати для програмування. Іншою частиною комплекту є додатковий модуль, який складається з 2 аналогових входів.

Також додатково є два модуля для виконання управління - модуль потенціометра та інтерфейсний модуль на 8 входів.

- Персональні комп'ютери на яких встановлені 2 операційні системи – Windows 10 та Linux Ubuntu, у кількості 15 штук. Окрім цього на кожній машині встановлено усе програмне забезпечення необхідне для виконання лабораторних робіт та накопичення практичних навичок.

Модель з'єднання усього переліченого вище лабораторне обладнання наведено нижче, на рисунку 1.4:

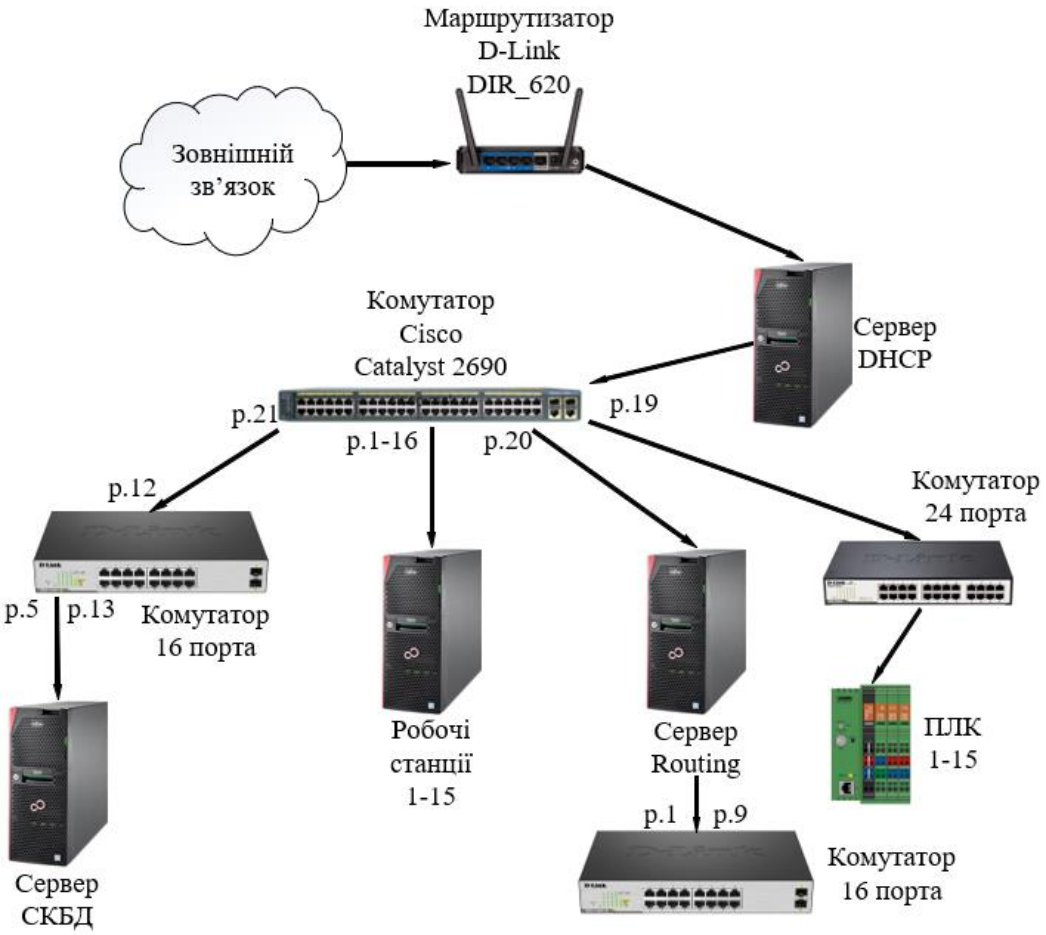

Рисунок 1.4 – Модель з'єднання лабораторного обладнання

Як ми бачимо на малюнку 1.1 зазначено модель підключення лабораторного обладнання між собою. Виконується вона таким чином:

- Мережевий кабель з кафедри (Зовнішній зв'язок) надходить до головного маршрутизатору лабораторії, D-Link DIR-620.

- Наступним кроком є з’єднання маршрутизатора разом із сервером DHCP, призначеного для генерації IP адресів лабораторному обладнанню.
- Далі DHCP сервер з’єднується з головним комутатором, патч-корд від DHCP сервера надходить до 19 порта комутатора. Комутатор в свою чергу виконує функцію розгалужувача між усім лабораторним обладнанням.
- Головний комутатор з 1 по 16 порти з’єднується з робочими станціями лабораторії. Порти 17 та 18 є вільними. Порт 19 з’єднується з комутатором на 24 порти. 20 порт з’єднаний з сервером Routing. Патч корд із 21 порта надходить до 12 порта іншого комутатора на 16 портів.
- Комутатор на 24 порти з’єднаний з ПЛК за допомогою портів з 1 по 15.
- Сервер routing необхідний для організації маршрутизації між лабораторним обладнанням з’єднується з 1 комутатором на 16 портів та займає до 1 і 9 порти.
- Другий комутатор на 16 портів з’єднаний з сервером СКБД лабораторії за допомогою 5 та 13 портів. Сервер СКБД необхідний для зберігання усієї інформації, яка може буди необхідна студентам для виконання лабораторних робіт.

1.3 Перелік існуючих технологій

Існує велика кількість різноманітних протоколів та додатків які, використовуються для створення віддаленого з’єднання. В ході проведення аналізу можливо зазначити наступні технології, а також їх переваги та недоліки:

Windows Remote Desktop Protocol (RDP) – цей протокол дозволяє бачити зображення на екрані та користуватися повноцінним функціоналом іншого віддаленого комп’ютера до якого ми підключаємося. Для виконання цього потрібно два компонента, RDP сервер та RDP клієнт. Перший є машиною або сервером до якого ми підключаємося та хочемо їм керувати. Другий це комп’ютер або інший пристрій через який ми і виконуємо особисте управління. Дане рішення можливо віднести до першого тупи технологій віддаленого доступу – технології віртуальної сесії. Перевагами даної технології можливо зазначити:

- Відсутність необхідності встановлювати окреме програмне забезпечення як на сервер так і на клієнт, якщо обидва працюють на операційній системі Windows.
- Надійність сесії підключення, у випадку розриву зв’язку на короткий термін, декілька секунд, протокол буде продовжувати відновлювання сесії.
- Можливість виконання з’єднання без необхідності підтвердження зі сторони “хоста”, використовуючи пароль, а також ім’я комп’ютера до якого виконується з’єднання.

Недоліками цього рішення є наступні:

- Необхідність налаштування зачиненої сесії у цілях безпеки з’єднання за допомогою окремих програмних або апаратних рішень, через відсутність вбудованих.
- Можливо приєднатися тільки до комп’ютерів під управлінням Windows.
- Відсутність налаштування тривалості сесії.

Іншим представником технології віддаленого доступу є Virtual Network Computing (VNC). Заснована на протоколі Remote Framebuffer Protocol (RFB) та розробляється з 90-х років. Ця технологія, як і в випадку з RDP, забезпечує віддалене керування комп’ютером. Усі пристрої, які підключенні до віддаленого комп’ютера, такі як прінтери та інші також доступними. На сьогодні використовуються для віддаленого доступу від комп’ютера який знаходиться вдома до віддаленої машини в університеті/офісі. Принцип роботи VNC полягає у відправці зображення, яке відображено на віддаленому комп’ютеру, за винятком того, що дозволяє виконувати операції на ньому. Це дозволяє віднести це рішення до другого типу технологій віддаленого доступу – технології захвату зображення. Його перевагами є:

- VNC є кросплатформеним рішенням. Іншими словами, це дозволяє приєднатися з комп’ютера на одній платформі до іншої, головне щоб був клієнт який дозволить це зробити.

Недоліками в свою чергу є:

- Через принципи роботи технології відсутня можливість відправки даних до віддаленого комп’ютера.
- Можлива робота тільки з програмним забезпеченням який знаходиться на хості, через принципи роботи VNC.
- Необхідно подбати про захист інформації через відсутність вбудованої системи захисту та шифрування даних.

Apple Remote Desktop (ARD) –програмне забезпечення для створення віддаленого робочого столу за допомогою пристроїв із екосистеми Apple. Дозволяє віддалено керувати як комп’ютерами на MacOS так і телефонами/планшетами на iOS. Дане рішення можливо віднести до першого типу технологій віддаленого доступу – технології віртуальної сесії Має при собі великий спектр налаштувань для моніторингу інформації про підключення до пристрою. Системи захисту від несанкціонованих підключень та захисту даних З його переваг можливо виділити:

- Захист підключення до віддаленого робочого стола за допомогою двох різних методів аутентифікації.
- Можливість створення списку пристрої, до яких потрібно виконати віддалений зв'язок.
- Ідентифікація у реальному часі до яких пристроїв є можливість підключитися, що дозволяє студентам відразу отримувати інформацію о вільних пристроях.
- Дозволяє переглядати дії віддаленого користувача, відправляти йому повідомлення, а також взаємодіяти разом із ними.
- Дозволяє віддалено встановлювати програмне забезпечення та виконувати налаштування відразу на декількох машин.

До недоліків можливо віднести:

- Відсутність управління тривалістю підключення.

Secure Shell (SSH) – широко реалізований універсальний протокол. Його структура та функціонал безпеки дає можливість використовувати різними способами, для віддаленого доступу, переадресації портів, тунелювання та

безпечної передачі файлів. Однією з найпоширеніших програм, яка використовує протокол SSH – PuTTY. До переваг даного рішення можливо віднести наступне:

- Програмне забезпечення, що підтримує протокол SSH присутнє майже на кожній операційній системі, а на MacOS та Linux є свої вбудовані рішення, які його підтримають.
- Дуже розвинута система шифрування та захисту мережи від несанкціонованих підключень.

Недоліками цього рішення є:

- Через відсутність графічного інтерфейсу, управління віддаленим пристроєм можливе лише за допомогою командної строки.
- Управління складними програмами, які установлені на віддаленому комп'ютері не є можливим. Через що користувачу потрібно встановлювати потрібні для роботи програми на свій комп'ютер.

Іншою технологією, яка дозволяє безпечно отримати доступ до віддаленого обладнання це віртуальна приватна мережа (VPN). VPN дає можливість встановлювати захищений мережевий зв`язок під час використання загальнодоступних мереж. VPN є гарним доповненням до інших технологій даної категорії, з точки зору організації безпеки. Організувати VPN зв`язок можливо як за допомогою програмних так і апаратних рішень. До переваг VPN можливо віднести:

- Згідно назви цієї технології між сервером та користувачем організовується окрема приватну "локальну" мережа, яка є захищена від несанкціонованих підключень.
- Шифрування даних відбувається у режимі реального часу.

Окремим прикладом рішення у вигляді додатку Splashtop. Пропрієтарне програмне забезпечення, яка в свою чергу втратила недоліки, які є у RDP. Перевагами такого рішення є:

- Дозволяє виконувати налаштування тривалість сесії підключення до лабораторного обладнання, для її запобігання багатогодинної експлуатації однією людиною.

- Дозволяє зробити захищену сесію підключення, через використання вбудованого рішення заснованого на VPN.
- Дозволяє декільком користувачам приєднуватися до одного комп’ютера, що дозволяє викладачам відразу перевіряти роботи студентів, або іншим студентам виконувати практичні заняття разом.
- Завдяки кросплатформеності є можливість отримувати доступ до комп’ютерів з операційною системою Windows, Mac або Linux з будь-якого пристрою на який можливо поставити програмне забезпечення.
- Гнучке та просте налаштування.

Наступний приклад технології, що реалізує віддалений робочий стіл є додаток від Google, Google remote desktop (GRD). Дуже простий у налаштуванні. Для праці на хості, до якого виконується підключення, а також комп’ютері студента повинен бути встановлений браузер Google Chrome, до якого і встановлюється розширення GRD. Перевагами цього рішення є наступне:

- Підтримка усіх доступних операційних систем, завдяки праці через браузер.
- Простота у використанні, налаштування даного рішення виконується в декілька натискань на клавіатурі.
- Можливість підключення через використання протоколу SSH.

До недоліків можливо зазначити наступні пункти:

- Неможлива робота у цілодобовому режимі, потрібно постійно підтверджувати підключення зі сторони хоста.
- Відсутня можливість налаштування тривалості сесії, клієнт може працювати з віддаленим комп’ютером поки він сам не вийде із сесії, або хост його не відключить.

Наступним прикладом технології віддаленого доступу є Virtual Desktop Infrastructure (VDI) - технології віртуального робочого столу. Технології такого типу працюють за рахунок створення на сервері необхідної кількості віртуальних робочих місць, які можливо налаштувати до роботи з конкретним обладнанням. В свою чергу користувач приєднується до робочого столу через веб-інтерфейс.

Одним з прикладів реалізації такої технології є екосистема, яка розроблена компанією VMware – Horizon. До переваг такої технології можливо віднести:

- Дозволяє гнучко та індивідуально налаштовувати робочу середу, під конкретні потреби лабораторій.
- Відсутність потреби студента встановлювати будь-які робочі програми, уся праця виконується за допомогою браузера.
- Дозволяє заощадити на кількості робочих машин, завдяки праця у віртуальному просторі.
- Є можливість переглядати дії студентів шляхом підключення до їх віртуальної сесії, та в необхідних випадках допомагати їм.
- Дозволяє зробити налаштування тривалості роботи сесії.

Недоліками такої технології є:

- Потребує створення цілої системи із декількох серверів, через великі потреби у розрахунковій потужності.
- Необхідно окремо подбати про створення окремого захищеного каналу зв’язку та шифрування даних користувачів.

1.4 Порівняння існуючих рішень

Кожне з розглянутих вище рішень має свої особливості у роботі, переваги та недоліки. Для отримання більшого розуміння того, яке програмне рішення є придатним для створення віддаленої лабораторії, основуючись на розумінні можливостей існуючого обладнання, потрібно виділити ряд ключових рішень, які будуть сприяти функціональності майбутньої дистанційної лабораторії:

- Безпека зв’язку.
- Кросплатформеність.
- Рівень передачі інформації між віддаленими абонентами.
- Рівень налаштування обмежень.
- Автономність.
- Інформованість.

- Можливість організації роботи у групах.
- Вимогу до потужності.

Безпека зв’язку – необхідно організувати з’єднання між користувачем та віддаленим обладнанням, шляхом створення відокремленого каналу зв’язку. Серед наведеного вище програмного забезпечення вбудоване рішення цього ключового моменту були ARD, GRD та Splashtop. VNC та RDP потребують окремого втручання в даному випадку, через відсутність вбудованих рішень. У випадку з VDI, якщо реалізовувати таке рішення самостійно то необхідно передбачити безпечне з’єднання. У випадку отримання такої послуги від комерційних організацій так рішення є передбаченим.

Кросплатформеність – в даному випадку найкращим рішенням є маніпулювання за допомогою web інтерфейсу. Це дозволить студентам виконувати працю з будь якого їх пристрою, так як підключення буде виконуватися за допомогою браузера. Приклад такого рішення продемонстрований у рішенні від Google – GRD.

Рівень передачі інформації між віддаленими абонентами (Клієнт-Хост) – тут розглядається формат передачі даних між абонентами віддаленої лабораторії. У випадку VNC дані передаються у вигляді зображення, тобто технологія виконує захват зображення та транслює його клієнту дозволяє виконувати маніпуляції із ним. Це не є гарним прикладом так як немає можливості взаємодіяти із існуючим обладнанням за допомогою свого персонального пристрою. Цю проблему вирішують RDP, ARD, GRD та Splashtop.

Рівень налаштування обмежень – в даному випадку мається на увазі не тільки обмеження студента в правах доступу на віддаленій машині, але і обмежень за часом роботи із ним, щоб запобігати надмірній експлуатації цього обладнання. RDP, VNC та GRD передбачають лише обмеження на рівні операційної системи, ніяких обмежень по часу підключення налаштувати не можливо. Повний контроль стосовно менеджменту обмежень надає додаток від Splashtop.

Автономність – дане рішення передбачає за собою можливість підключення без підтвердження зі сторони сервере або автоматичне підтвердження шляхом

перевірки даних з сервера. Це необхідно, щоб студент мав можливість підключитися в режимі 24/7. Майже всі наведенні рішення вирішують цю проблему, окрім GRD, в рішенні від Google хост повинен не тільки постій відправляти ключ для підключення, але і підтверджувати запит на підключення.

Інформованість – можливість отримувати інформацію стосовно, який віддалений пристрій зараз використовується чи є вільним дуже прискорить роботу студентів. Єдиний представник серед приведених вище технологій є ARD. Рішення від Apple показує не тільки який пристрій зараз зайнятий і ким, але і дозволяє переглянути повну історію подій даного пристрою у режимі реального часу.

Можливість роботи у групі – до цього рішення відноситься реалізації можливості одночасного маніпулювання однієї машини декільком людям, наприклад студент виконує роботи і викладач має можливість приєднатися до нього, перевірити його роботи чи разом із ним виконувати операції на машині. З усіх наведених рішень такий функціонал має при собі ARD та Splashtop.

Вимоги до потужності – рішення повинне тільки спокійно працювати на будь якому пристрої студентів, але і показувати прийнятні показники продуктивності на лабораторному обладнанні. Для організації стабільної роботи VDI необхідно мати окремий парк із серверів, через особливості самої технології.

1.5 Висновок до розділу 1

В даному розділі ми розглянули різноманітні рішення, які у майбутньому можуть надати можливість реалізувати віддалений доступ до лабораторії і до обладнання у ній. Виділили ключові типи цих технологій технології віддаленого доступу, а саме:

- Технології віддаленої сесії.
- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Кожне з цих рішень має свої особливості та методи у реалізації. Вході короткого розглядання рішень на основі цих технологій та існуючого обладнання у лабораторії були виявлені основні вимогу до системи організації віддаленого доступу до лабораторії.

Також завдяки проведенню аналізу існуючих рішень були висунуті ряд вимог, яким має відповідати майбутнє рішення:

- Безпека зв’язку.
- Кросплатформеність.
- Рівень передачі інформації між віддаленими абонентами.
- Рівень налаштування обмежень.
- Автономність.
- Інформованість.
- Можливість організації роботи у групах.
- Вимогу до потужності.

Рішення яке буде відповідати усім цим вимогам, у майбутньому буде застосовано при складанні рекомендації щодо реалізації технології віддаленого доступу до існуючої лабораторії.

2 ЗАВДАННЯ НА ДОСЛІДЖЕННЯ

У період великого розвитку мережевих технологій, а також необхідності у достатній підготовці професійних спеціалістів, стає питання у наданні не тільки теоретичній підготовці, а і достатньої кількості практичного досвіду роботи із реальним обладнанням. Особливо це питання стає гострим у випадку труднощів із фізичною присутністю студента у вищому навчальному закладі.

Основними інструментами рішення подібного питання є технології віддаленого доступу. Ці технології можуть розрізнятися по принципам їх роботи, так і тим, для чого їх планують застосовувати. Через що вони по різному можуть відповідати вимогам, які можуть бути висунуті про складанні рекомендації щодо технології віддаленого доступу до існуючої лабораторії.

Об’єктом дослідження даної роботи виступає існуюча лабораторія автоматизації.

Предметом дослідження у даному випадку виступає технології віддаленого доступу до існуючої лабораторії.

2.1 Мета роботи

Метою даної роботи є проведення дослідження технологій віддаленого доступу, для отримання даних, які дозволять виконати розробку пропозиції стосовно використанню існуючих рішень віддаленого доступу, або створення пропозиція винаходження свого особистого рішення, із усіма необхідними функціями, для організації дистанційної роботи лабораторії кафедри. Це є необхідним для організації можливості студентам отримувати практичні навики праці з існуючим обладнанням та створення можливості виконувати роботу на

лабораторному обладнані, на будь-якій машині та у зручному для студента місці, якщо виконання роботи при особистій присутності у лабораторії не є можливою.

2.2 Завдання на дослідження

Задля виконання поставленої мети потрібно виконати ряд задач, які перераховані нижче:

- Висування вимог до існуючих рішень для виявлення оптимально необхідних характеристик при проведенні аналізу та створенню майбутніх пропозицій.
- Проведення аналізу існуючих технологій і рішень створених на їх основі, виявлення їх переваг і недоліків.
- Порівняння існуючих рішень між собою, задля виявлення необхідних характеристик майбутнього рішення.
- Створення математичних моделей та проведення теоретичних досліджень на їх основі.
- Основуючись на отриманих даних від аналізу існуючих рішень, математичних моделей та їх теоретичного аналізу, виконати розробка пропозиції організації віддаленої лабораторії за допомогою існуючих рішень або створення особистого рішення організації дистанційного доступу до лабораторного обладнання.

2.3 Вимоги до існуючих рішень

Перед початком опису існуючих рішень потрібно зазначити ряд вимог яким має відповідати майбутня система для створення віддаленого доступу:

- Наявність системи захисту від несанкціонованих підключень, шляхом аутентифікації користувачів.
- Можливість налаштування обмежень для студентів, стосовно прав користування віддаленим обладнанням.

- Рішення повинне мати кросплатформеність, тобто у користувача повинна бути можливість як виконати підключення, так і виконувати операції з віддаленим обладнанням за допомогою того пристрою, який є для нього зручним.
- Організація можливості студентам підключатися до лабораторного обладнання в умовах 24/7.
- Можливість налаштування обмеження часу роботи сесії, одна сесія небільше 30 хвилин, за для запобігання надмірної експлуатації лабораторного обладнання одним студентом.
- Живучість підключеної сесії, система повинна намагатися відновити підключення у випадку несанкціонованого відключення, наприклад при відключенні інтернету зі сторони студента.
- У період робочої сесії дані роботи студента із лабораторним обладнання, у випадку несанкціонованого відключення, має надійно зберігатися до кінця цієї сесії.
- У системі має бути передбачена можливість декільком користувачам підключатися до однієї машини, для надання можливості викладачу допомагати, перевіряти чи вказувати на помилки студенту під час робочої сесії із лабораторнім обладнанням.

2.4 Вхідні та вихідні дані

Вхідними даними для проведення дослідження технологій віддаленого доступу є:

- Технічні характеристики існуючої лабораторії.
- Програмні та апаратні рішення технологій віддаленого доступу.
- Приклади реалізованих лабораторій із віддаленим доступом.

Вихідними даними для дослідження технології віддаленого доступу є:

- Вимоги до майбутнього рішення віддаленого доступу до лабораторії.
- Графіки та таблиці із результатами проведення дослідження існуючих технологій і рішень віддаленого доступу.

2.5 Висновки до розділу 2

В даному розділі були зазначені основні задачі до кваліфікаційної роботи магістра. Завдяки чому була зазначена мета роботи, її актуальність та доцільність її виконання. Також були розглянуті основні вимоги до існуючих рішень в результаті чого було визначено критерії які дозволяють оцінювати існуючі рішення, а саме:

- Безпека зв’язку.
- Кросплатформеність.
- Рівень передачі інформації між віддаленими абонентами.
- Рівень налаштування обмежень.
- Автономність.
- Інформованість.
- Можливість організації роботи у групах.
- Вимогу до потужності.

Був визначений об’єкт дослідження – існуюча лабораторія автоматизації. Також були визначений предмет дослідження – технології віддаленого доступу до віддаленої лабораторії.

3 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ВІДДАЛЕНОГО ДОСТУПУ

В ході виконання аналізу були виявленні 4 різних технології за принципами побудови мережи та їх майбутньої роботи, за допомогою яких можливо створіння доступу до віддаленої лабораторії:

- Технології віддаленої сесії.
- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Для розуміння, яке рішення із вище зазначених є більш продуктивним необхідно провести детальне дослідження цих технологій, а також вирішити задачі з моделювання та проведення розрахунків ефективності створених на їх основі мереж.

3.1 Дослідження технологій віддаленого доступу

Як було зазначено вище, в нас є три технології, які відрізняються за принципами роботи. Та почнемо ми розглядання із технології віддаленої сесії.

3.1.1 Технології віддаленої сесії. Для розглядання такого типу технологій візьмемо найпоширеніший протокол Remote desktop protocol (RDP). Основна функція RDP укладаються у передачі інформації з монітора(пристроїв виводу) від віддаленого сервера до клієнта та інформацію з клавіатури і / або миші (пристроїв вводу) від клієнта до віддаленого сервера. Зв’язок у часі може бути вкрай асиметричним, тобто потік даних від сервера до клієнта значно більший, за потік від клієнта до сервера. Стек протоколу RDP виглядає наступним чином:

<table>
<tr><td colspan="2">RDP</td><td colspan="2"></td></tr>
<tr><td>ENCRYPTION</td><td>T.125 MCS</td><td colspan="2"></td></tr>
<tr><td>T.125 MCS</td><td>x.224</td><td colspan="2"></td></tr>
<tr><td>x.224</td><td>TPKT</td><td colspan="2">FastMode DATA</td></tr>
<tr><td>TPKT</td><td colspan="2">TLS</td><td>ENCRYPTION</td></tr>
<tr><td colspan="4">TCP</td></tr>
</table>

Рисунок 3.1 - Стек протоколу RDP

Складові частини стеку протоколу:

- TPKT – транспортна служба ISO поверх TCP. Дозволяє одноранговим вузлам здійснювати обмін інформаційними блоками.
- X.224 – транспортний протокол, який орієнтований на встановлення з’єднання. Використовується у початковому запиті та відповіді на з’єднання.
- T.125 MCS – служба багатопотокового зв’язку. Дозволяє виконувати обмін даними та керувати декількома каналами.
- RSA RC4 – служба, що відповідає за шифрування з’єднання.

Відправка даних за допомогою стеку RDP за сутністю до моделі OSI для зв’язку. Дані, які підлягають передачі поділяються, скеровуються в канал, шифруються, упаковуються, кадруються і упаковуються перед перечую по мережі до іншої сторони, потім проходять той самий процес у зворотному порядку.

Організація безпеки у RDP ‘протоколі можливо поділити на два типи

- Стандартна організація безпеки - трафік шифрується за допомогою алгоритму шифрування RSA RC4 з використанням випадкових значень клієнта та сервера, які обмінюються під час фази обміну основними параметрами під час ініціалізації з’єднання.
- Посилена організації безпеки - цей тип безпеки дозволяє RDP передавати всі операції безпеки (шифрування/дешифрування, перевірку цілісності тощо) на зовнішній протокол безпеки (TLS, RDPTLS, CredSSP).

Підключення за допомогою RDP протоколу можливо розбити на декілька етапів:

- Ініціація підключення.

- Обмін базовими параметрами.
- Підключення каналу.
- Початок безпеки.
- Безпечний обмін параметрами
- Ліцензування.
- Обмін можливостями.
- Завершення підключення.
- Обмін даними.

Підключення за даними етапами виконується у наступному порядку:

Рисунок 3.2 - Етапи підключення протоколу RDP

Ініціація підключення проводилася зі сторони клієнта за допомогою x.244 з’єднання відправляє PDU запит. Даний пакет зберігає запит на погодження RDP, містить кілька прапорів підключення та протоколів безпеки, які підтримуються зі сторони клієнта. Підтвердження підключення виконується зі сторони сервера за

допомогою x.244 з’єднання підтверджуючим PDU. Даний макет містить відповідь на погодження RDP, який використовується для інформування клієнта об обраним протоколом безпеки, який буде використовуватися протягом усього часу підключення.

Обмін базовими параметрами, на даному етапі обмін проходить між клієнтом та сервером використовуючи MCS Connect Initial PDU та MCS Connect Response PDU. Дані налаштування для клієнту та серверу включають:

- Основні дані – версія RDP, роздільна здатність робочого столу, глибина кольору, інформація про клавіатуру, ім’я хоста, інформація про клієнтське програмне забезпечення.
- Дані безпеки – методи шифрування, розмір ключів сеансу, довільний сервер і сертифікат сервера.
- Дані мережі – інформація про запитані та виділені віртуальні канали. Він містить кількість каналів і масив конкретних віртуальних каналів. Клієнт запитує точний тип каналів у запиті, а сервер надає фактичні ідентифікатори каналів у відповіді.

Підключення каналів. Після встановлення списку віртуальних каналів, які будуть застосовуватися у сесії RDP, настає етап на якому підключається кожний канал індивідуально. Поділяється він наступним образом:

- Запит прямого домену MSC.
- Прикріплений запит користувача MSC – запит ID каналу користувача.
- Прикріплена відповідь користувача MSC – підтвердження ID каналу користувача.
- Запит та підтвердження на приєднання до каналу MSC – клієнт, використовуючи їх ID, почнуть запитувати приєднання до віртуальних каналів, а саме канал користувача, канал вводу-виводу та іншими канали, які узгоджені базовими налаштуваннями. У свою чергу сервер почне підтвердження кожне успішне приєднання до каналу.

Початок безпеки. З цього етапу наступний трафік RDP піддається шифруванню. Клієнт відправляє обмін безпеки PDU, який містить клієнтське

випадкове шифрування із серверним відкритим ключем. Після цього клієнт та сервер використовують випадкове число (із обміну базовими налаштування) для створення ключа шифрування сесії.

Безпечний обмін параметрами. Клієнт відправляє шифровану PDU клієнтської інформації, що містить інформацію про підтримувані типи стиснення, домен користувача, ім’я користувача, пароль, робочий каталог тощо.

Ліцензування. Даний етап зроблений для надання дозволу авторизованим користувачам підключатися до термінального серверу. Це зроблено для підтримки більше двох одночасних підключень.

Обмін можливостями. Сервер надсилає можливості, які він підтримує у PDU активного попиту, а саме 28 типів наборів можливостей. Це може бути загальні (версія ОС, загальне стиснення), введення (тип і функція клавіатури), шрифти, віртуальні канали, растрові кодеки та інші. Після цього сервер може надіслати PDU макету монітора, щоб описати монітори дисплея на сервері. Потім клієнт відповідає PDU активного підтвердження, що містить його власний набір можливостей.

Завершення підключення. Клієнт та Сервер обмінюються кількома типами PDU для завершення організації зв’язку. Усі типи PDU починаються зі сторони клієнта, можуть бути відправлені один за одним без очікування відповіді. До даних PDU відносяться:

- PDU синхронізації – використовується для синхронізації ідентифікаторів користувача між клієнтом та сервером.
- PDU керування (співпраця) – спільне надсилання від клієнта та сервера один одному для вказання спільного контролю на сеансом.
- PDU контролю – клієнт надсилає запит на контроль, сервер його надає.
- Постійний список ключів PDU – клієнт надсилає серверу список ключів, кожен ключ ідентифікує кешований растровий малюнок. Це дозволяє кеш-пам'яті бітового зображення бути постійним (на відміну від обмеження терміном життя з'єднання). Кешування растрового зображення — це механізм, який використовується для зменшення мережевого трафіку, необхідного для передачі графічного виводу від сервера до клієнта.

- PDU списку шрифтів/мапи – містить інформацію про шрифти для сесії RDP.

Обмін даними – після завершення організації зв’язку, загальну частину обміну даних між клієнтом і сервером будуть:

- Вхідні дані (від клієнта до сервера) – містить інформацію о роботі миші та клавіатури та періодичної синхронізації.
- Вихідні дані (від сервера до клієнта) – містить побітову карту сесії користувача на сервері.

Додаткові дані які можуть бути переміщені, до них відноситься інформацію управління зв’язком та віртуальний канал повідомлень.

3.1.2 Технологія захвату зображення. До розглядання даного типу технологій можливо сміливо обрати Remote Framebuffer protocol (RFB). Призначений для віддаленого доступу до незалежних від віконної системи графічних інтерфейсів. Даний протокол дозволяє виконувати маніпуляції із “кінцевої точки” користувача, іншими словами за допомогою засобу для перегляду або RFB клієнта. Цей клієнт складається із монітора, клавіатури та вказівний пристрій (миші) та віддаленої системи, де застосовуються зміни до фреймового буфера, тобто сервера RFB. RFB є протоколом, у якого низькі вимоги до клієнтської сторони, що дуже сильно спрощує його розгортання на різних апаратних платформах. Приклад зв’язку клієнта із сервером проілюстровано на рисунку 3.3:

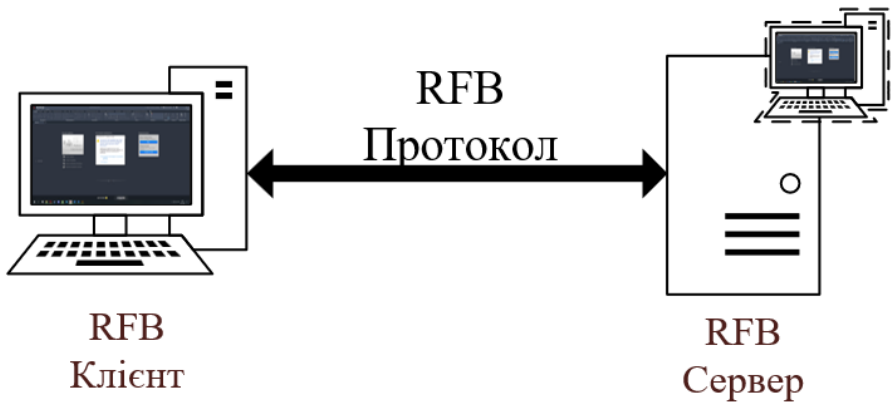

Рисунок 3.3 - Ілюстрація зв`язку RDP клієнт - сервер

Усі зміни в інтерфейсі користувача завжди зберігається на стороні сервера, незалежно від підключення клієнта. Це означає, що клієнт, який відключається та повторно підключається, бачитиме той самий графічний стан, і навіть кілька кінцевих точок клієнта можуть отримати доступ до одного сервера та бачити той самий стан. Це незалежне від розташування властивість рівномірного перегляду є однією з основних переваг протоколу RFB.

Процес з`єднання за допомогою RFB починається з клієнтської сторони. Його можливо поділити на 3 етапи:

- Рукостискання.
- Ініціалізація.
- Нормальна взаємодія протоколу(відправка повідомлень між клієнтом та сервером).

На першому етапі виконується синхронізація клієнта та сервера, визначається версія, тип безпеки, пароль (якщо заданий) та інша інформація, яка буде необхідна на наступному етапі ініціалізації.

На другому етапі клієнт відправляє повідомлення типу ClientInit, у 1 байт не нульового значення для індикації того, що сервер можливо поділити між декількома користувачами та нульове значення, якщо підключення має бути ексклюзивним. Після отримання цього повідомлення сервер до клієнта відправляє своє повідомлення ServerInit. Це повідомлення складається із розмірів буфера кадрів, формату пікселів та імені робочого столу.

На останньому етапі, зі сторони клієнта до сервера надходить 6 повідомлень, а саме:

- SetPixelFormat – встановлює формат пікселів. У випадку коли повідомлення не надсилається, сервер форматує пікселі, як встановлено в ServerInit.
- SetEncoding –
- FramebufferUpdateRequest – нагадає серверу про необхідність оновлення деякої області в буфері кадрів.
- KeyEvent – вказує на натискання на кнопку.

- PointerEvent – вказує на переміщення або натискання на кнопки міші.
- ClientCutText – синхронізація із буфером обміну, нагадає про наявність нової інформації у буфері обміну з клієнтської сторони.

Зі сторони сервера до клієнта надходить 4 види повідомлень, а саме:

- FramebufferUpdate – відповідь на запит на оновлення деякої області в буфері кадрів.
- SetColorMapEntries – надсилається за першим запитом клієнта, якщо в піксельному форматі використовується колірна карта. Усі записи кодуються у 15 бітах для кожного червоного, зеленого та синього кольорів.
- Bell – надсилає звукове повідомлення до клієнта.
- ServerCutText – надсилається коли сервер оновив інформацію у буфері обміну.

Стосовно безпеки, вбудоване рішення протоколу є слабкою, але протокол RFB є гнучким на впровадження та застосування сторонніх рішень, наприклад шифрування каналу з використанням SSH та інших.

3.1.3 Технології віртуальної сесії. До представників такого рішення можливо сміливо віднести Virtual desktop infrastructure (VDI). Дане рішення дозволяє віддалено керувати віртуальними системами. Реалізація цього рішення має за собою налаштування значної апаратної частини. Найчастіше такі рішення будуються за допомогою за допомогою протоколу PCoIP – Personal computer over Internet protocol. Цей протокол дає можливість поширити робочу середу, додатки, зображення та аудіо контент для великого кола користувачів у локальній та глобальній мережі. Протокол має можливість компенсувати збільшення затримки та зменшення пропускної здатності, щоб кінцевий користувач мали достатню працездатність незалежно від стану мережи. Процес створення сенсу за протоколом PCoIP складається із наступних етапів:

- Ініціалізація журналу операцій.
- Обмін даних між клієнтом та сервером. Цей етап потрібен для майбутньої ідентифікації клієнта сервером. Клієнт до сервера відправляє ім’я клієнта, версію програмного забезпечення та його платформу.

- Встановлення адреси та поведінки при неперевіреної сертифікації. Клієнт дізнається адресу сервера до якого намагається підключитися, вказується обробка помилок у випадку коли неможливо перевірити дані сервера.
- Аутентифікація між сервером та клієнтом. На цьому етапі у сервера запитується метод аутентифікації, після чого клієнт відправляє інформацію для її виконання до сервера із використанням цього метода.
- Після успішної аутентифікації, сервер надає клієнту список можливість обрати віртуальну систему.
- Підключення до віртуальної машини. На цьому етапі сервер підключає клієнта до обраної віртуальної машини.

Шифрування даних виконується за допомогою протоколу TLS – Transport Layer Security. Для цього використовується алгоритм обміну ключів RSA. Виконується він наступним чином:

- Ініціація. Клієнт ініціює рукостискання, надсилаючи на сервер повідомлення «привіт». Повідомлення включатиме версію TLS, яку підтримує клієнт, підтримувані набори шифрів, а також рядок випадкових байтів, відомих як «випадковий клієнт».
- Відповідь сервера. У відповідь на привітальне повідомлення клієнта, сервер надсилає повідомлення, що містить сертифікат SSL сервера, вибраний сервером набір шифрів і «випадковий сервер», інший випадковий рядок байтів, згенерований сервером.
- Аутентифікація. Клієнт перевіряє сертифікат SSL сервера в центрі сертифікації, який його видав. Це підтверджує, що сервер є тим, ким він є, і що клієнт взаємодіє з фактичним власником домену.
- Надсилання секретного повідомлення. Клієнт надсилає додатковий набір випадкових чисел. Це повідомлення шифрується відкритим ключем і може буди відкрите тільки приватним ключем сервера.
- Використання приватного ключа. Сервер розшифровує секретне повідомлення.

- Створення сесійного ключа. Обидва клієнт та сервер генерують сесійний ключ із випадкових чисел клієнта, сервера та секретного повідомлення. Обидва мають однаковий результат.
- Готовність клієнта. Клієнт надсилає серверу шифроване сесійним ключем повідомлення про готовність роботи.
- Готовність сервера. Сервер надсилає клієнту шифроване сесійним ключем повідомлення про готовність роботи.
- Завершення рукостискання. Зв’язок організовано та його виконання продовжується за допомогою ключів сеансу.

3.1.4 Технології віддаленого об’єднання у мережу. Яскравим прикладом такого типу технології є протокол Secure Shell (SHH). Це мережевий протокол який дозволяє організувати віддалене та безпечне з’єднання між двома комп’ютерами. SSH шифрує дані, для запобігання несанкціонованого втручання до трафіку між цими пристроями.

Даний протокол складається з 3 рівнів, які зображені на рисунку 3.4:

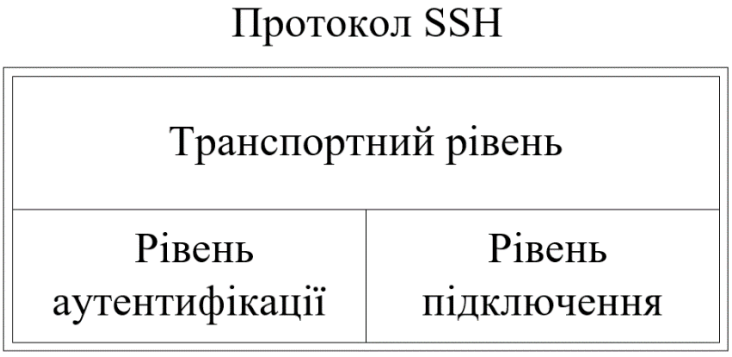

Рисунок 3.4 - Складові частини протоколу SSH

Розберемо кожний з цих рівнів:

- Транспортний рівень – впроваджує безпечний та захищений зв’язок між клієнтом та сервером підчас та після аутентифікації. Цей рівень контролює шифрування та дешифрування і захист цілісності даних. Також він допомагає прискорити обмін даними завдяки забезпеченню стиснення даних і кешування.

- Рівень аутентифікації – дозволяє повідомити клієнта про методи аутентифікації, які підтримуються. Проводить весь процес аутентифікації користувача.
- Рівень підключення – керує зв’язком між клієнтом та сервером після успішно проведеної аутентифікації. Обробляє відкриття та закриття каналів зв’язку, дозволяє використовувати декілька каналів для кількох сеансів.

Підключення. Протокол SSH використовує симетричне шифрування, асиметричне шифрування та хешування, щоб захистити передачу інформації. Зв’язок за допомогою SSH між клієнтом та сервером виконується у три етапи:

- Верифікація сервере клієнтом.
- Генерація ключів сесії для шифрування усього періоду зв’язку.
- Аутентифікація клієнта.

Верифікація сервера починається з ініціації клієнтом сесії зв’язку із сервером. Сервер прослуховує стандартний 22 порт(може бути змінений) для SSH підключення. На даному етапі ідентифікація сервера перевіряється. В ході перевірки може бути два вихідних випадка:

- Якщо клієнт звертається до сервера вперше, у клієнта просять пройти аутентифікацію сервера вручну, перевіривши публічний ключ сервера. Після перевірки ключа, сервер додається у файл known_hosts у каталозі у клієнтський машині. Цей файл містить інформацію про всі перевірені клієнтом сервери.
- Якщо клієнт не вперше отримує доступ до сервера, ідентифікатор сервера порівнюється із попередньо записаною інформацією із файлу known_hosts для перевірки.

Після підтвердження серверу, обидві сторони узгоджують ключ сеансу, цей процес виконується згідно алгоритму Деффі-Хеллмана. Цей алгоритм розроблений таким чином, що обидві сторони вносять однаковий внесок у генерації сесійного ключа. Згенерований ключ сеансу є спільним симетричним ключем, тобто той самий ключ використовується як для шифрування так і для дешифрування даних.

Кінцевим етапом є аутентифікація клієнта. Аутентифікація здійснюється за допомогою пари ключів SSH. Як випливає з назви, пара ключів SSH — це не що

інше, як пара з двох ключів для двох різних цілей. Одним з них є відкритий ключ, який використовується для шифрування даних і яким можна вільно ділитися. Інший - закритий ключ, який використовується для розшифровки даних і ніколи нікому не передається.

Після встановлення симетричного ключа аутентифікація виконується наступним чином:

- Клієнт надсилає серверу ідентифікатор пари ключів, за допомогою якої він хоче виконати аутентифікацію.
- Сервер перевіряє файл authorized_keys акаунта на який клієнт намагається увійти за допомогою ідентифікатора ключа.
- Якщо публічний ключ та ідентифікатором які перевіряються, знаходять у файлі, сервер генерує випадкове число, використовує публічний ключ щоб зашифрувати це число та відправляє це шифроване повідомлення.
- Якщо клієнт має правильний приватний ключ, він дешифрує повідомлення, щоб отримати те випадкове число яке згенерував сервер.
- Клієнт комбінує отримане випадкове число із поділеним сесійним ключем та обчислює хеш MD5 цього значення.
- Потім клієнт надсилає цей хеш MD5 до сервера як відповідь на зашифроване числове повідомлення.
- Сервер використовує той самий поділений сесійний ключ та оригінальне число, яке він відправляв до клієнт, щоб той підрахував значення MD5 самостійно. Він порівнює свій підрахунок із тим, яке клієнт надіслав назад. Якщо ці два значення співпадають, це доказує, володів приватним ключем і дає добро на аутентифікацію.

Асиметрія ключів дозволяє аутентифікувати клієнта, оскільки клієнт може розшифрувати повідомлення, лише якщо він має правильний асоційований приватний ключ.

Ще однією технологію віддаленого об’єднання у мережу є VPN, Virtual Private Network. Реалізація віддаленого доступу за допомогою VPN дозволяє окремим користувачам встановлювати безпечні з’єднання з віддаленою

комп’ютерною мережею. Ці користувачі можуть отримати доступ до захищених ресурсів у цій мережі, як якщо б вони були безпосередньо підключені до серверів мережі. Модель зв’язку між абонентам при використанні VPN позначена на рисунку 3.5:

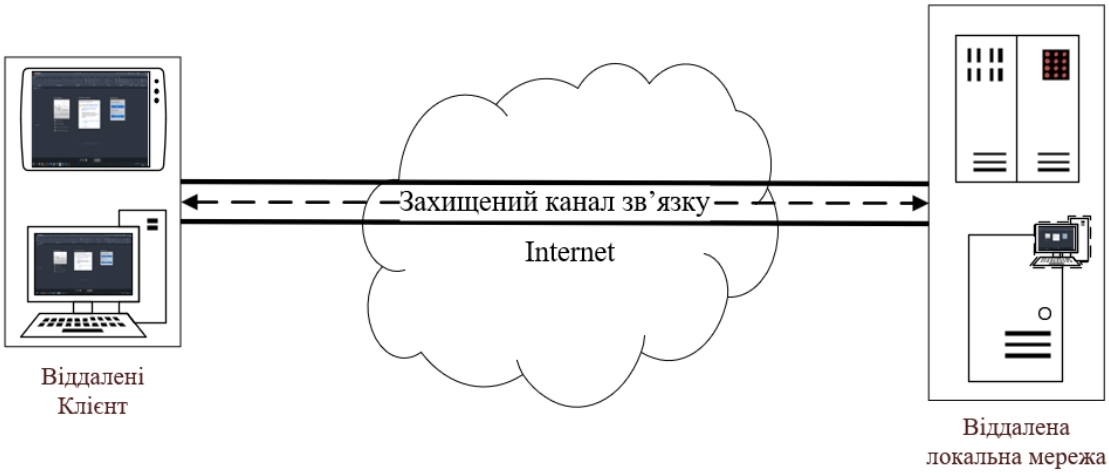

Рисунок 3.5 – Модель зв’язку абонентів VPN

Для реалізації віддаленого доступу за допомогою VPN необхідні два компоненти:

- Перший — це сервер доступу до мережі. Він може бути виділеним сервером або одним із кількох програмних додатків, які працюють на спільному сервері. Це NAS, до якого користувач підключається з Інтернету, щоб використовувати VPN. Сервер вимагає від користувача надати дійсні облікові дані для входу в VPN. Для аутентифікації облікових даних користувача NAS використовує власний процес аутентифікації або окремий сервер аутентифікації, що працює в мережі.

- Іншим обов'язковим компонентом VPN з віддаленим доступом є клієнтське програмне забезпечення. Іншими словами, студенти, які хочуть використовувати VPN зі своїх комп’ютерів, потребують програмного забезпечення на цих комп’ютерах, яке може встановлювати та підтримувати з’єднання з VPN. Більшість операційних систем сьогодні мають вбудоване програмне забезпечення, яке може підключатися до VPN з віддаленим доступом, хоча деякі VPN можуть

вимагати від користувачів замість цього встановити певну програму. Клієнтське програмне забезпечення встановлює тунельне з'єднання з NAS, яке користувач вказує своєю адресою в Інтернеті. Програмне забезпечення також керує шифруванням, необхідним для забезпечення безпеки з'єднання.

3.2 Модель підключення до віддаленої лабораторії

Для спрощення усіх майбутніх розрахунків є пропозиція використовувати об'єктно орієнтованим принцип побудови майбутніх моделей підключення мережи лабораторії з віддаленим доступом. Кожна модель складається з:

- Локальні об'єкти - елементи мережі, які розташовуються безпосередньо у приміщенні лабораторії.
- Віддалені об'єкти – елементи мережі, які розташовуються поза території приміщення лабораторії, наприклад особистий пристрій студента.
- Транзитні об'єкти – елементи які використовуються виключно для організації зв'язку та передачі даних між локальними та віддаленими об'єктами.

Спробуємо створити загальну модель підключення до лабораторії. Вона зображена на рисунку 3.6:

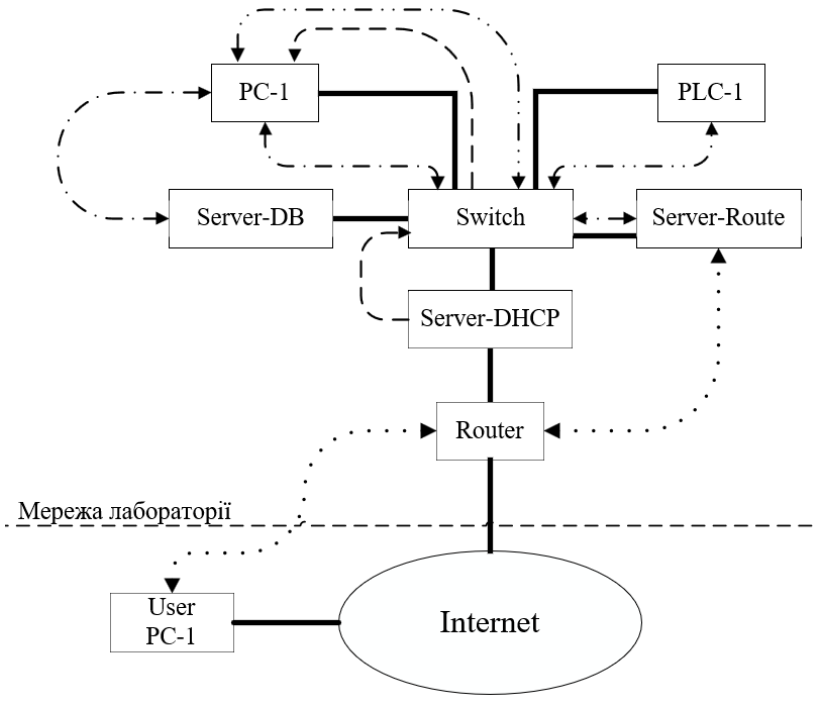

Рисунок 3.6 – Модель підключення до віддаленої лабораторії

На даній моделі можливо побачити з’єднання між віддаленим користувачем та усією мережею лабораторії. Спочатку почнемо з пояснення складових частин мережі:

- User PC-1 – віддалений персональний пристрій студента, за допомогою якого він виконує зв’язок із лабораторією.
- Internet – зовнішня мережа чи всесвітня павутина, являє собою уособлену групу мережевого обладнання (маршрутизатори та комутатори), які зв’язані між собою, являє собою транзитну частину від віддаленого користувача до мережі лабораторії.
- Router – головний маршрутизатор у лабораторній мережі, виконує функцію попереднього перенапрямку між пристроями перед сервером Route.
- Server DHCP – сервер DHCP, який призначений для розповсюдження статичних IP адресів для оперативних пристроїв локальної мережі лабораторії.
- Server Route – сервер маршрутизації, відповідає за перевірку аутентифікації користувачів та їх наступний перенапрямок до необхідних пристроїв.
- Server DB – сервер локальної бази даних, виконує функцію зберігання усієї необхідної інформації для виконання роботи за лабораторним устаткуванням.
- Switch – комутатор локальної мережи, головний інструмент для усього фізичного об’єднання лабораторного обладнання між собою, а також не останній у виконанні перенапрямку пакетів.
- PC-1 – локальний комп’ютер лабораторний мережі, на ньому встановлено усе необхідне програмне забезпечення для виконання лабораторних робіт та через нього виконується зв’язок із іншим лабораторним обладнанням, наприклад програмуємо логічного контролера (PLC).
- PLC-1 – програмуємо логічний контролер, локальне обладнання для виконання практичних завдань.

Крім обладнання на моделі можливо зазначити різноманітні види ліній, які з’єднують пристрої між собою. Кожна із цих ліній уособлює свою операцію у мережі віддаленої лабораторії. Спробуємо розібрати кожну з них:

- Пунктирна лінія між User PC-1, Router, Server Route показує зв’язок між пристроями шляхом паранапрямку пакетів від PC-1 до Server Route. Перенапрямок портів – це технологія, що дозволяє звернутися з зовнішньої мережи до пристрої які знаходяться у внутрішній мережі за маршрутизатором.
- Суцільна лінія – фізичний зв’язок між віддаленим пристроєм та локальної мережі лабораторії.
- Штрихована лінія між Server DHCP та PC-1 організує призначення та передачу локальній машині статичної IP адреси для майбутнього перенапрямку її управління до віддаленого пристрою користувача.
- Штрих-пунктирна лінія між Server Route, Switch та PC-1 являє собою маршрут для перенапрямку підключення від User PC-1 до PC-1. Це необхідно для надання можливості віддаленому користувачу виконувати роботу на локальній машині у мережі. Можливо це завдяки попередньому призначенню статичної адреси локальній машині від сервера DHCP.
- Штрих-2 пунктирна лінія між PC-1, Switch та PLC-1 організує зв’язок між локальної машиною та локальним обладнанням, шляхом використанням спеціального програмного забезпечення, яке встановлене на цієї локальній машині. Необхідними даними для цієї операції є IP та MAC адреси локального обладнання.

3.3 Моделі мережі віддаленої лабораторії

Першим кроком для створення моделі мережи лабораторії з віддаленим доступом є формування усіх множин існуючих елементів. До них відносяться:

- Першими множинами є робочі станції PC-i ($i \in \{1,2,\ldots, n\}$, n – загальна кількість абонентів), вони же абоненти локальні ($A_{Л1\text{-}n}$) та віддалені ($A_{B1\text{-}n}$), обчислюється від 1 до n, де n є кількістю абонентів у мережі.
- Наступною множиною є лабораторне обладнання PLC-i ($i \in \{1,2,\ldots, n\}$, n – загальна кількість обладнання) ($O_{Л1\text{-}n}$), обчислюється від 1 до n – кількість обладнання у мережі.

- Іншою множиною є сервера ($S_{Л1\text{-}n}$), можуть розрізнятися, в залежності від того яка задача стоїть перед ними (DHCP, Data Base, Route, WEB).
- Маршрутизатори Router ($R_{1\text{-}n}$) – є наступною множиною елементів, яка служать для організації зв'язку між лабораторії та зовнішнім середовищем.
- Комутатори Switch ($K_{1\text{-}n}$) – множина елементів, які служить для фізичного об'єднання усієї мережи між собою.
- Останньою є множина зв'язків упорядкованої кількості комутаторів ($К_{TPi\text{-}n}$) та маршрутизаторів ($R_{TPi\text{-}n}$), де i ∈ {1,2,…, n}, n – загальна кількість обладнання у зовнішній мережі Internet ($M_{СВ}$).

За допомогою усіх цих елементів можливо скласти моделі підключення до мережи віддаленої лабораторії, звертаючи увагу на те, які типи та методи зв'язку застосовуються під час проектування цієї мережи.

Будемо розглядати наступні моделі підключення до віддаленої лабораторії:

- Підключення від віддаленого абонента до локальної робочої станції.
- Пряме підключення від віддаленого абонента до локального обладнання.
- Підключення від віддаленого абонента до віртуального робочого столу.
- Підключення від віддаленого абонента до локальної робочої станції по WEB інтерфейсу.
- Підключення від віддаленого абонента до локального обладнання по WEB інтерфейсу.

Розглядання моделей підключення до віддаленої лабораторії почнемо з моделі підключення від віддаленого абонента до локальної робочої станції, яка зображена на рисунку 3.7.

Ця модель передбачає підключення віддаленого абонента User PC-i (A_{Bi}), до локального абонента PC-i ($A_{Лn}$). Підключення виконується наступним шляхом:

- Перед підключенням на сервері організуються усі можливі маршрути підключення в локальній мережі. За допомогою сервера DHCP ($S_{Л1}$) усьому локальному обладнанню роздаються статичні IP адреси. Усі статичні IP адреси

разом із номерами портів комутаторів до яких підключені ці пристрої фіксуються на сервері Route ($S_{Л2}$), через який і виконується уся наступна маршрутизація.

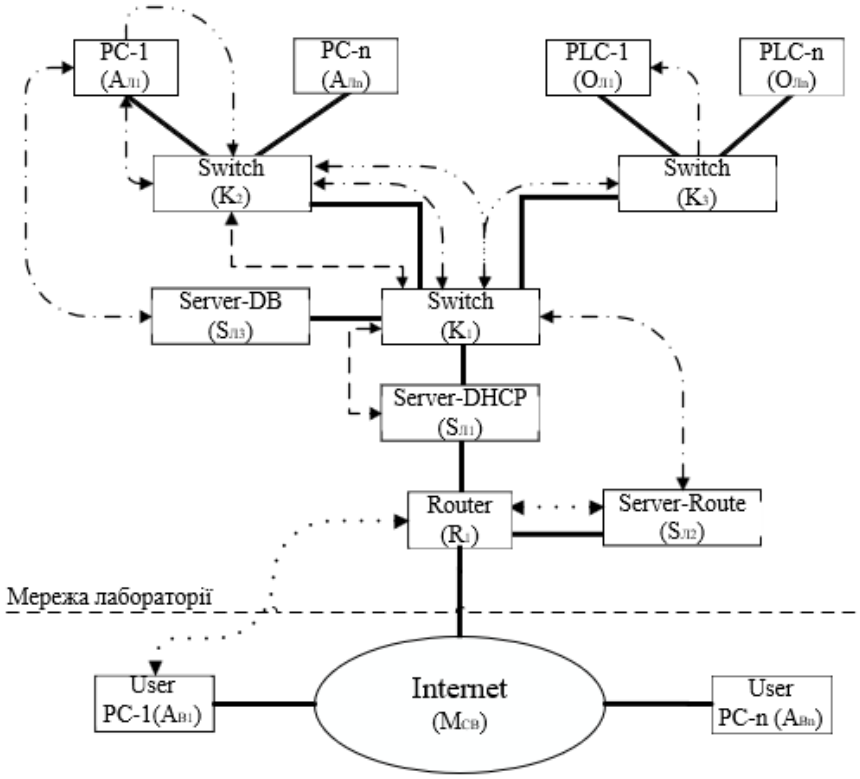

Рисунок 3.7 – Модель підключення від віддаленого абонента до локальної робочої станції

- Віддалений абонент User PC-і (A_{Bn}) відправляє пакет даних через зовнішню мережу до маршрутизатора Router (R_1) у лабораторній мережі.
- Потрапляючи до маршрутизатор (R_1) пакет, завдяки перенапрямку пакетів переходить до локального сервера Route ($S_{Л2}$), який перевіряє право віддаленого користувача (A_{Bn}) на вхід та очікує від нього відповіді.
- Після отримання відповіді від віддаленого користувача (A_{Bn}) сервер Route ($S_{Л2}$), перенаправляє користувача до обраної локальної робочої станції PC-і ($A_{Лn}$), це виконується завдяки попередньо налаштованим маршрутам, які зазначені на сервері Route..

- Для виконання практичних занять та лабораторних робіт необхідно організувати зв’язок із локальним обладнанням PLC-і ($О_{Лі\text{-}n}$) виконується за допомогою одній із обраних локальних робочих станцій PC-і ($А_{Лі\text{-}n}$).

- У випадку необхідності додаткових матеріалів для виконання лабораторних робіт користувачу необхідно підключається до сервера DB ($S_{Л3}$). Виконується це шляхом маніпулювання локального абонента PC-і ($А_{Лі\text{-}n}$) до якого були виконано підключення.

Відправка пакету даних від локальної робочої станції до віддаленого абоненту виконується у зворотному порядку. В даному випадку цим пакетом даних є інформація з пристроїв виводу локального абоненту PC-і ($А_{Лі\text{-}n}$).

Другою моделлю підключення до віддаленої лабораторії є модель підключення від віддаленого абонента до локального обладнання, яка зазначена на рисунку 3.8:

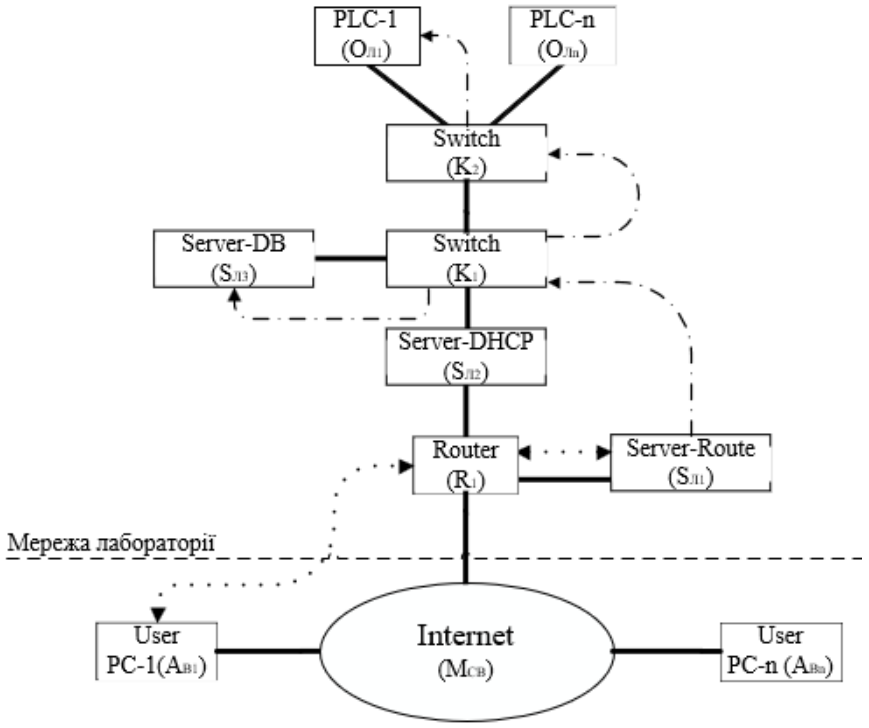

Рисунок 3.8 – Модель підключення від віддаленого абонента до локального обладнання.

Згідно цієї моделі програмне забезпечення для виконання лабораторних робіт знаходиться на робочому пристрої студента, через що в даному випадку необхідно

організувати зв’язок із лабораторним обладнанням. Підключення виконується наступним шляхом:

- Студент через віддалений пристрій User PC-i (A_{Bi-n}) відправляє пакет даних через зовнішню мережу ($M_{СВ}$) до маршрутизатора (R_1), який знаходиться у лабораторній мережі.
- Після потрапляння до маршрутизатора (R_1), пакет даних переходить до сервера Route ($S_{Л2}$), який потребує підтвердження на вхід до мережи від віддаленого пристрою User PC-i (A_{Bi-n}).
- Після отримання підтвердження прав на роботу у мережі, сервер Route ($S_{Л2}$) перенаправляє пакет даних до лабораторного обладнання PLC-i ($O_{Лі-n}$) при умові що воно є вільним.
- У випадку необхідності додаткових матеріалів для виконання лабораторних робіт користувач підключається до сервера DB ($S_{Л3}$).

Третя модель, яка підлягає розгляданню є модель Підключення від віддаленого абонента до віртуального робочого столу, яка зазначена на рисунку 3.9:

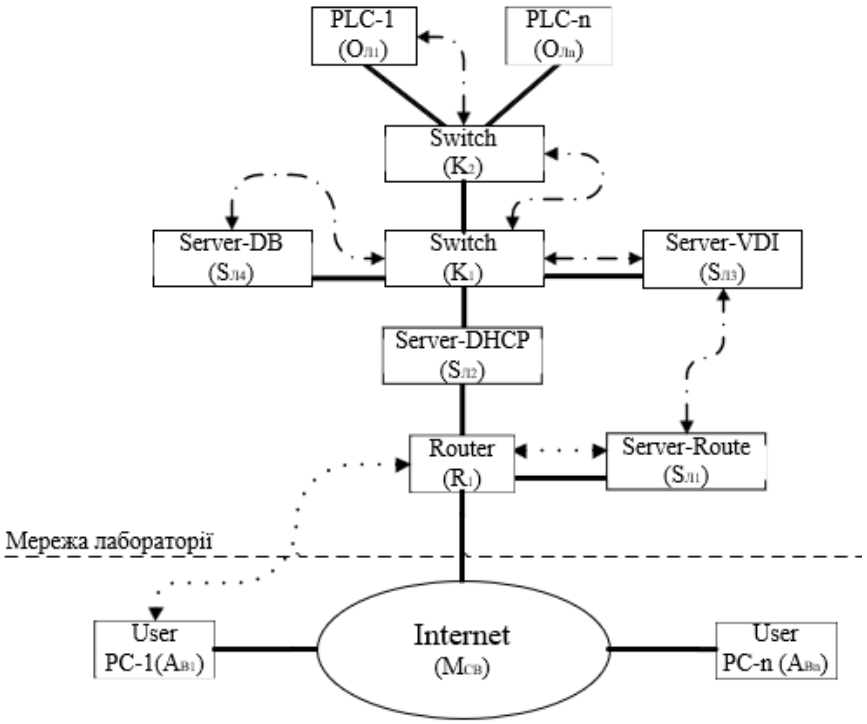

Рисунок 3.9 – Модель підключення від віддаленого абонента до віртуального робочого столу.

Згідно цієї моделі підключення від віддаленого абонента виконується до одного із віртуальних робочих столів, виконується це наступним шляхом:

- За допомогою спеціального програмного забезпечення, студент на віддаленому пристрої User PC-і (A_{Bi-n}) виконує підключення до одного із віртуальних робочих столів на сервері VDI ($S_{Л1}$).
- Пакет даних від User PC-і (A_{Bi-n}) через зовнішню мережу ($M_{СВ}$) потрапляє до маршрутизатора (R_1), який знаходиться у лабораторній мережі.
- Далі маршрутизатор (R_1) перенаправляє пакет даних до серверу ($S_{Л1}$), який в свою чергу відправляє запит на підтвердження прав на користування.
- Після отримання підтвердження прав, сервер ($S_{Л1}$) перенаправляє пакет даних до серверу VDI ($S_{Л3}$) через маршрутизатор (R_1), сервер DHCP ($S_{Л2}$) та комутатора (K_1). На сервері ($S_{Л3}$) отримує особисте віртуальне середовище для роботи.
- Далі сервер ($S_{Л3}$) підключає користувача до лабораторного обладнання PLC-і ($O_{Лi-n}$), яке на той час є вільним, через комутатори (K_1) та (K_2).
- У випадку необхідності додаткових матеріалів для виконання лабораторних робіт користувач підключається до сервера DB ($S_{Л4}$).

Четвертою моделлю підключення до віддаленої лабораторії, яка підлягає розгляданню є модель підключення від віддаленого абонента до локального обладнання по WEB інтерфейсу, яка зазначена на рисунку 3.10.

Згідно цієї моделі віддалений абонент підключається та авторизується через WEB сервер, за допомогою якого виконується усі наступні маніпуляції по обміну даних, робота з базою даних та вибір до якого лабораторного обладнання потрібно підключитися, відображається вільне воно чи ні. Підключення виконується у такий спосіб:

- Віддалений абонент User PC-і (A_{Bi-n}) підключається через зовнішній мережу ($M_{СВ}$) до маршрутизатор (R_1).
- Маршрутизатор (R_1) перенаправляє пакет до WEB сервера ($S_{Л1}$), який у відповідь відправляє запит до користувача на підтвердження прав доступу.

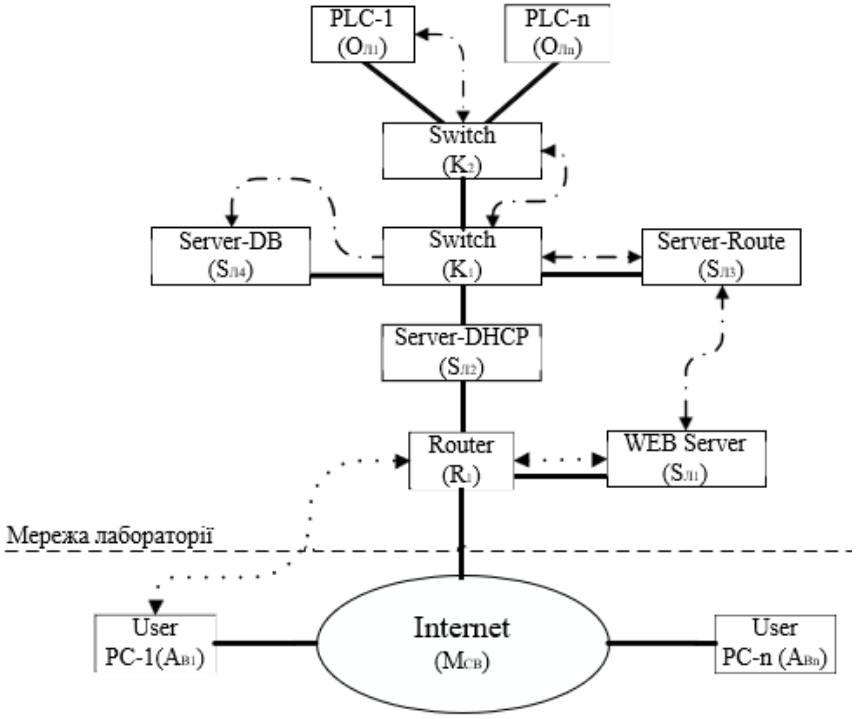

Рисунок 3.10 – Модель підключення від віддаленого абонента до локального обладнання по WEB інтерфейсу.

- Після підтвердження прав сервер ($S_{Л1}$), перенаправляє пакет даних до сервера Route ($S_{Л3}$), через маршрутизатор (R_1), сервер DHCP ($S_{Л2}$) та комутатор (K_1).
- Наступним кроком сервер ($S_{Л3}$) перенаправляє пакет даних до обраного лабораторного обладнання PLC-і ($О_{Лі-n}$).
- У випадку потреби у додаткових матеріалах для виконання практичних робіт, віддаленому абоненту PC-і ($А_{Вi-n}$) необхідно отримати доступ до сервера DB ($S_{Л4}$), який отримується за допоиогою сервер ($S_{Л1}$).

Відправка пакету даних назад до віддаленого абонента виконується в зворотному порядку.

Останньою модулю підключення до віддаленої лабораторії є від віддаленого абонента до локальної робочої станції по WEB інтерфейсу. Модель зображена на рисунку 3.11:

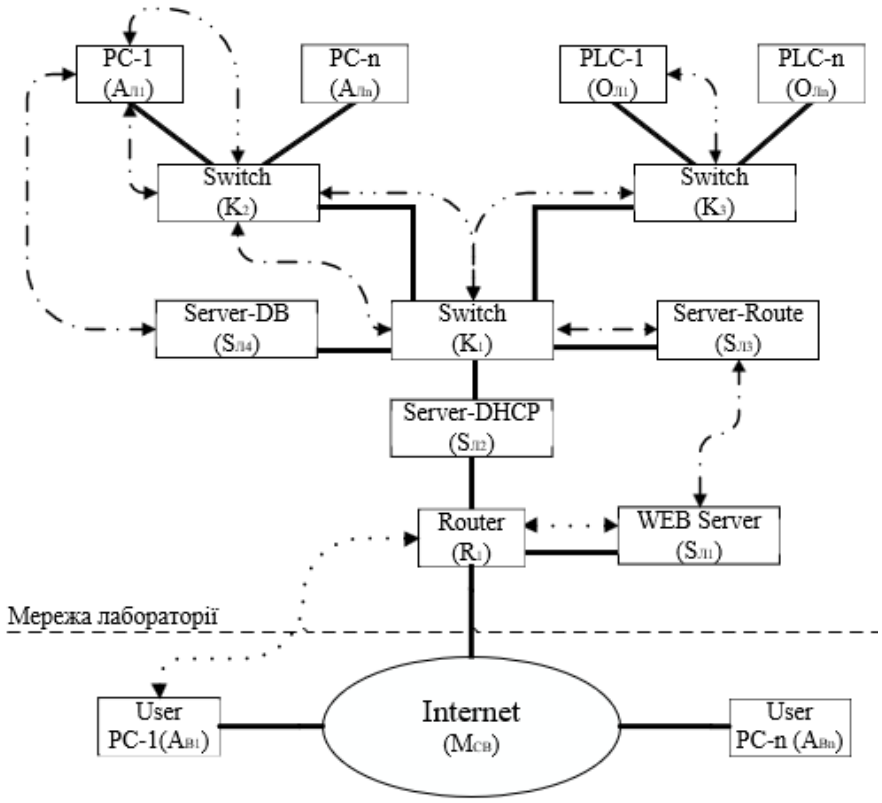

Рисунок 3.11 – Модель підключення від віддаленого абонента до локальної робочої станції по WEB інтерфейсу.

Згідно цієї моделі робота на локальних робочих станцій виконується за допомогою підключення та авторизація віддаленого абонента через WEB сервер. Уся наступна маніпуляція у мережі лабораторії виконується на локальній робочій станції, робоче простір якої транслюється за допомогою WEB сервера. Підключення виконується у наступний спосіб:

- Віддалений абонент User PC-i (A_{Bi-n}) відправляє пакет даних до WEB сервер ($S_{Л1}$) через зовнішній мережу ($M_{СВ}$).
- Пакет даних потрапляє до маршрутизатору (R_1), після чого він його перенаправляє до серверу ($S_{Л1}$).
- Після отримання вхідного пакету сервер ($S_{Л1}$), відправляє запит на підтвердження прав доступу від віддаленого абоненту (A_{Bi-n}), коли ($S_{Л1}$) отримує підтвердження він перенаправляє пакет далі.

- Пакет даних від серверу ($S_{Л1}$) потрапляє до серверу Route ($S_{Л3}$) через сервер DHCP ($S_{Л2}$) та комутатор (K_1), який в свою чергу перенаправляє усі дані до обраної локальної робочої станції PC-і ($A_{Лі\text{-}n}$) через комутатори (K_1) та (K_2).
- Наступний зв’язок із лабораторним обладнанням PLC-і ($O_{Лі\text{-}n}$) чи сервером DB ($S_{Л4}$), коли необхідний додатковий матеріал, виконується через обрану локальну робочу станцію PC-і ($A_{Лі\text{-}n}$).

3.4 Висновки до розділу 3

В даному розділі було проведено дослідження технологій віддаленого доступу:

- Технології віддаленої сесії.
- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Були виявленні особливості роботи кожної із цих технологій. Виходячи із їх принципів роботи були створені моделі підключення, які були максимально наближенні до реальної моделі підключення лабораторії із віддаленим доступом. Це дозволило отримати дані, які в майбутньому допоможуть розробити пропозицію організації лабораторії із віддаленим доступом.

4 РЕКОМЕНДАЦІЯ ЩОДО ТЕХНОЛОГІЇ ДОСТУПУ ДО ІСНУЮЧОЇ ЛАБОРАТОРІЇ

В даному розділі будемо розглядати рішення які в майбутньому часі мають перспективу бути використаними у розробці рекомендації щодо реалізації технології віддаленого доступу до існуючої лабораторії.

4.1 Розбір технологій віддаленого доступу на існуючій лабораторії

В ході проведення дослідження технологій доступу до віддаленої лабораторії були зазначені основні види технологій які вирішують цю проблему. Після проведення моделювання цих рішень можливо виділити три рішення, які найкраще підходять для побудови лабораторії із віддаленим доступом:

- Remote desktop services (RDS).
- Virtual private Network (VPN).
- Virtual desktop infrastructure (VDI).

Та перед тим, як порівнювати ці технології та обрати кращу для побудови майбутньої лабораторії із віддаленим доступом, приведемо список реального обладнання та схему його підключення.

Лабораторія до якої потрібно організувати віддалений доступ складається із:

- Головний маршрутизатор мережи D-Link DIR-620. Зв’язує лабораторне обладнання із зовнішнім середовищем.
- Головний комутатор Cisco catalyst 2960 на 24 порти, через нього проходять усі можливі маршрути в локальній мережі.
- Периферійні комутатори Allied telesis, at-fs724 на 24 порти для з’єднання із ПЛК та at-fs716 на 16 портів.
- ПЛК Phoenix Contact ILC 130 Starterkit, у кількості 15 штук

- Локальні робочі станції, у кількості 15 штук.
- Сервер DHCP, для роздачі статичних IP адресів у мережі.
- Сервер Route, організує усю маршрутизацію у локальній мережі.
- Сервер DB, зберігання усієї необхідної інформації у лабораторії.

Нижче, на рисунку 4.1 приведена схема підключення лабораторного обладнання:

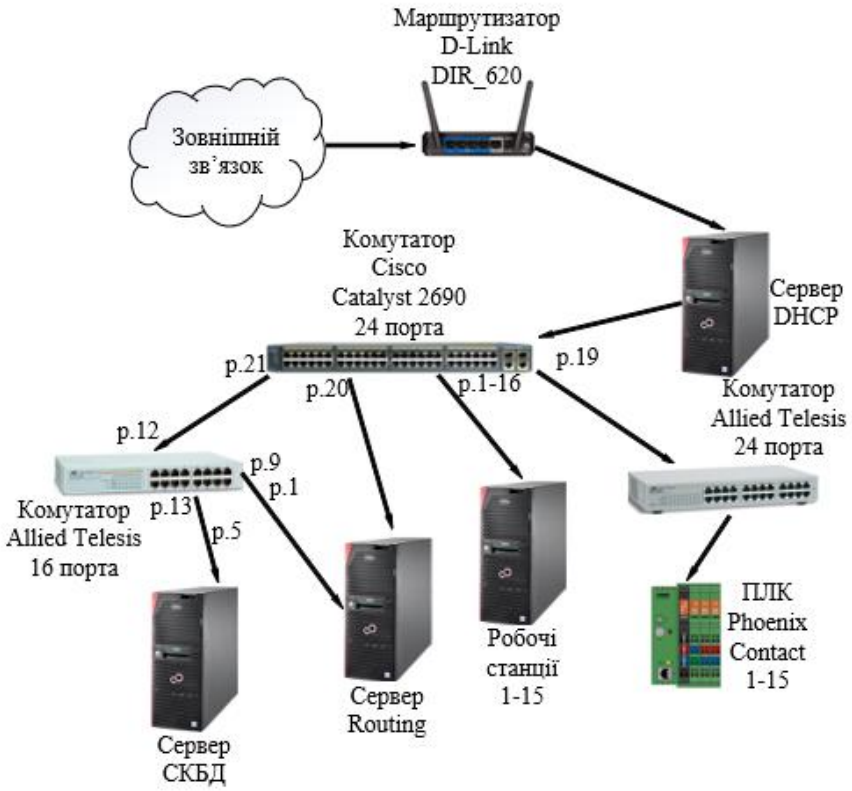

Рисунок 4.1 – Модель з'єднання локальної мережі лабораторії віддаленого доступу

Відтепер розберемо кожне із обраних рішень, виділяючи ключові моменти та виберемо максимально наближену до можливостей лабораторного обладнання. Зазначимо ключові вимоги, дотримування яких є основним при виборі рішення для побудови лабораторії із віддаленим доступом:

- Безпека зв'язку.
- Рівень налаштування обмежень користувача.
- Автономність.

- Вимоги до потужності.
- Кросплатформеність.

Розбір обраних рішень почнемо із VPN. Є достатньо популярним засобом підключенням до віддаленої мережі, дозволяючи користуватись усіма ресурсами цієї мережі, а саме дані та обладнання. Віддалений користувач без яких небудь проблем має можливість підключитися до мережі і відчуватися це буде так, якби він був частиною мережі у фізичному сенсі, якби знаходився безпосередньо у університеті. Модель взаємодії зображена на рисунку 4.2:

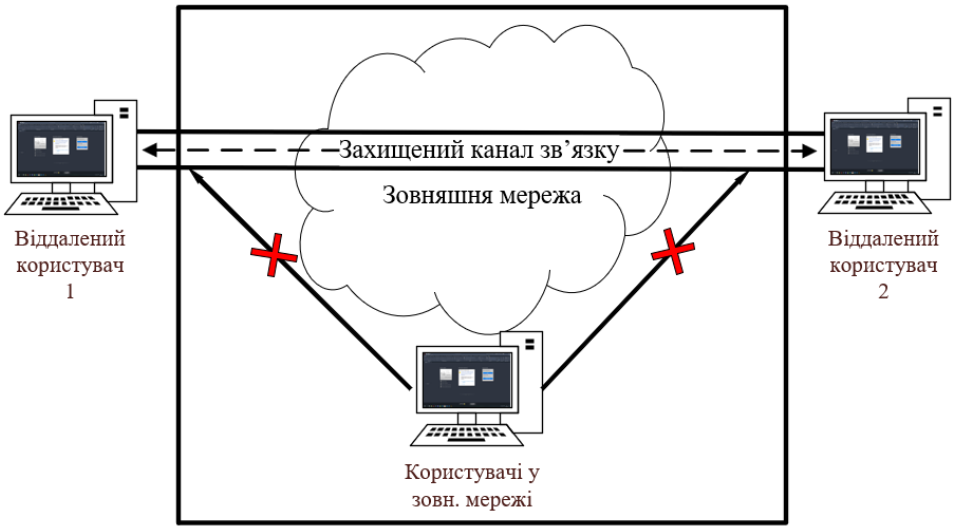

Рисунок 4.2 – Модель взаємодії VPN з'єднання

Так, як бачимо на рисунку, головним плюсом усього цього є те, що об'єднання у мережу виконується відокремленим каналом зв'язку, який знаходиться над усією зовнішньою мережею. Крім того, що дані передаються по захищеному та відокремленому каналі даних вони ще є шифрованими. Дешифровку вони проходять тільки на кінцях каналу, тобто на пристроях між яким він створений. До недоліків цього рішення стосовна нашої проблеми можливо віднести те, що VPN не дозволяє виконувати маніпуляції на віддаленому пристрої. Уся взаємодія між пристроями зводиться у об'єднання у мережу, тобто відсутня можливість керування віддаленим пристроєм. В умовах нашої лабораторії користувач зможе отримати доступ до лабораторного обладнання по типу ПЛК та

бази даних для виконання практичних занять, але усі програмні додатки потрібні будуть встановленні на робочих станція студентів. Крім цього, усі безкоштовні VPN додатки мають обмежену кількість користувачів у одній мережі. Тому використання цього рішення для побудови лабораторії із віддаленим доступом можливо вважати недоцільним.

Другим рішенням із цього списку є VDI. Ця технологія передбачає у мережі окремий сервер із віртуальними машинами до яких користувач і виконує підключення. Модель з'єднання зображена на рисунку 4.3:

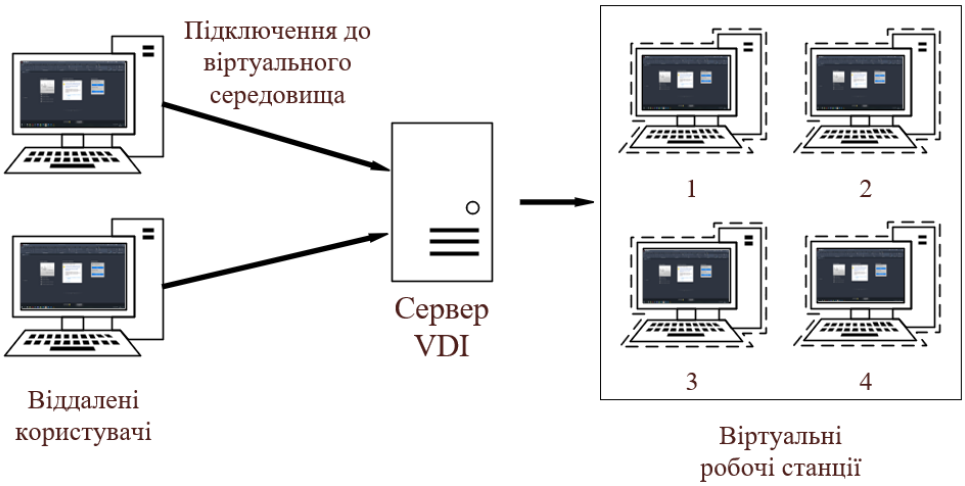

Рисунок 4.3 – Модель VDI з'єднання

Якщо подивитись на рисунок та спробувати розібрати трохи докладніше, такі системи складаються із двох рівнів:

- Фізичного, сервера та гіпервізори, безпосередньо на ньому і проходить налаштування системи та розбиття на віртуальні системи.
- Віртуальний, різноманітні програмні рішення, якими і керує віддалений користувач, створюється із образа який знаходиться на сервері.

Дані рішення є достатньо комплексними і складними у керуванні. Плюсами є те, що усі віртуальні машини є однаковими, адміністрування подібних систем є достатньо зручною, у випадка коли потрібно відновити версії програмного забезпечення, то оновлюється тільки 1 образ, а не весь фізичний парк робочих станцій. Кількість користувачів умовно не є обмеженими, як це наприклад можливо

із реальними робочими станціями. Але це також і є недоліком, у рішень які побудовані за принципами VDI дуже великі вимоги то потужності сервера, через те що усі розрахунки лежать на ньому. Крім цього потрібно подбати про системи захисту зв’язку та передачі даних від користувача до віртуальної системи. В умовах нашої лабораторії таке рішення не є доцільним.

Останнім рішенням, із обраних для організації віддаленого доступу до лабораторії є RDS. Дуже часто це рішення називають сервісом терміналов. Воно дозволяє користувачам увійти до віддаленого робочого столу, який підключено до серверу. Це рішення дозволяє доставляти образ графічного інтерфейсу від сервера до користувача та отримує від другого команди по маніпуляції цим графічним інтерфейсом. Зв’язок між пристроями зображено на рисунку 4.4:

Рисунок 4.4 - Схема зв’язку між пристроями по протоколу RDP

Сам RDS складається із трьох компонентів:

- Посередник підключення до віддаленого робочого столу (Remote Desktop Connection Broker) – є посередником підключення між користувачем та віддаленим сервером. У випадку несанкціонованого відключення, надає право перепідключитися без втрати даних.
- Шлюз віддаленого робочого столу – підключення до віддаленого робочого столу через інтернет.
- Ліцензування віддаленого робочого столу – відстеження ліцензії для розгортання RDP.

Значним плюсом цього рішення є те, що воно є пропрієтарним для усіх систем від Microsoft, іншими словами воно я на кожній системі із операційною

системою сімейства Windows. Також до плюсів цього рішення можливо віднести його простоту у використанні та продуктивність відносно рішень, які були переглянути раніше. Налаштування обмежень виконується за допомогою серверу. Якщо підходити з точки зору безпеки то в рішенні використовується стандартні функції безпеки:

- Обмеження кількості користувачів, що підключаються.
- Аутентифікація за допомогою пароля.
- Шифрування даних
- Можливість створити “Whitelist” IP адресів, що можуть підключитися.

Через що можливо зробити наступний висновок. Рішення на базі RDS, якщо його порівнювати із попередніми рішеннями, в тому чи іншому випадку виконує усі поставлені вимоги, які були висунуті до технологій віддаленого доступу до лабораторії.

4.2 Методи підключення до віддаленої лабораторії

Перед початком підключення є ряд налаштувань які необхідно виконати як зі сторони клієнта так і зі сторони серверу.

Зі сторони клієнта для початку роботи необхідно відкрити додаток Підключення до віддаленого робочого столу, цей додаток зображено на рисунку 4.5:

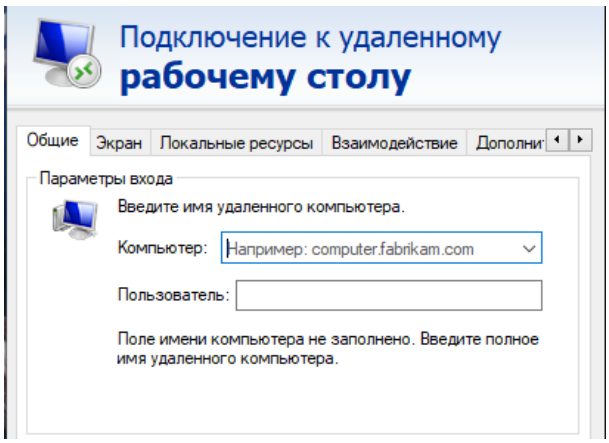

Рисунок 4.5 - Приклад додатку Підключення до віддаленого робочого столу

Можливо побачити, налаштування виконується в 5 різних вкладок:

- Вкладка «Загальні» - передбачає заповнення полів даними необхідними для підключення до тої віддаленої машини, до якої ми хочемо підключитися. У полі комп’ютер вказується IP адреса потрібного віддаленого абонента. У полі користувач вказується ім’я, яке зареєстроване у віддаленій робочій станції
- Вкладка «Екран» - передбачає налаштування розширення екрану, а також глибини кольору для віддаленого сеансу.
- Вкладка «Локальні ресурси» - параметри передачі аудіо та відео даних від віддаленого користувача, а також вибір локального обладнання.
- Вкладка «Взаємодія» - передбачає налаштування швидкості з’єднання для досягнення оптимальної швидкодії .
- Вкладка «Додатково» - Перевірка автентичності сервера.

Після виконання налаштування та введення даних для підключення можливо підключатися. Графічний інтерфейс підключеного віддаленого пристрою зображено на рисунку 4.6:

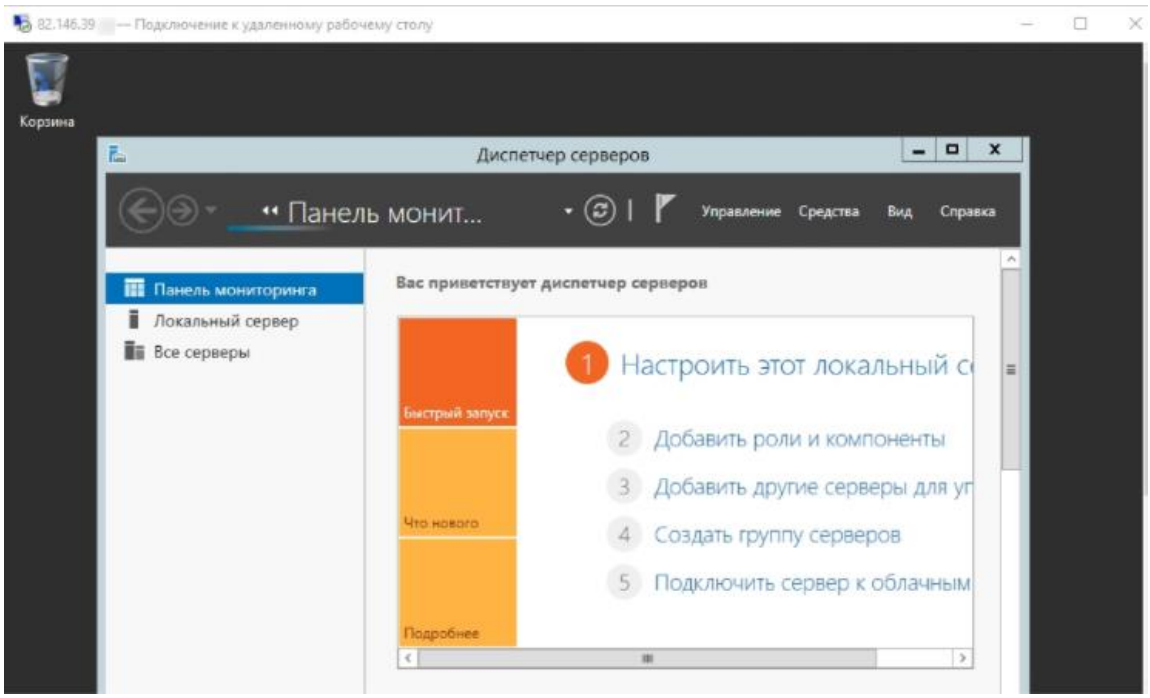

Рисунок 4.6 - Графічний інтерфейс підключеного віддаленого пристрою

Зі сторони сервера перед початком підключення виконується цілий спектр налаштувань, які можливо розділити на 4 етапи.

Етап перший - постановка ролі та компонентів. На цьому етапі встановлюються тип постановки, вибір ролі сервера, вибір служби серверу:

- У панелі швидкого запуску відкрити Диспетчер серверів.
- Натискаєм Управління – Додати ролі та компоненти.
- Натискаємо Далі до «Оберіть ти постановки». Залишаємо Постановка ролей та компонентів і натискаєм.
- У вікні «Вибір ролей сервера» обираємо Службу віддалених робочих столів.
- Натискаємо Далі, поки не з’явиться «Вибір служб ролей» та обираємо наступні - Ліцензування віддалених робочих столів та Вузол сеансів віддалених робочих столів.
- Натискаємо далі, якщо з’явиться запит на постановку додаткових компонентів погоджуємося. При необхідності, так само ставимо інші галки.
- Натискаємо Далі і у наступному вікні Встановити. Чекаємо на закінчення процесу установки і перезавантажуємо сервер.

Етап другий - постановка служб віддаленого робочого столу. В ході цього етапу вибирається тип розгортання та його сценарій:

- Після перезавантаження відкриваємо Диспетчер серверів та натискаємо Управління - Додати ролі та компоненти.
- У вікні «Вибір типу постановки» обираємо Постановка служб віддалених робочих столів і натискаємо Далі.
- У вікні «Вибір типу розгортання» обираєм швидкий запуск і натискаєм Далі.
- В «Вибір сценарію розгортається» - Розгортання робочих столів на основі сеансов.
- Натискаємо Далі. При необхідності ставимо галочку «Автоматично перезапускаємо кінцевий сервер, якщо це потрібно» і натискаємо Розгорнути.

Етап третій - налаштування ліцензованих робочих столів. Для коректної роботи сервера, необхідно налаштувати службу ліцензування.

- Відкриваємо диспетчер серверів та натискаємо по засобам – RDS. Диспетчер ліцензування віддалених робочих столів.
- В відкритому вікні натискаємо праву кнопку по нашому сервері та обираємо Активувати сервер.
- У відкритому вікні двічі натискаємо Далі – заповнюємо форму – Далі - Далі-Знімаємо галочку «Запустити майстер установки ліцензій» - Готово.
- Знову відкриваємо диспетчер серверів та переходимо до «Служби віддалених робочих столів».
- В «Огляді розгортання» натискаємо на Завдання - Змінити властивості розгортання.
- У вікні, що відкрилося, переходимо в Ліцензування - Вибираємо тип ліцензій - прописуємо ім'я сервера ліцензування (в даному випадку локальний сервер) і натискаємо Додати.
- Застосовуємо налаштування, натиснувши ОК.

Етап четвертий. Додавання ліцензії:

- Відкриваємо диспетчер серверів та натискаємо по Засоби - Remote Desktop Services - Диспетчер ліцензування віддалених робочих столів:
- У вікні, що клікаємо правою кнопкою миші по нашому серверу і вибираємо Встановити ліцензії.
- У вікні натискаємо Далі.
- Вибираємо програму, за якою куплені ліцензії, наприклад, Enterprise Agreement.
- Натискаємо Далі - вводимо номер угоди та дані ліцензії - вибираємо версію продукту, тип ліцензії та їх кількість.
- Натискаємо Далі - Готово.

4.3 Кроки обробки запитів

Опис процесу підключення та наступного виконання віддаленого управління. Цей сценарій відображає реалізацію процесу підключення від віддаленого абонента до локальної робочої станції, а також наступне виконання віддаленого управління, що зображено на рисунку 4.6:

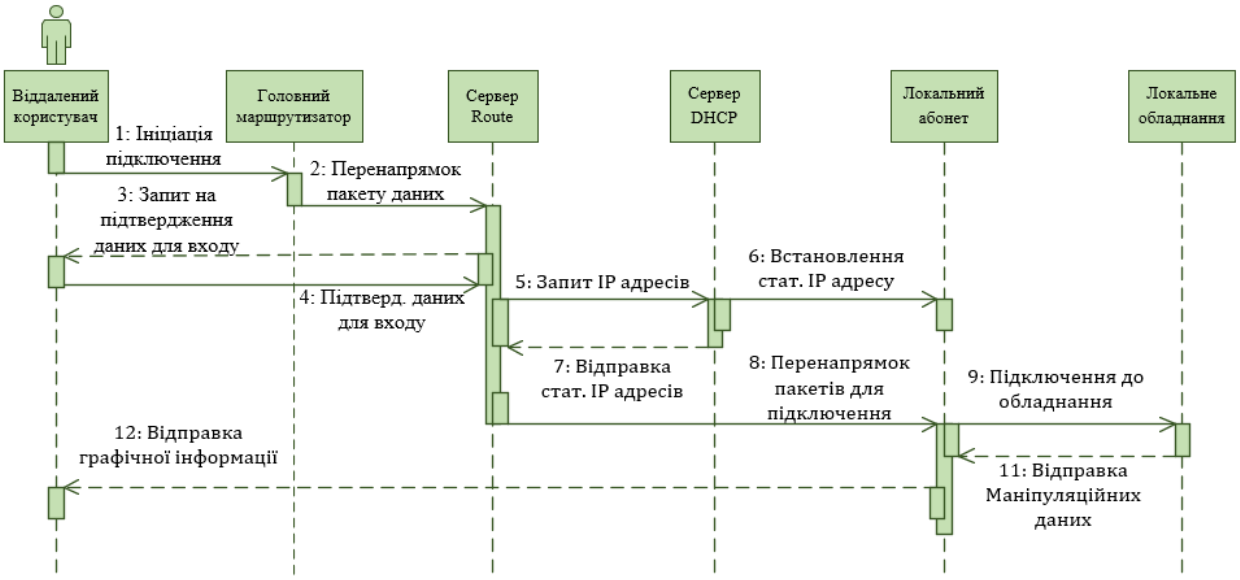

Рисунок 4.6 Сценарій процесу підключення та наступного виконання віддаленого управління

Як можливо побачити цей сценарій складається із 11 етапів, розберемо кожний із них:

- Перший. На цьому етапі процес ініціації підключення. Він починається зі сторони віддаленого користувача, відправкою пакету даних до локальної мережі лабораторії.
- Другий. Пакет даних шляхом перенапрямку портів від головного маршрутизатора переходить до серверу Route.
- Третій. Сервер Route питає у віддаленого користувача право на подальше виконання операції у мережі.

- Четвертий. Віддалений користувач відправляє дані для підтвердження запиту на право подальшого використання локальної мережи сервер Route.
- П’ятий. Майже одночасно з отриманням повідомлення від користувача, сервер Route робить запит до серверу DHCP про конфігурацію статичних IP адресів для подальшого перенаправлення віддаленого користувача до точки його призначення.
- Шостий. Сервер DHCP призначає усьому локальному обладнанню статичні IP адреса.
- Сьомий. Сервер DHCP відправляє конфігурацію IP адресів до сервера Route.
- Восьмий. Після отримання конфігурації IP адресів у мережі, сервер Route перенаправляє пакет даних від віддаленого користувача до локальної робочої станції, віддалений користувач має графічний інтерфейс від локальної робочої станції
- Дев’ятий. Віддалений користувач за допомогою локальної робочої підключається до локального обладнання (ПЛК) для подальшого виконання практичних занять.
- Десятий. Від локального обладнання до локальної робочої станції поступає дані про виконання програми написаній на спеціально програмному забезпеченню.
- Одинадцятий. Відображення на графічному інтерфейсі успішного виконання практичного заняття.

4.4 Оцінка рішення

Для розуміння ефективності організації лабораторії із віддаленим доступом спробуємо розібрати три випадки використання лабораторного обладнання студентами.

Перший випадок. Студент А, використовує лабораторне обладнання лише на практичних заняттях. Практичне заняття проходить 1 раз на неділю, час

заняття – 1 година 30 хвилин. Коефіцієнт використання лабораторного обладнання 3n (n = 30 хвилинам).

Другий випадок. Студент B, крім практичних занять, відвідує консультаційні години, консультація проходить 1 раз на тиждень, лабораторія відкрити з 8 години ранку і працює до 16 години дня, але консультація починається з 13:00, іншими словами студент має можливість використовувати лабораторне обладнання додаткові 4 година кожну неділю. Коефіцієнт використання лабораторного обладнання - 11n.

Третій випадок. Студент C має можливість працювати з лабораторним обладнанням тільки дистанційно, за допомогою віддаленого доступу. Через існування віддаленого доступу лабораторія може працювати 24/7. Припустимо, що студент C підключається до лабораторного обладнання кожний день та резервує собі обладнання на 2 години. Тоді ми маємо 14 годин праці із лабораторним обладнанням кожної неділі. Коефіцієнт використання лабораторного обладнання - 28n. На рисунку 4.7 зображений графік порівняння цих трьох випадків:

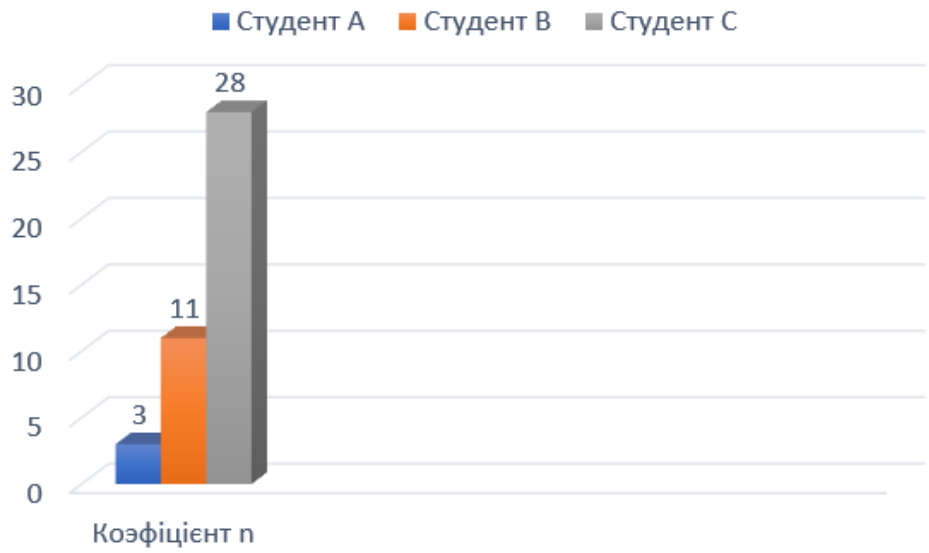

Рисунок 4.7 Відношення між кількістю корисного навантаження на лабораторне обладнання

Таким чином ми бачим велику різницю стосовно корисного навантаження на лабораторне обладнання, тобто воно використовується за призначенням – надання можливості студентам заробити якомога більше практичного досвіду.

4.5 Висновок до розділу 4

В даному розділі була проведена робота по складанню рекомендації щодо технології доступу до існуючої лабораторії. В ході її складання були виділені три технічних рішення, які розрізнялися між собою принципами роботи:

- Remote desktop services (RDS).
- Virtual private Network (VPN).
- Virtual desktop infrastructure (VDI).

Після проведення порівняння цих рішень із вимогами, які висувалися у зв’язку з особливістю технічного оснащення лабораторії, вибір для подальшого використання в складенні рекомендації пав на RDS.

Був розібраний сценарій процесу підключення та наступного виконання віддаленого управління при використанні RDS. Крім цього була проведена оцінка рішення, у якій було наглядно показано переваги лабораторії із віддаленим доступом над звичайною лабораторією, стосовно надання можливості студентам заробити якомога більше практичного досвіду.

ЗАГАЛЬНІ ВИСНОВКИ

В ході виконання даної роботи за основну мету було поставлено складання рекомендації щодо технології віддаленого доступу до існуючої лабораторії. В ході проведення аналізу було виділено чотири типи технологій віддаленого доступу:

- Технології віддаленої сесії.
- Технології захвату зображення.
- Технології віртуальної сесії.
- Технології віддаленого об’єднання у мережу.

Кожна з цих технологій має свої особливості у принципі роботи та сферах їх застосування. В ході аналізу, засновані на цих технологіях рішення були перевіренні на можливість їх застосування на існуючій лабораторії і як особливості цих технологій відображаються на працездатності лабораторії.

Також завдяки проведенню аналізу існуючих рішень були висунуті ряд вимог, яким має відповідати майбутнє рішення, яке потім буде застосовано при створені рекомендації щодо технології віддаленого доступу до існуючої лабораторії:

- Безпека зв’язку.
- Кросплатформеність.
- Рівень передачі інформації між віддаленими абонентами.
- Рівень налаштування обмежень.
- Автономність.
- Інформованість.
- Можливість організації роботи у групах.
- Вимогу до потужності.

Були розглянуті методи та порядок підключення рішень, які базуються на чотирьох обраних технологіях. Основуючись на них були розроблені наступні моделі підключення:

- Підключення від віддаленого абонента до локальної робочої станції.

- Пряме підключення від віддаленого абонента до локального обладнання.
- Підключення від віддаленого абонента до віртуального робочого столу.
- Підключення від віддаленого абонента до локальної робочої станції по WEB інтерфейсу.
- Підключення від віддаленого абонента до локального обладнання по WEB інтерфейсу.

За допомогою цих моделей було зазначено яким чином трафік пакетів пересуваються по мережі при використанні того чи іншого рішення.

В останньому розділі була складена рекомендація щодо технології віддаленого доступу до існуючої лабораторії. Розглянули сценарій процесу підключення та наступного виконання віддаленого управління існуючою лабораторією. Також в ході проведення оцінки рішення, було наглядно продемонстровані переваги лабораторії із віддаленим доступом над звичайною лабораторією, у випадку надання студентам можливість отримати якомога більше практичного досвіду.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Ariel Stolerman. RFC 6143: The Remote Framebuffer (RFB) Protocol Analysis - CS544, Drexel University,2017.

2. Xiaomei Chen, Hongyi Gao. A Remote PLC Laboratory Design and Realization – Procedia Engineering, 2012.

3. T. Ylonen. The Secure Shell (SSH) Protocol Architecture, 2006. [Електронний ресурс], https://datatracker.ietf.org/doc/html/rfc4251

4. How a VPN (Virtual Private Network) Works, [Електронний ресурс]

5. What is Remote Acceess, [Електронний ресурс], https://remoteaccess.itarian.com/what-is-remote-access.php.

6. PCoIP Seccion-Creation Steps and Actors , [Електронний ресурс], https://www.teradici.com/web-help/pcoip_client_sdk/windows/19.11/pcoip_session_creation_steps_and_actors/.

7. How does SSH work, [Електронний ресурс], https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

8. Remote Desktop Protocol: Basic Connectivity and Graphics Remoting, [Електронний ресурс], https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/5073f4ed-1e93-45e1-b039-6e30c385867c?redirectedfrom=MSDN

9. Литвин О.І., Криловський І.В. Організація процесу навчання на базі VNC технологій, Збірник наукових праць Дніпровського державного технічного університету. – 2015, [Електронний ресурс], http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Znpddtu_2015_1_65

10. Securing Remote Desktop (RDP) for System Administrators, [Електронний ресурс], https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators