Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіті другий (магістерський)
(повна назва)

Модернізація корпоративної мережі навчального закладу

(тема)

Виконав:

здобувач 2 року навчання,

групи ІМІм-23-1

Дудник Г.О.
(прізвище, ініціали)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник: доц. Харченко Н.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Здобувач _____ / Дудник Г.О. /
(підпис) (прізвище та ініціали)

Керівник _____ / Харченко Н.А. /
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“ 28 ” жовтня 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Дуднику Герману Олеговичу
(прізвище, ім’я, по батькові)

1. Тема роботи Модернізація корпоративної мережі навчального закладу

затверджена наказом по університету від “ 28 ” жовтня 2024 р. № 1148Ст

2. Термін подання студентом роботи до екзаменаційної комісії 22 січня 2025 р.

3. Вхідні дані до роботи Дослідити поточний стан корпоративної мережі навчального закладу на прикладі локальної мережі Слов’янського фахового коледжу транспортної інфраструктури (СФКТІ). Проаналізувати питання безпеки, можливостей масштабування та мережних налаштувань. Визначити варіанти модернізації та впровадження захисту корпоративної мережі. Провести організацію системи відеоспостереження та створення веб-сервера з базою даних по навчальним матеріалам, що необхідні для освітнього процесу у змішаній формі навчання.

4. Перелік питань, що потрібно опрацювати у роботі Вступ
1 Корпоративна мережа
2 Аналіз поточного стану корпоративної мережі СФКТІ
3 Модернізація захисту корпоративної мережі СФКТІ
4 Організація веб-сервера з базою даних
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) слайди презентації в форматі Power Point (назва, мета та задачі роботи; загальні поняття про корпоративну мережу; етапи аналізу корпоративної мережі; план території та основні поверхи навчального закладу; схема мережі навчального закладу в програмі Cisco Packet Tracer; дослідження мережі за допомогою аналізатора мережних протоколів Wireshark; дослідження мережі за допомогою програмного засобу iPerf; вибір обладнання для системи відеоспостереження; тестування роботи IP-камер в середовищі Cisco Packet Tracer; оновлена схема мережі навчального закладу в програмі Cisco Packet Tracer; схема живлення відеоспостереження; аналіз та модернізація сервера СФКТІ; створення RAID-5, організація веб-сервера з базою даних; створення користувачів для роботи з веб-сервером, налаштування автентифікації; висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ	28.10.2024	виконано
2	Підбір літератури за темою роботи	31.10.2024	виконано
3	Виконання розділу 1	07.11.2024	виконано
4	Виконання розділу 2	21.11.2024	виконано
5	Виконання розділу 3	30.11.2024	виконано
6	Виконання розділу 4	18.12.2024	виконано
7	Оформлення презентаційного матеріалу	27.12.2024	виконано
8	Подача диплома на перевірку та рецензування	13.01.2025	виконано

Дата видачі завдання 28 жовтня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Харченко Н.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 36 рис., 3 табл., 28 джерел, 2 додатки.

Об'єкт дослідження – корпоративна мережа навчального закладу СФКТІ.

Мета роботи – дослідження та аналіз поточного стану корпоративної мережі навчального закладу СФКТІ, модернізація захисту за допомогою впровадження системи відеоспостереження, організація веб-сервера з базою даних для поліпшення навчання.

Кваліфікаційна робота присвячена дослідженню та модернізації корпоративної мережі. Розглядаються два методи аналізу: з допомогою візуалізації (Cisco Packet Tracer та Visio) та програмного аналізу (iPerf та Wireshark). Створено систему відеоспостереження, де окрему увагу приділено схемі живлення та обладнанню. Проведено порівняльну характеристику накопичувачів для системи відеоспостереження та серверу. Створено веб-сервер, з метою поліпшення навчання та надання спільного доступу до навчальних ресурсів.

КОРПОРАТИВНА МЕРЕЖА, СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ, ВЕБ-СЕРВЕР, IPERF, WIRESHARK, CISCO PACKET TRACER, RAID, POE, NVR, VMS, MIKROTIK.

THE ABSTRACT

Explanatory note: 69 p., 36 fig., 3 tab., 28 sources, 2 app.

The object of study is the corporate network of the SFKTI educational institution.

Purpose - to study and analyze the current state of the corporate network of the educational institution of the SFKTI, to modernize security through the introduction of a video surveillance system, to organize a web server with a database to improve learning.

The qualification work is devoted to the research and modernization of the corporate network. Two methods of analysis are considered: visualization (Cisco Packet Tracer and Visio) and software analysis (iPerf and Wireshark). A video surveillance system is created, where special attention is paid to the power supply circuit and equipment. A comparative characterization of the drives for the video surveillance system and the server is carried out. A web server was created to improve learning and provide shared access to educational resources.

CORPORATE NETWORK, VIDEO SURVEILLANCE SYSTEMS, WEB SERVER, IPERF, WIRESHARK, CISCO PACKET TRACER, RAID, POE, NVR, VMS, MIKROTIK.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

СФКТІ – Слов’янський фаховий коледж транспортної інфраструктури;

End Devices – кінцеві пристрої, які є джерелами та одержувачами даних у корпоративній мережі, наприклад: комп’ютери, ноутбуки, сервери, мобільні пристрої та інші мережні пристрої;

ОС – операційна система;

MikroTik – маршрутизатор керований операційною системою RouterOS;

Firewall – комплекс апаратних чи програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього, відповідно до заданих правил;

cmd – команда строка;

WI-FI – це технологія бездротової мережі, на якій функціонують пристрої стандарту IEEE 802.11;

RTSP (Real Time Streaming Protocol) – це протокол мережевого управління, розроблений спеціально для використання в системах потокового мультимедіа;

ONVIF (Open Network Video Interface Forum) – це міжнародний стандарт, який забезпечує взаємодію і сумісність між пристроями відеоспостереження різних виробників;

HDD (Hard Disk Drive) – це жорсткий диск, пристрій для зберігання даних, який використовує магнітний запис для запису і зчитування інформації;

SSD (Solid State Drive) – це твердотільний накопичувач, який використовує флеш-пам’ять для зберігання даних;

UPS – автоматичний пристрій, що дає можливість підключеному обладнанню деякий час працювати від акумуляторів дбж при зникненні світла;

ККД – коефіцієнт корисної дії;

ОЗУ – оперативний запам’ятовуючий пристрій;

RDP - це протокол віддаленого робочого столу, розроблений Microsoft, який дозволяє підключатися до іншого комп’ютера або сервера через мережу;

SNAT – статичний NAT, який використовує одну загальну публічну IP-адресу;

NAT (Network Address Translation) — це спосіб поділити одну спільну інтернет-адресу на кілька пристроїв усередині локальної мережі.

ВСТУП

Прогрес не стоїть на місці, відкриваються нові знання, нові технології, сучасні умови спонукають до переосмислення підходів до навчання та до мережі в цілому. Все це пояснює зростання попиту до модернізації корпоративних мереж в закладах освіти, адже потрібно забезпечити ефективне функціонування навчальної та адміністративної діяльності. Станом на сьогодні, навчальні заклади повинні: забезпечувати безперебійну та захищену роботу корпоративної мережі, впроваджувати нові технології для організації та автоматизації навчального процесу. У цьому контексті модернізація корпоративної мережі стає важливим завданням, оскільки стає зрозуміло, чи відповідає навчальний заклад новим вимогам чи ні.

Актуальність роботи обумовлена тим, що більшість навчальних закладів потребують створення сучасної корпоративної мережі, яка здатна витримувати змінні умови навчання та щоденні навчальні процеси. Більшість корпоративних мереж застрягли в минулому, вони використовують старі налаштування мережі, які потребують оновлення обладнання та зміни конфігурації. Застаріле обладнання викликає наступні проблеми: низька пропускна здатність, недостатня безпека мережі та навчального закладу в цілому, відсутність підтримки нових стандартів та протоколів. Тому виникає необхідність у модернізації мережі, яка дозволить не лише усунути ці недоліки, а й значно покращити автоматизацію освітнього процесу.

Об’єктом дослідження виступає корпоративна мережа навчального закладу СФКТІ (стара назва СлКТІ), а предметом – процеси модернізації та технологічні рішення, які можуть бути використані для покращення та автоматизації її роботи.

1 КОРПОРАТИВНА МЕРЕЖА

1.1 Загальні відомості про корпоративну мережу

Корпоративна мережа – це інформаційне серце підприємства, яке об'єднує комп'ютери, сервери, маршрутизатори, ір-камери, та інші пристрої за допомогою дротового та бездротового з’єднання [1]. Виконання з’єднань виконується за двома наступними топологіями: зірка (пасивна та активна) та деревоподібна (змішана).

Топологія визначає такі аспекти, як вибір типу обладнання, тип кабелю та методи управління мережею. Вона також впливає на надійність роботи мережі та її можливості для розширення. Найбільш широко призначання в корпоративних мережах набула саме деревоподібна. Свою назву ця топологія отримала за рахунок комбінування декількох топологій зірка.

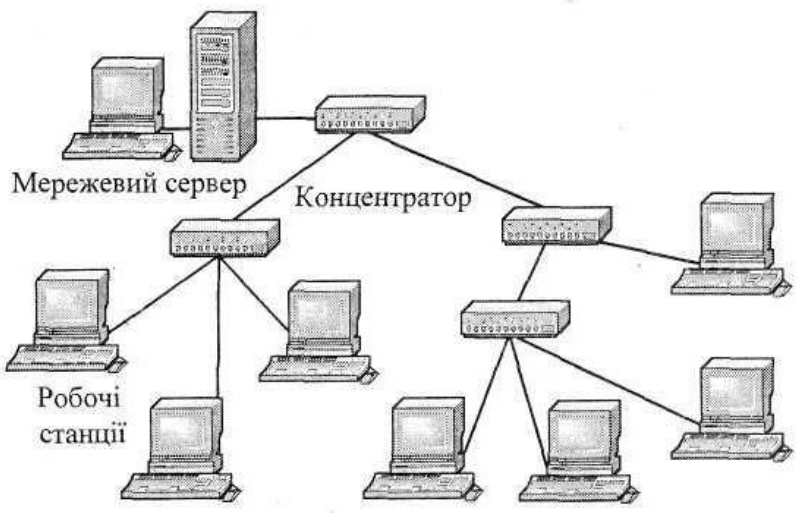

Рисунок 1.1 – Деревоподібна топологія

Топологія зірка – це топологія, в якій всі пристрої підключені до центрального пристрою, який виконує функцію точки збору і розподілу даних у мережі. Топологія зірка може бути: пасивною – тобто не керованою, в центрі якої

знаходиться хаб або концентратор, та активною – в центрі якої знаходиться активне обладнання: маршрутизатор, комп'ютер або сервер.

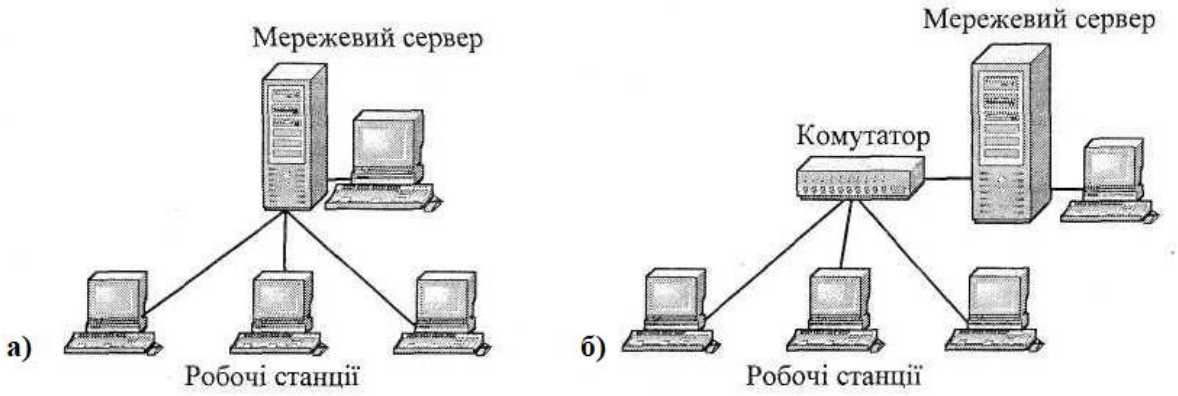

Рисунок 1.2 – Топологія зірка: а) активна; б) пасивна

Корпоративна мережа створюється з метою: забезпечення швидкого та надійного спільного доступу до ресурсів підприємства, обміну даними, комунікації між співробітниками, налаштування відеоспостереження, централізованого управління.

1.2 Компоненти корпоративної мережі навчального закладу

Корпоративна мережа в навчальному закладі зазвичай охоплює: комп'ютерні класи, сервери, сервіси аутентифікації, відеоспостереження, бібліотечні ресурси, корпоративні підрозділи, що забезпечують навчальний процес і підтримують роботу закладу. Виходячи з цього, корпоративна мережа включає в себе наступні компоненти:

1) Локальну мережу (LAN) – це комунікаційна мережа, яка об'єднує всі пристрої закладу між собою, використовуючи унікальний ідентифікатор та MAC-адресу. Локальна мережа дозволяє користувачам комунікувати один з одним за допомогою протоколів:

− Ethernet – протокол для передачі даних. Він визначає фізичні та канальні рівні, забезпечуючи передачу даних між вузлами, пристроями, серверами, тощо.

− TCP (Transmission Control Protocol) – протокол, який керує логічним сеансом зв’язку (установлює, підтримує й закриває з’єднання) між процесами й забезпечує доставку прикладних даних від процесу до процесу [2].

− UDP (User Datagram Protocol) – протокол, який забезпечує передачу пакетів без встановлення попереднього з’єднання. Тобто, якщо пакет загубиться або буде пошкоджений під час передачі, протокол не спробує повторно передати його.

− IP – протокол, який використовується для адресації та маршрутизації пакетів у локальній мережі. Варто зазначити, якщо під час просування пакета відбулася якась помилка, то протокол IP зі своєї ініціативи нічого не робить для її виправлення, його задача просто надіслати пакет. Разом із протоколом TCP (TCP/IP) забезпечує безпомилкову та гарантовану передачу даних [2].

− ARP (Address Resolution Protocol) – протокол, необхідний для визначення коректної MAC-адреси на основі IP-адреси в мережі. Якщо ця відповідність не була підтверджена, дані не передаються, або стають на призупинення передачі, поки коректний MAC-адрес не з’явиться у мережі.

− ICMP (Internet Control Message Protocol) – протокол, який призначений для обміну обміну діагностичними повідомленнями між вузлами, маршутизаторами, серверами, тощо. ICMP повідомляє про неможливість доставки пакета, перевищення часу життя, аномалії, зміни маршруту. Найпоширеніша команда для перевірки доступності інших пристроїв у мережі «ping».

− DHCP (Dynamic Host Configuration Protocol) – протокол, який дозволяє автоматично отримати IP-адресу в одному повідомленні для кожного пристрою в мережі. Для налаштування потрібно підключитися до DHCP-серверу на маршрутизаторі або сервері. Якщо не має до чого підключатися, то створити його та налаштувати (визначити пул та діапазон адрес) [2].

2) Маршрутизатори та комутатори – це пристрої мережі, за допомогою яких виконується з’єднання «End Devices». Маршрутизатор – це головний пристрій мережі, який будує оптимальну та надійну таблицю маршрутів, слідкує

за безпекою та контролює трафік кожного «End Devices». Комутатори в свою чергу – об’єднують «End Devices» в одну мережу за допомогою MAC-адрес. Комутатори мають таблицю комутації, де зберігається інформація про те, які пристрої підключені до портів, що дозволяє швидко передавати дані без колізій. Колізія – це явище, коли два чи більше пристрої відправляють дані одночасно через спільний канал передачі, в наслідок чого повідомлення пошкоджуються та втрачаються [3].

3) Сервери та бази даних – це комп’ютерна система, на яку встановлюється ОС та комплект програм, які забезпечують виконання певних сервісів. Наприклад, DHCP, VPN, DNS, веб-сервіси, поштові сервіси, файлові сервери, бази даних, тощо. База даних слугує як організоване сховище, яке створюється для того, щоб сервер знав де знайти інформацію на запит користувача.

4) Системи моніторингу та управління – це системи, які допомагають адміністраторам керувати конфігурацією та покращувати роботу мережі. Системи моніторингу включають в себе реєстрацію подій, які записуються в журнал, де вказується вся інформація стосовно роботи мережі та її користувачів.

5) Мережні кабелі та медіа-конвертери – це розхідні матеріали, які потрібні для прокладання зв’язку між різними «End Devices». Медіа-конвертори використовують коли потрібно з’єднати різнорідні типи носіїв, які працюють у різних середовищах (світлова хвиля, електричний імпульс), а мережні кабелі коли потрібно виконати фізичне з’єднання, яке буде забезпечувати високу швидкість та надійність мережі.

Корпоративна мережа навчального закладу включає в себе всі компоненти звичайної корпоративної мережі підприємства, але з впровадженням нових технологій потребує модернізації. Далі проведено аналіз поточного стану корпоративної мережі навчального закладу СФКТІ.

2 АНАЛІЗ ПОТОЧНОГО СТАНУ КОРПОРАТИВНОЇ МЕРЕЖІ СФКТІ

2.1 Огляд компонентів мережі начального закладу за допомогою візуалізації

Для оцінки стану корпоративної мережі навчального закладу потрібно провести технічний аналіз поточного стану, ознайомитися: з планом будівлі, логічною та фізичною схемою мережі. В навчальному закладі який досліджується – 5 поверхів. Для цього дослідження буде використано програми візуалізації, за допомогою яких буде побудовано план першого та другого поверхів, на інших трьох поверхах підключення до мережі не передбачене.

Візуалізація інфраструктури корпоративної мережі навчального закладу є важливим етапом у її оцінці та аналізі. Вона дозволяє адміністраторам мережі отримати чітке уявлення про всі компоненти, їх взаємозв’язки, можливості модернізації та її загальний стан. За допомогою програми Cisco Packet Tracer можна схематично представити логічну схему, на якій показано розташування та підключення «End Devices» кожного робочого місяця в мережі [8].

Логічна схема включає в себе планування та опис роботи мережі на рівні взаємодії пристроїв, підмереж, маршрутизації даних та рівнів доступу. Логічна мережа навчального закладу СФКТІ розбита на пули адрес, за допомогою маршрутизатора MikroTik [12]. Логічна структура:

1. Мережа навчально закладу: 192.168.1.0;
2. Головний маршрутизатор MikroTik: 192.168.1.1;
3. Wi-Fi обладнання: 192.168.1.2 – 192.168.1.10;
4. ПК викладачів: 192.168.1.11 – 192.168.1.50;
5. ПК студентів: 192.168.1.50 – 192.168.1.90;
6. ПК керуючого персоналу: 192.168.1.91 – 192.168.1.120;
7. Невідомі користувачі: 192.168.1.120 – 192.168.1.254.

Схема роботи мережі наступна:

1) Пристрій підключається до Wi-Fi або через кабель до мережі.

2) DHCP-сервер, налаштований на маршрутизаторі MikroTik, видає IP-адресу в залежності від MAC-адресу пристрою.

3) Трафік передається на маршрутизатор, де налаштовані правила міжмережевої безпеки (Firewall).

4) Доступ до внутрішніх ресурсів надається залежно від рівня доступу, налаштованого в пулі адрес.

5) У разі підключення невідомих пристроїв вони автоматично потрапляють в пул «Невідомі користувачі» з обмеженням доступу та обмеженою пропускною здатністю (192.168.1.120 – 192.168.1.254).

На рисунку 2.1 представлено схему території коледжу СФКТІ, де показано фізичне розташування всіх будівель навчального закладу, а також головний комп’ютеризований корпус №2.

Рисунок 2.1 – Схема території коледжу СФКТІ

План будівлі навчального закладу включає схематичне відображення всіх приміщень будівлі, де розташовані аудиторії, адміністративні приміщення, коридори, комп’ютерні класи та інші важливі об'єкти. Такий план важливий для дослідження та розуміння як організована мережа всередині закладу.

На рисунку 2.2 представлено схему мережі СФКТІ, де показано фізичну топологію та підключення по кабінетам та поверхам.

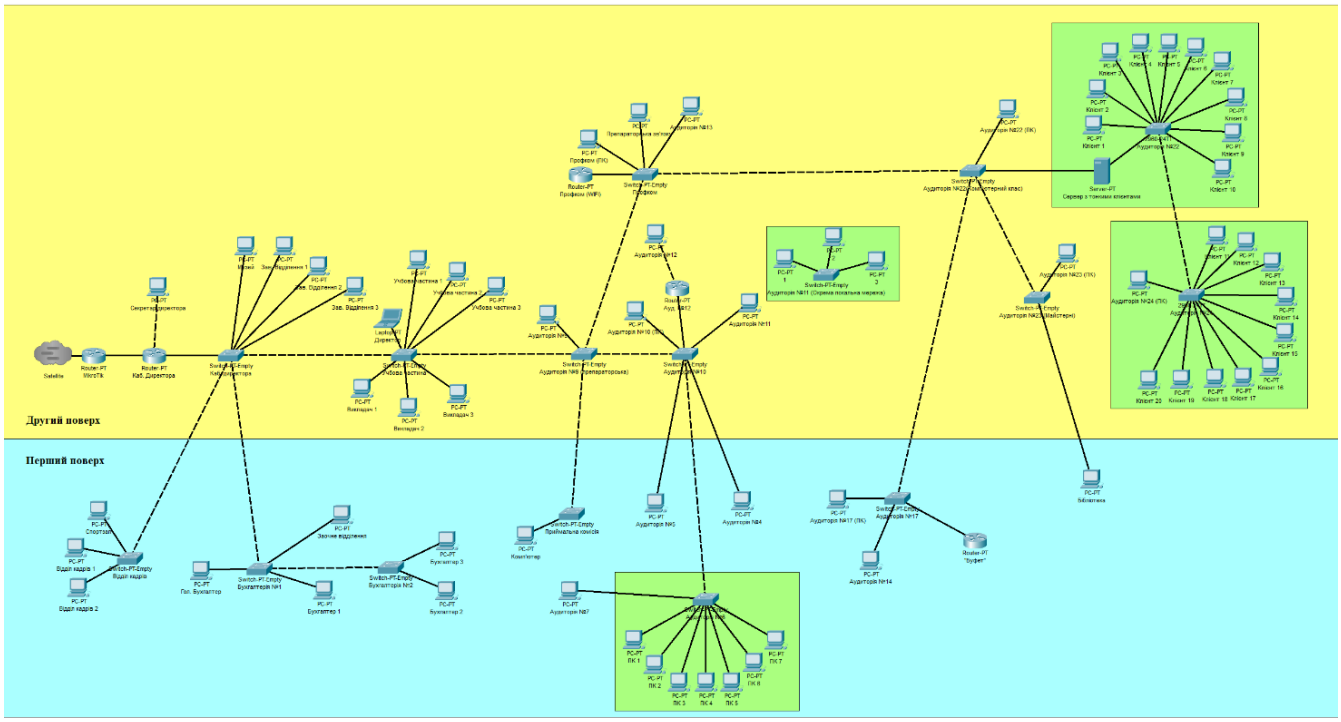

Рисунок 2.2 – Схема корпоративної мережі навчального закладу СФКТІ

Додатково слід зазначити, що з’єднання «End Devices» виконується за допомогою: витої пари категорії 5е - «OK-Net FTP кат.5е КППЭ-ВП»; Wi-Fi роутерів TL-WR841N V14; маршрутизатора MikroTik hAP lite (RB941-2ND); комутаторів на 8 портів TL-SF1008D; комутаторів на 16 портів TL-SG1016D [10-14].

Для огляду основних поверхів навчального закладу (поверхи першого та другого головного корпусу №2) була використана схема, створена в програмному забезпеченні Visio [9].

Рисунок 2.3 – План першого поверху

Починати огляд корпоративної мережі слід з другого поверху (рис. 2.4), адже там знаходиться обладнання провайдера ONU термінал. Він необхідний для перетворення оптичних сигналів в електричні сигнали через оптоволоконний кабель.

Після ONU розташовано головний маршрутизатор мережі MikroTik. В корпоративній мережі навчального закладу налаштовано SNAT з параметром Masquerade. Masquerade - це метод NAT, який дозволяє приховати реальні IP-адреси пристроїв внутрішньої локальної мережі та змінити їх на загальну IP-адресу для зовнішньої мережі. Masquerade – самостійно шукає і прописує IP-адресу присвоєну провайдером.

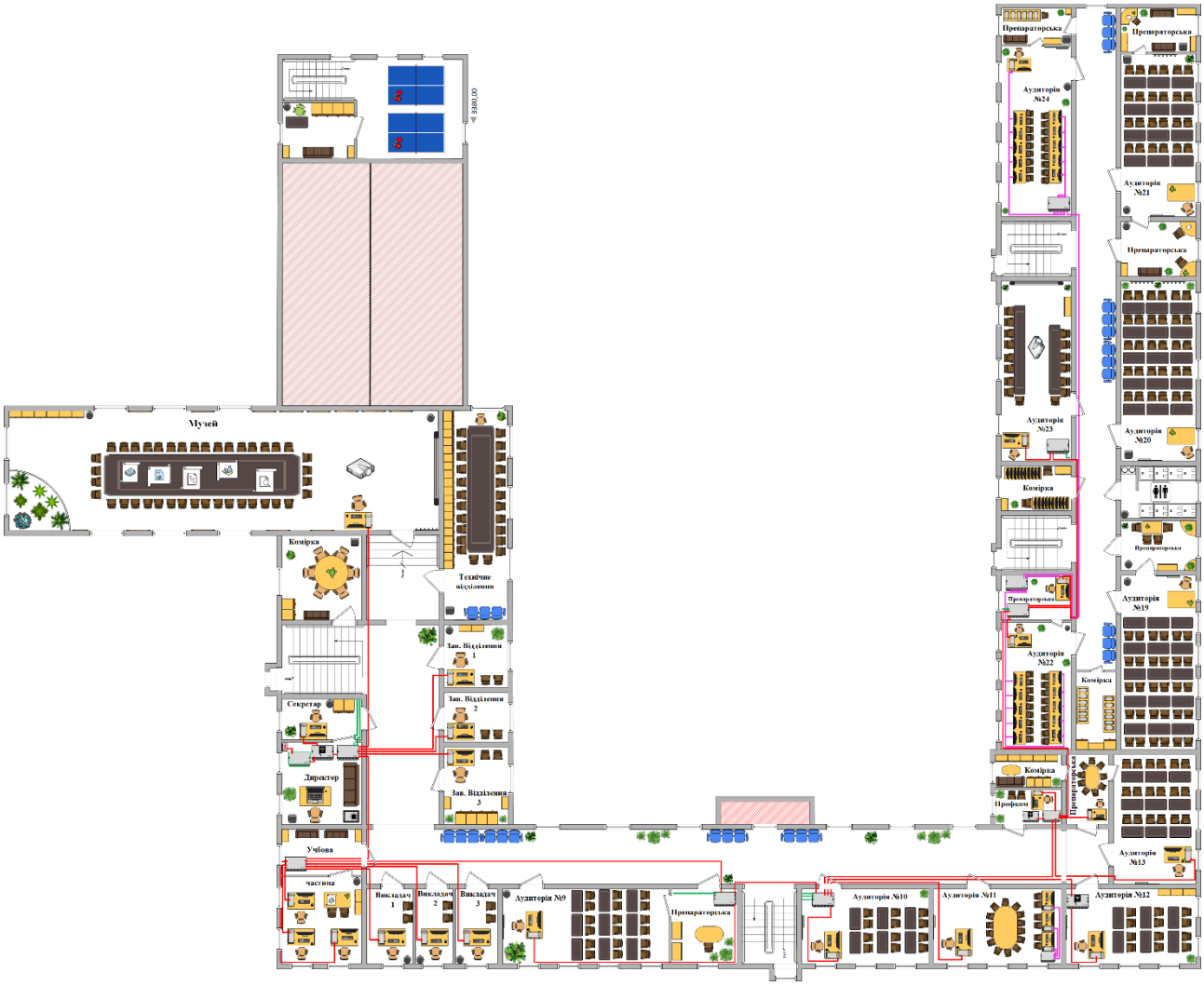

Рисунок 2.4 – План другого поверху

Нормальне функціонування мережі залежить від налаштувань безпеки, тому на маршрутизаторі MikroTik налаштовані правила Firewall:

1) Перше правило одночасно дозволяє Established (коли пакет вже встановив з'єднання, спілкується та все добре працює) і Related (це зв'язне з'єднання, тобто посередник) для – «input» і «forward». Це правило потрібно для того, щоб налаштувати Firewall на роботу лише з новими пакетами. Все, що вже не нове і з чимось взаємодіє – вже не вимагає перевірки.

2) Друге правило для пакетів Invalid , для - «input» і «forward». Це робиться для того, щоб пакети Invalid (поламані пакети, які не призначені маршрутизатору, або поламалися у процесі доставки) – були відкинуті.

3) Третє правило стосується сервісів віддаленого доступу до MikroTik. Усі порти управління, які є – закриваємо.

На рисунку 2.5 більш детально показано кабінет директора, на якому показано підключення зовнішнього проводу провайдера Satellite та розташування маршрутизатора MikroTik. Маршрутизатор виділено зеленим контуром.

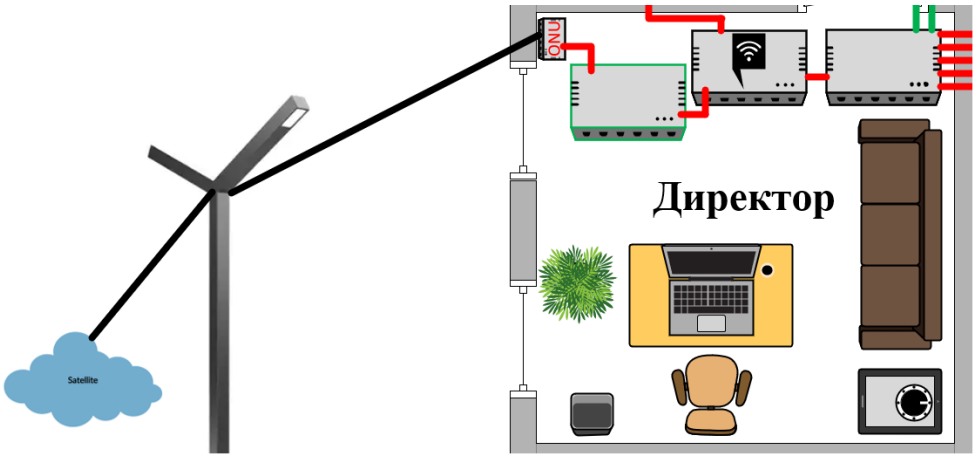

Рисунок 2.5 – Кабінет директора

Для полегшення відслідковування який провід куди йде було використано палітри кольорів: зелений – вита пара першого поверху; червоний – вита пара другого поверху; фіолетовий – окремі локальні мережі, які не мають підключення до корпоративної мережі і працюють окремо (рис. 2.6).

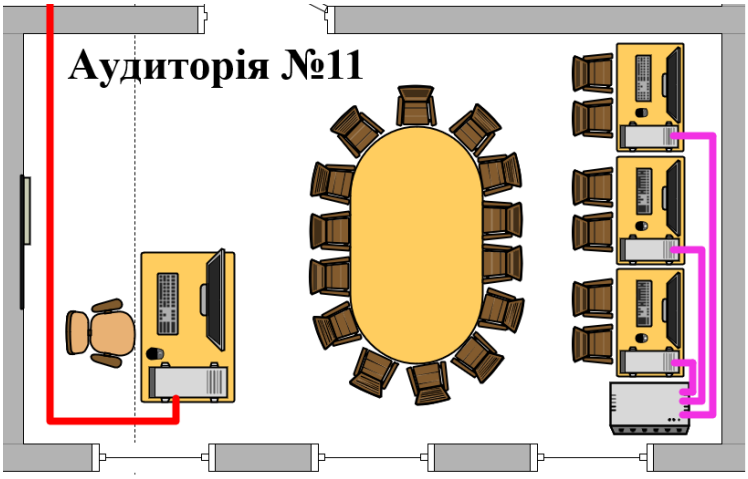

Рисунок 2.6 – Приклад аудиторії №11

Завдяки візуалізації, дистанційному моніторингу, тестуванню швидкості та моделюванню мережі можна провести дослідження стану корпоративної мережі навчального закладу. Це дозволяє оцінити та виявити існуючі проблеми перед модернізацією. Таким чином, завдяки спеціалізованим програмам виконується аналіз на можливість введення нових технологій в навчальні заклади.

2.2 Аналіз мережі за допомогою програмних засобів

Аналіз поточного стану начального закладу слід починати з діагностики мережі. Цей етап є ключовим для виявлення слабких місць та можливих проблем, наприклад, відсутність зв’язку, поганий зв’язок з головним маршрутизатором або сервером, затримка надходження повідомлень, низька пропускна здатність. Діагностика дозволяє оцінити продуктивність та безпеку всієї мережі в цілому, окрім технічних аспектів. Процес діагностики повинен охоплювати декілька етапів:

− дослідження трафіку;

− дослідження безпеки та тестування на проникнення;

− можливість масштабування мережі для введення нових технологій;

− перевірку мережевих налаштувань.

Одним з методів для аналізу мережі - є використання спеціальних утиліт, які допомагають системним адміністраторам контролювати всі данні корпоративної мережі організації [4]. Завдяки спеціальним програмам адміністратори мають змогу діагностувати мережі в будь-якій точці закладу.

Далі детальніше розглянемо дві програми, за допомогою яких виконувалася діагностика мережі навчального закладу СФКТІ.

2.2.1 Wireshark

Wireshark (стара назва Etherea) - це аналізатор мережевих протоколів. Він дозволяє перехоплювати та інтерактивно переглядати трафік, що проходить

через корпоративну мережу. Він має різноманітний набір функцій і є найпопулярнішим у світі інструментом такого типу [5]. Аналіз трафіку у цій програмі дозволяє зрозуміти: як використовуються мережеві ресурси, які протоколи використовуються, чи є втрата пакетів, які користувачі використовують більше трафіку.

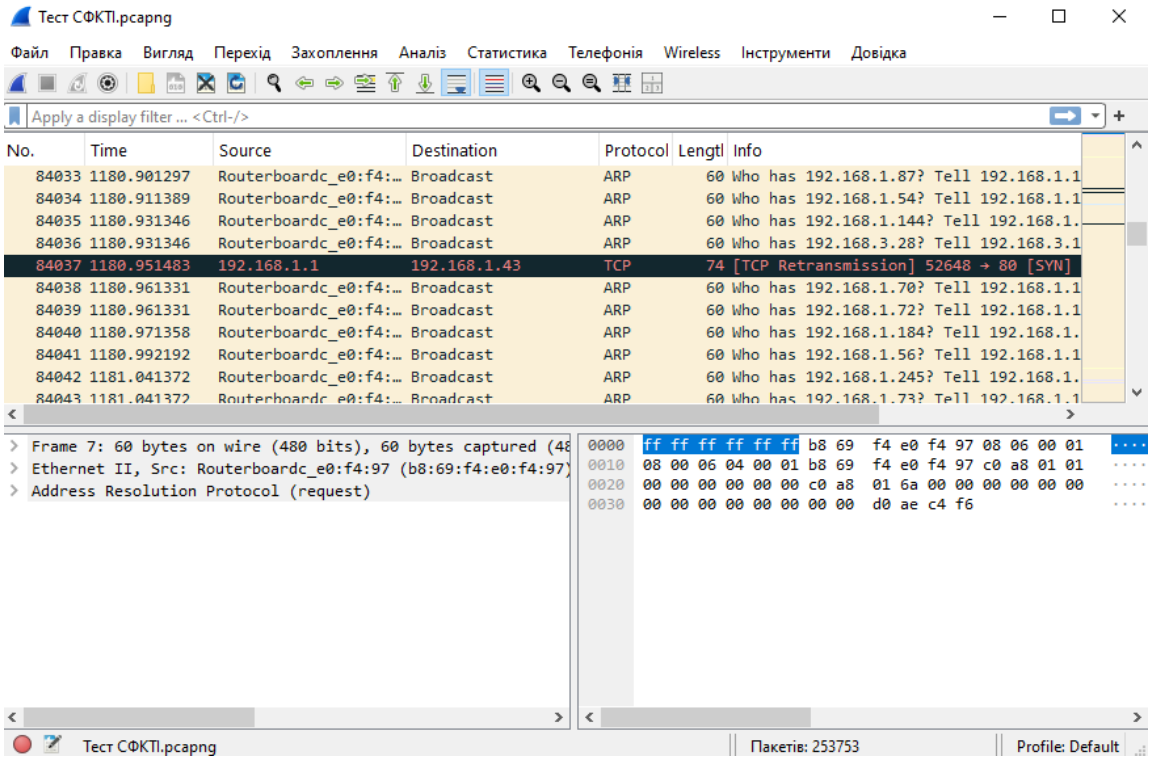

Рисунок 2.7 – Перегляд пакетів в мережі СФКТІ

На рисунку 2.1 можемо спостерігати пакети всієї мережі навчального закладу. Дослідження проводилося в період найменшого навантаження на мережу, доказ цього – це маршрутизатор MikroTik, з IP-адресою 192.168.1.1, який шукає пул адресів за допомогою протокола ARP. Це свідчить, що в корпоративній мережі є DHCP-сервер, який налаштований на окремі пули з прив’язкою MAC-адрес.

На рисунку 2.2. показано нормальну роботу по tcp протоколу, який передає дані на IP-адресу 192.168.1.51, це ноутбук який розташовувався в бухгалтерії закладу. Саме через нього і перевірялася робота корпоративної мережі з новими

приладами, що підтвердило легку масштабованість мережі. Спрацьовували налаштування MikroTik, а саме Firewall, де прописані правила стосовно нових підключень та пакетів. А саме: обмеження пропускної здатності, заборона доступу до інтернету, та відкидання поламаних пакеті.

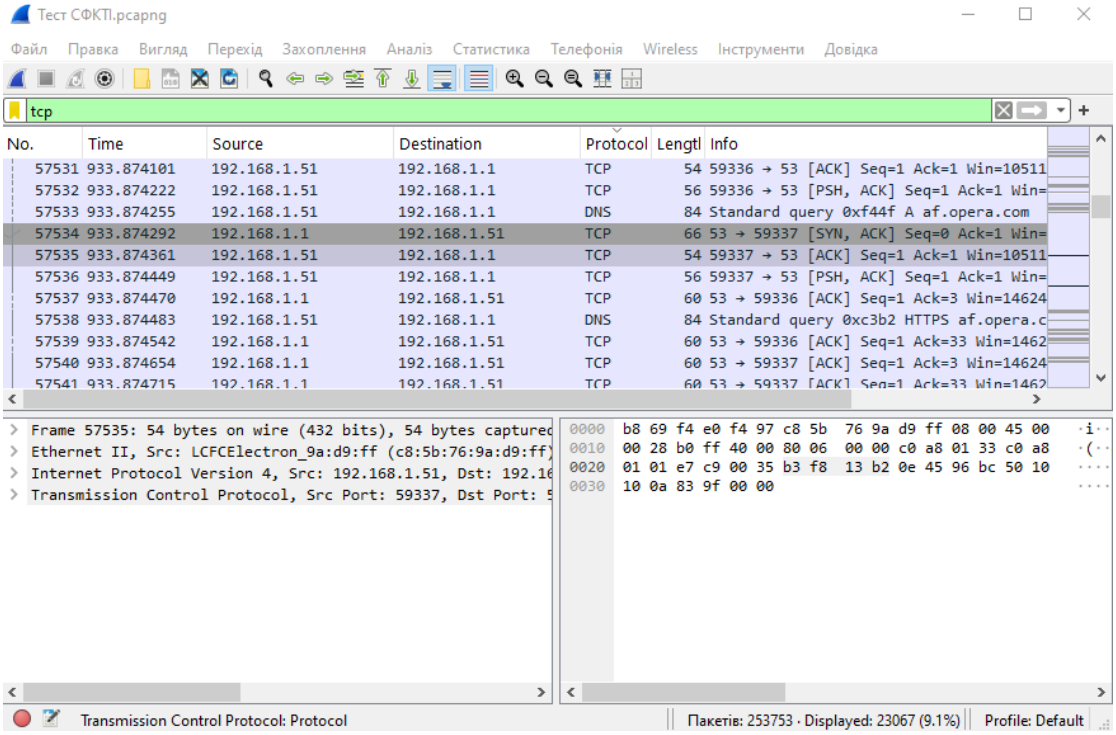

Рисунок 2.8 – Перегляд нових з’єднань в мережі СФКТІ

На рисунку 2.9 приведена діаграма помилок tcp пакетів корпоративної мережі. Помилки мінімальні та допустимі, нижче 1% [6].

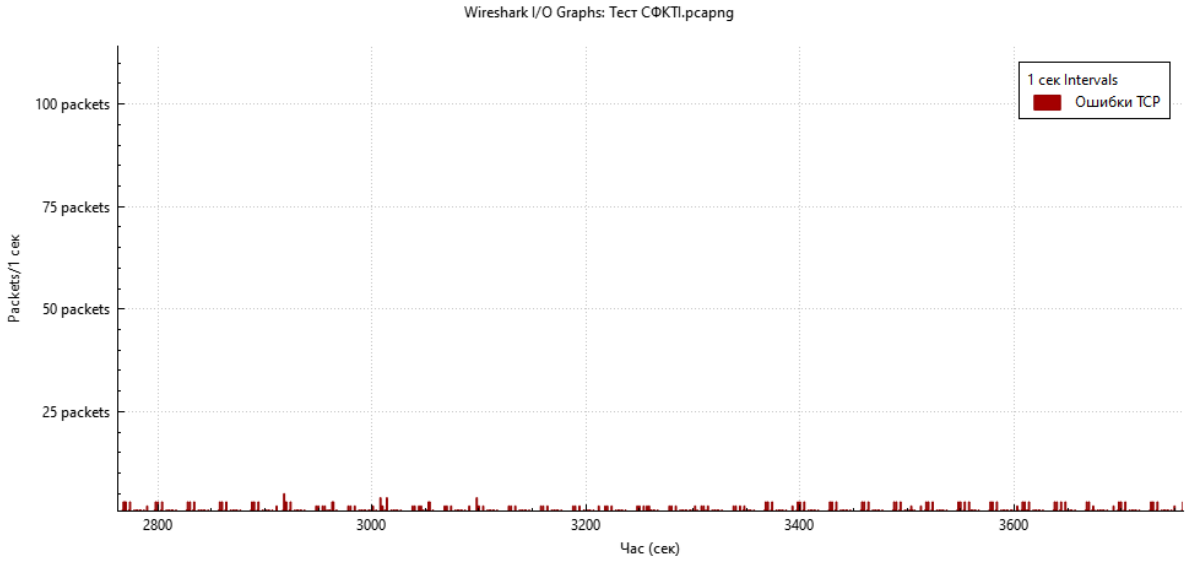

Рисунок 2.9 – Діаграма помилок tcp пакетів

Підведення результатів дослідження показано на рисунку 2.10, де стисло зображено статистику та результати роботи програми Wireshark.

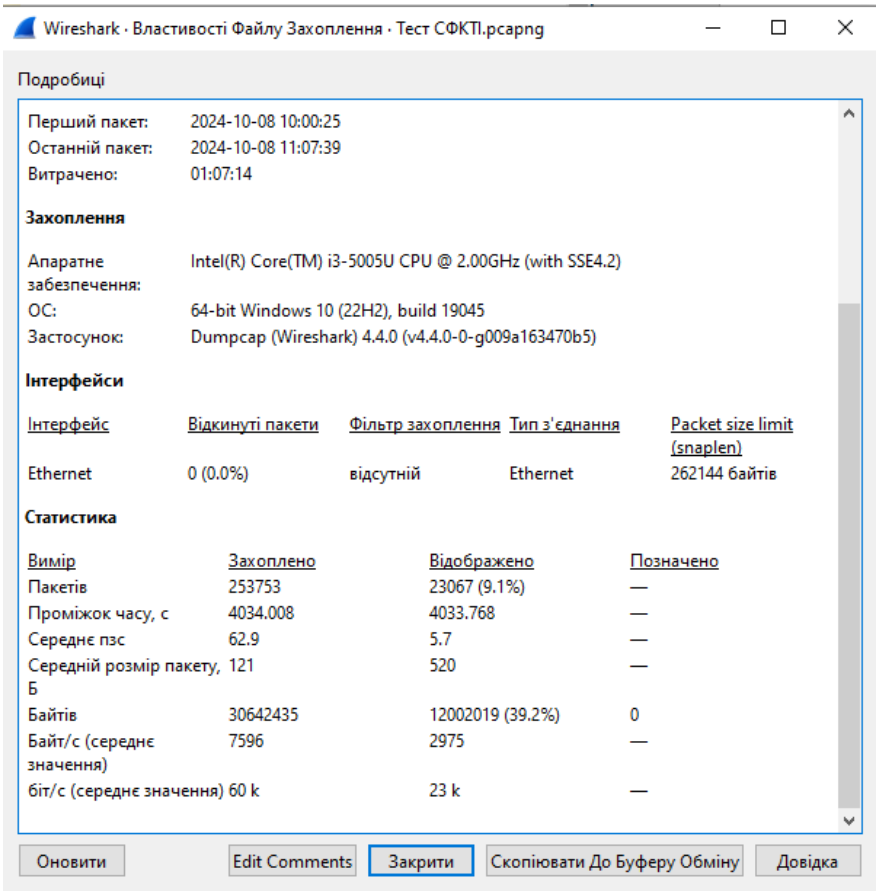

Рисунок 2.10 – Загальна інформація дослідження

2.2.2 iPref

iPref – це інструмент, який дозволяє замірити максимальну пропускну здатність між двома вузлами мережі. Ця програма вміє генерувати трафік різного типу, підтримується багатопотокова робота. iPref підтримує налаштування різних параметрів, пов'язаних з таймінгом, протоколами і буферами [7].

Щоб розпочати дослідження максимальної пропускної здатності мережі, для більшої точності потрібно вимкнути інші «End Devices», та на одному ПК налаштувати параметр «сервер», а на іншому ПК налаштувати параметр «клієнт».

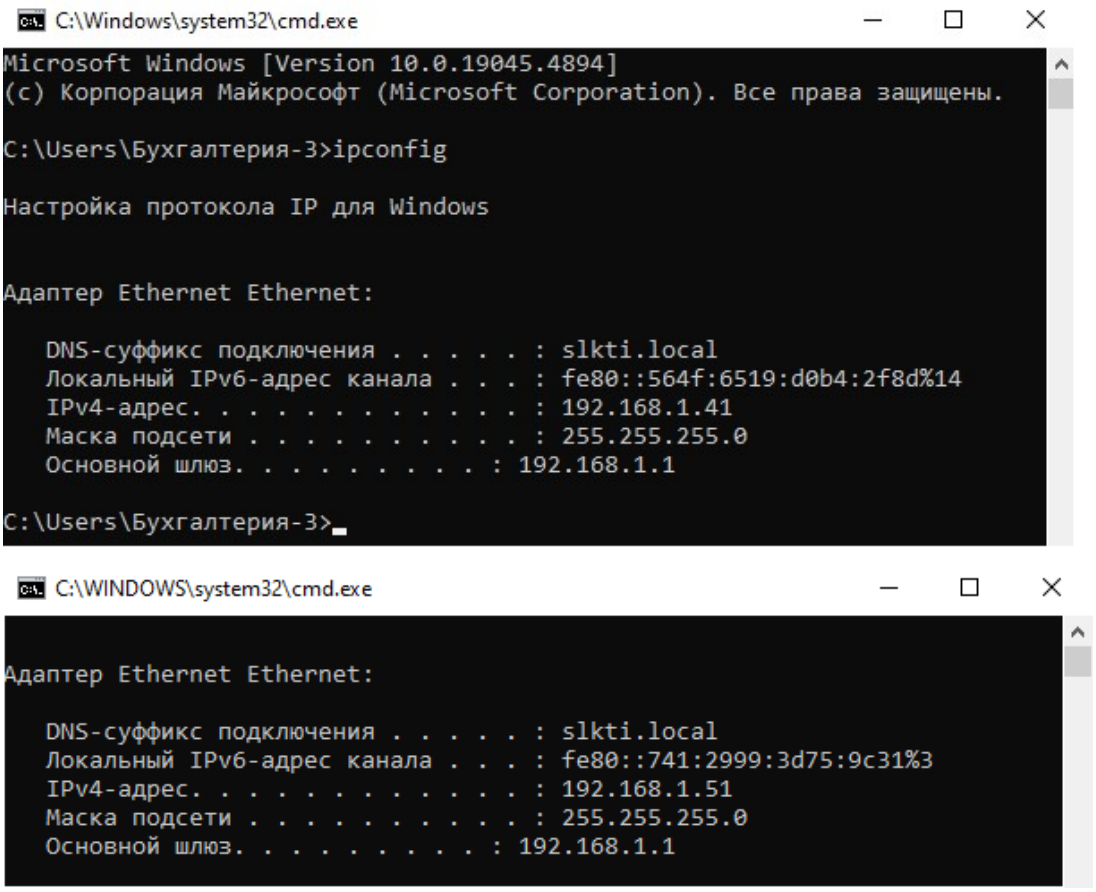

Рисунок 2.11 – Відображення конфігурації мережі

Для подальшого тестування потрібно дізнатися конфігурацію комп’ютерів. Дізнатися можна за командою «ipconfig», де 192.168.1.51 – клієнт, а 192.168.1.41 – майбутній сервер. Для подальшого налаштування потрібно відрити «cmd» та прописати шлях до програми за допомогою команди «cd».

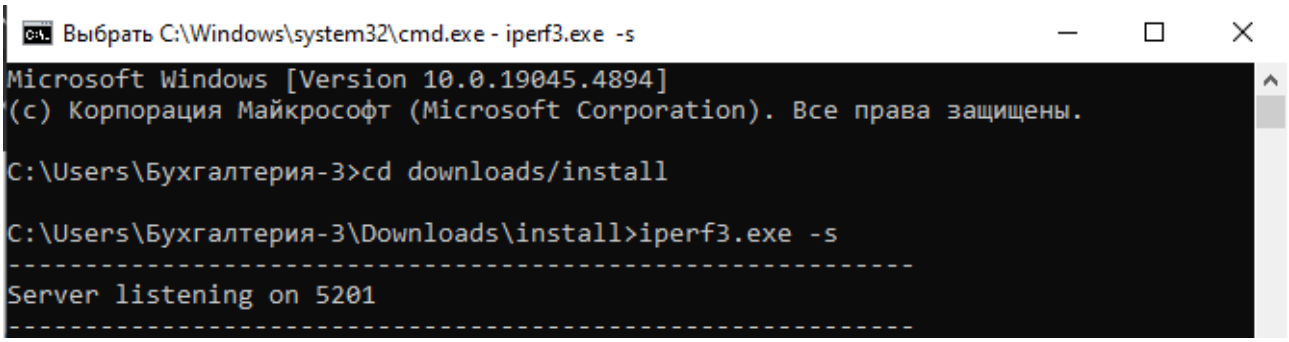

Рисунок 2.12 – Налаштування програми на ПК-сервері

За допомогою команди «ipref3.exe -s» виконується автоматичне налаштування комп’ютера в якості сервера (рис. 2.12), після чого вже налаштовується ПК-клієнт та виконується підключення.

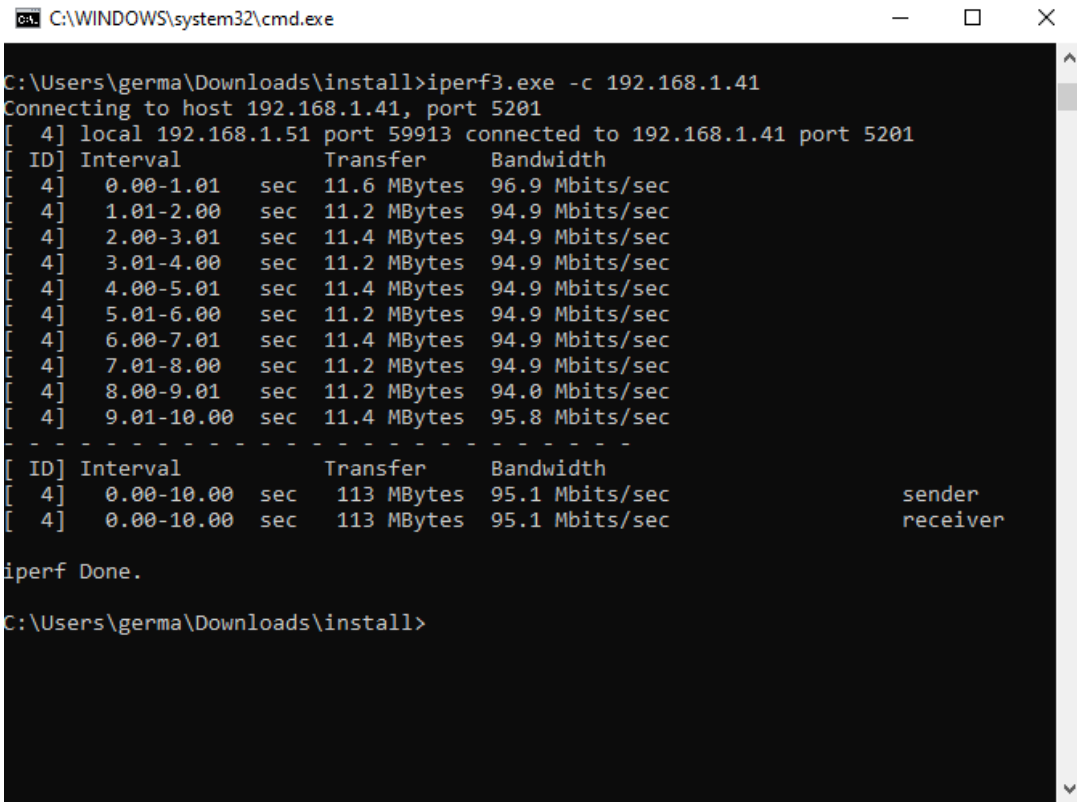

Рисунок 2.13 – Налаштування програми на ПК-клієнті

Підключення до серверу виконується за допомогою команди «ipref.exe -c 192.168.1.41». Програма розпочинає дослідження та сбір даних між вузлами, показуючи швидкість максимальну та обмежену, яка корегуються налаштуванням маршрутизатора MikroTik, та затримку. Спостерігаючи за пропускною здатністю (bandwidth) можна зробити висновок про максимально допустиму швидкість обробки трафіку мережної карти, яка встановлена в комп'ютерах корпоративної мережі навчального закладу, що дає змогу оцінити можливості майбутньої модернізації з можливістю часткової заміни обладнання, або збереженням старого.

3 МОДЕРНІЗАЦІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ СФКТІ

В результаті огляду корпоративної мережі СФКТІ, проведеному у другому розділі, можна зробити такі загальні висновки:

– комп’ютери відповідають нормам та технічним характеристикам, стосовно пропускної здатності;

– мережа функціонує нормально, без затримок, без втрат;

– топологія мережі – деревоподібна;

– головний маршрутизатор MikroTik налаштований правильно, з певними правилами Firewall;

– керування та зміна конфігурації мережі можлива лише з кабінету директора, там розташований маршрутизатор MikroTik та оптичний термінал провайдера з виходом в інтернет;

– IP-адреса для виходу в інтернет – статична, яка використовує одну загальну публічну IP-адресу;

– мережа включає в себе 4 комп'ютерні класи: 2 комп'ютерні класи с тонкими клієнтами та сервером; 1 комп'ютерний клас відокремлений від мережі (окрема локальна мережа без доступу в інтернет); 1 комп’ютерний клас з повноцінними комп’ютерами;

– мережа підтримує модернізацію та розширення.

Дослідження корпоративної мережі навчального закладу СФКТІ довели, що модернізація можлива. Для підвищення безпеки буде розроблена мережа відеоспостереження, яка дозволить здійснювати моніторинг в режимі реального часу та аналізувати події, архівувати записи для подальшого використання, це покращить безпеку обладнання та студентів. Окрім цього, для покращення автоматизації та підвищення ефективності процесу навчання буде організований веб-сервер (локальна бібліотека) з доступом до навчальних матеріалів та онлайн-тестів.

3.1 Створення системи відеоспостереження

Створення системи відеоспостереження в корпоративній мережі навчального закладу – це важливий крок для підвищення рівня безпеки студентів та викладачів. Відеоспостереження дозволяє в режимі реального часу спостерігати за поведінкою студентів та викладачів на занятті або перерві, спостерігати за майном закладу та переглядати що відбувається в навчальному закладі, зберігати відеозаписи для аналізу й реагувати на інциденти які дуже часто трапляються з студентами.

Камери можуть бути встановлені у стратегічно важливих місцях закладу: на входах і виходах, в коридорах, біля аудиторій, на території закладу і в зонах підвищеного ризику (наприклад, у лабораторіях або комп'ютерних класах). З попереднього дослідження стало зрозуміло, що система відеоспостереження може працювати в існуючій корпоративній мережі.

Для впровадження відеоспостереження потрібно виконати певні умови, які необхідні для нормального функціонування системи.

– Створення системи відеоспостереження починається з вибору камер, адже це основний компонент системи, які розрізняються за формою та підключенням. Підключення IP-камер відбувається за допомогою дротів (вита пара або коаксіальний) та технології Wi-Fi. За формою IP-камери бувають купольні та циліндричні.

Купольні – добре підходять для внутрішнього користування, тобто у приміщеннях, легко інтегруються в дизайн кімнати та забезпечують широкий кут огляду за допомогою чого можуть легко масштабувати зображення.

Циліндричні – встановлюються на вулиці, оскільки мають кращий захист від навколишнього середовища. Циліндричні камери розраховані на нічну зйомку та в свою чергу можуть охоплювати далекі відстані, але в кімнатах їх краще не ставити, вони мають менший кут огляду.

– Система відеоспостереження повинна працювати в існуючій корпоративній мережі навчального закладу СФКТІ. Не мати виходу в інтернет та підключатися до NVR та VMS.

NVR (Network Video Recorder) – це мережевий відеореєстратор, який використовують для зберігання та управління відеозаписами з IP-камер. NVR отримує відеосигнал безпосередньо від IP-камер через локальну мережу. Він не підключається до камер безпосередньо через кабель, як це відбувається з аналоговими системами, а використовує протоколи передачі даних RTSP або ONVIF. Тобто, не потрібно підключати кожну камеру до NVR, з'єднання відбувається через один провід який під'єднується до мережі. NVR має вбудоване або зовнішнє сховище даних (в вигляді резервного копіювання на хмарний сервіс), яке може бути у вигляді накопичувачів HDD та SSD. Для підвищеного захисту, краще ховати NVR в сейф або щось подібне, бо це перше що шукають зловмисники. Також потрібно подбати про безперебійне живлення, яке забезпечить роботу пристрою у випадку тривалого відключення [15].

VMS (Video Management System) – це програмне забезпечення для управління системами відеоспостереження, яке дозволяє моніторити, записувати, зберігати і аналізувати відеопотоки, що надходять від IP-камер спостереження. Основна роль VMS полягає у створенні централізованої платформи для керування великою кількістю камер та доступу до відеоданих в режимі реального часу або архівних записів [16].

– Ефективність роботи системи відеоспостереження залежить від правильного підключення її до мережі живлення. Це забезпечує стабільність роботи камер і всього обладнання, запобігає збоям у роботі системи, втраті відеоданих і зменшує ризик виникнення аварійних ситуацій. Для підключення живлення IP-камер в системі є два основні способи: за допомогою блоку живлення або за допомогою PoE.

Power over Ethernet (PoE) дозволяє одночасно передавати живлення та дані через один Ethernet-кабель. Для цього використовуються спеціальні PoE-комутатори або PoE-адаптори, які забезпечують живлення камери через

мережевий кабель. Якщо з'являється питання про безперебійне живлення, то до PoE-комутатора можна під'єднати резервне живлення, яке стане в нагоді при раптовому зникненні світла, що підвищить відмовостійкість системи відеоспостереження [17].

Проводка для системи відеоспостереження повинна бути правильно прокладена з урахуванням електромагнітних хвиль, які заважають коректно без перешкод передавати сигнал на VMS та NVR.

У таблиці 3.1 наведено порівняння блоку живлення і PoE-адаптора.

Таблиця 3.1 – Відомості про порівняння блоку живлення і PoE-адаптора

Параметр	Блок живлення	PoE-адаптор
Кількість кабелів	Потрібен окремий кабель для живлення та окремий кабель для передачі даних	Один Ethernet-кабель для живлення і передачі даних
Дальність передачі живлення	Обмежена, особливо для довгих кабелів	До 100 метрів без втрати якості
Складність установки	Потрібна окрема проводка для живлення	Менша кількість кабелів, простіша інсталяція
Зручність для великомасштабних систем	Менш зручний через велику кількість кабелів	Ідеальний для великої кількості камер
Вартість	Дешевші блоки живлення, але складніша інсталяція	Дорожче обладнання, але простіша інтеграція

3.2 Вибір обладнання для системи відеоспостереження

Система відеоспостереження буде побудована в навчальному закладі СФКТІ м. Слов'янськ.

Перш за все потрібно подбати про живлення IP-камер та їх легке масштабування. Для цього було 5-портовий PoE-комутатор TP-LINK TL-SF1005P, він має захист від перенавантажень та функцію пріоритетності портів: порт 1> порт 2> порт 3> порт 4 [18].

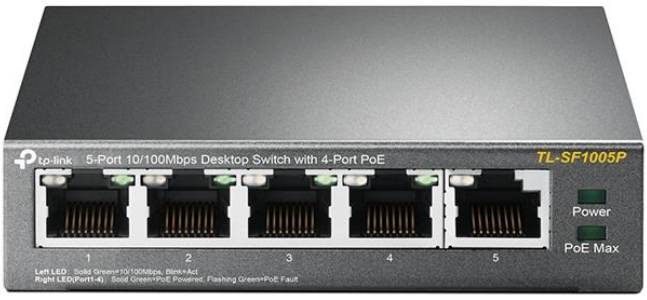

Рисунок 3.1 – TP-LINK TL-SF1005P

Для покращення безпеки обладнання та стратегічних відділів буде встановлено 8 купольних IP-камер Hikvision DS-2CD1321-I(F) [19].

Рисунок 3.2 – Hikvision DS-2CD1321-I(F)

Камери Hikvision DS-2CD1321-I(F) можуть розміщуватися як на вулиці так і в приміщеннях, що робить їх універсальними. Для підвищення функціоналу камер потрібно підключити їх до NVR, який буде виконувати запис на HDD. З цим завданням може справитися NVR Tiandy TC-R3108, він має вісім портів PoE-портів та підтримує запис з всіх камер одночасно. Також він має VMS, який підримує підключення камер від різних вендорів [20].

Рисунок 3.3 – NVR Tiandy TC-R3108

Жорсткий диск слід обирати з врахуванням того, що система буде працювати 24/7. Для цих цілей підійде HDD Western Digital Purple 1TB 64MB 5400rpm WD11PURZ. Ці диски розроблені спеціально для відеоспостереження, щоб допомогти витримати високі коливання тепла та вібрацію обладнання в середовищах NVR [21].

Рисунок 3.4 – HDD WD11PURZ

Для з’єднання камер між комутаторами та системою NVR буде використовуватися вита пара 5e - «OK-Net FTP кат.5e КППЭ-ВП». Для безперебійного живлення системи NVR буде використовуватися зарядна станція, яка зможе працювати з режимом UPS, а саме Bluetti EB3A. Ця станція розрахована на 268 Вт/год, що дає змогу працювати NVR декілька днів без світла та підтримувати безпеку навчального закладу [22].

Рисунок 3.5 – Bluetti EB3A

3.3 Встановлення та налаштування системи відеоспостереження

Після того як обладнання підібране, можна його встановлювати на місця узгодженого з керівником підприємства. Згадуючи функціонал MikroTik, ми можемо створити ще одну мережу. Це потрібно для того, щоб захистити IP-камери від внутрішнього перегляду сторонніх осіб, адже кожний користувач може перебрати IP-адреси та знайти камеру. Тобто-то адреса корпоративної мережі 192.168.1.0, мережа відеоспостереження 192.168.0.1.

Тестування роботи камер проводились в середовищі Cisco Packet Tracer, результати роботи наведені на рисунку 3.6.

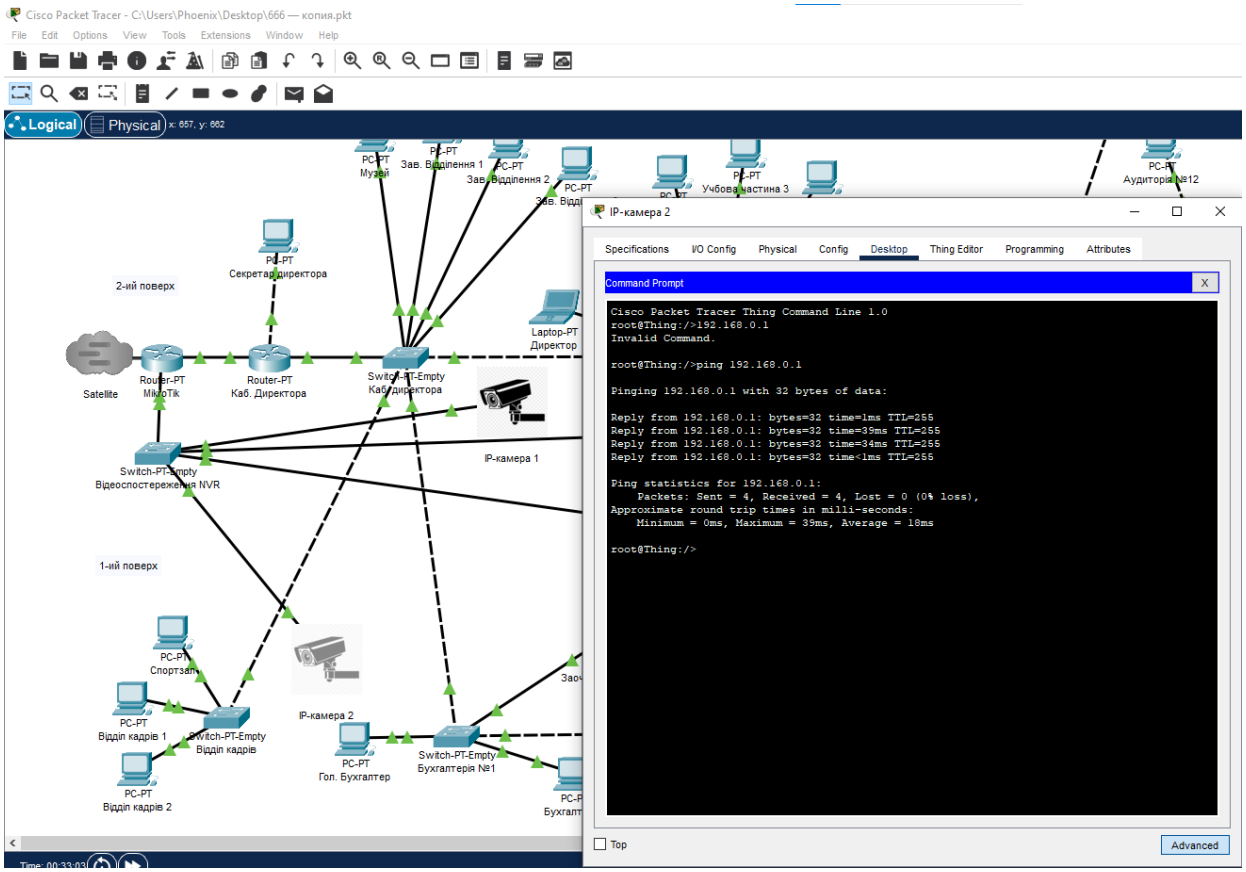

Рисунок 3.6 – Робота IP-камер в мережі 192.168.0.1

Коли мережа буде створена та встановлена на місця за планом, потрібно налаштувати IP-камери на NVR, а саме прописати статичні IP-адреси.

Після налаштування IP-камер потрібно подбати про безпеку NVR. NVR – буде розміщено в сейфі директора, це створить додаткові проблеми для відключення його зловмисниками, також в сейфі розміщуємо Bluetti EB3A. Віддалене керування буде здійснюватися за допомогою локальної адреси до якої підключено відеоспостереження. Для додаткової безпеки NVR буде записувати інформацію в два етапи: запис на HDD та запис в хмарне середовище Google Drive [23].

Оновлена схема корпоративної мережі після її модернізації за допомогою відеоспостереження наведена на рисунку 3.7.

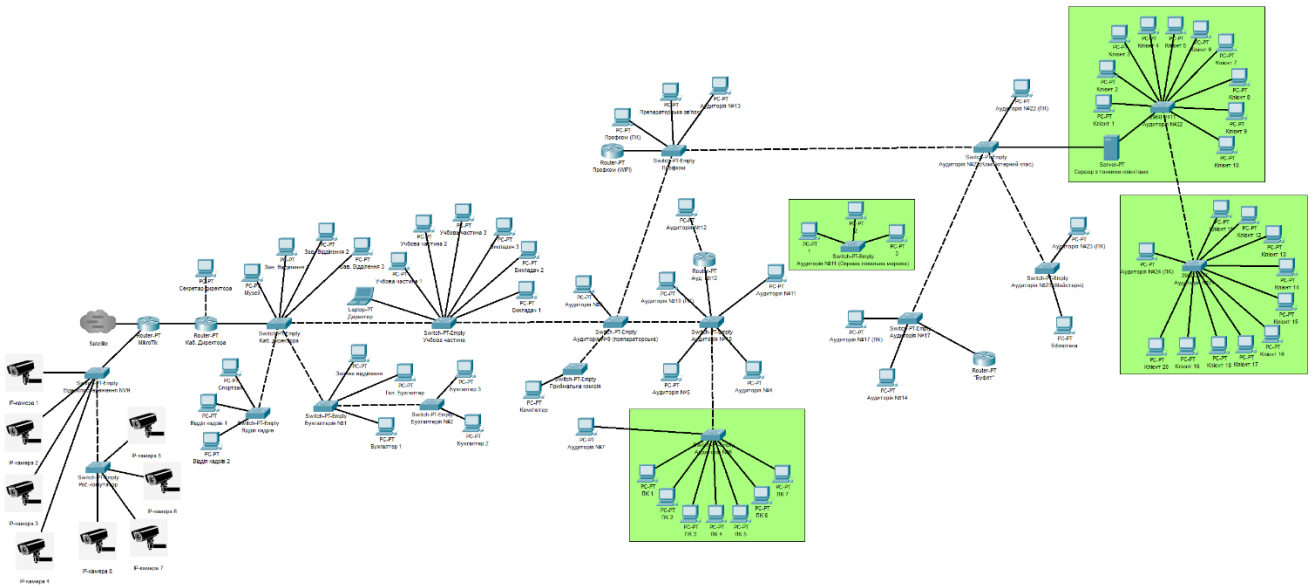

Рисунок 3.7 – Оновлена схема корпоративної мережі СФКТІ

IP-камери будуть розташовані на першому та другому поверсі. Це обумовлено тим, що всі важливі місця знаходяться саме там (комп’ютерні класи та адміністративні кімнати).

Схема живлення відеоспостереження розбита на два етапи.

– Перший етап, це живлення від самого NVR. NVR має 8 портів, які підтримують технологію PoE, але є проблема, це довжина будівлі. Вита пара має обмеження для передачі сигналу (максимум 100 м), тому необхідно ставити регенератор сигналу.

– Другий етап, це PoE-комутатор TP-LINK TL-SF1005P, який буде грати роль регенератора. Він має п’ять портів, їх буде достатньо для підключення IP-камер які знаходяться на великій відстані від NVR.

Схема відеоспостереження для першого та другого поверху показана на рисунку 3.8 та 3.9.

Рисунок 3.8 – Схема відеоспостереження для другого поверху

На рисунку 3.8 та 3.9 можна побачити підключення та розташування купольних IP-камер Hikvision DS-2CD1321-I(F): червоний – IP-камера 1; жовтий – IP-камера 2; синій – IP-камера 3; зелений – IP-камера 4; рожевий – IP-камера 5; коричневий – IP-камера 6; чорний – IP-камера 7; сірий – IP-камера 8; фіолетовий – з’єднання NVR та PoE-комутатора.

Рисунок 3.9 – Схема відеоспостереження для першого поверху

4 ОРГАНІЗАЦІЯ ВЕБ-СЕРВЕРА З БАЗОЮ ДАНИХ

Прогрес не стоїть на місці, відкриваються нові знання, нові технології, сучасні умови спонукають до переосмислення підходів до навчання. Сучасні підходи повинні орієнтуватися на комбіновані методи навчання. Вони можуть бути дистанційними та очними, які включать підготовку через віддалену платформу, наприклад, віртуальні сервіси, які допомагають навчатися професійним навичкам [24].

4.1 Планування та вибір обладнання

Для автоматизації навчального процесу необхідно створити сервер-бібліотеку, на якому буде розміщено розділи для студентів та викладачів.

Розділ викладачів включає в себе: журнали для оцінок, з можливістю редагування; літературу для викладання предметів; робочі програми.

Розділ для студентів включає в себе: розклад сесії та навчального року; практичні програми для лабораторних та практичних робіт, які доступні лише для завантаження; електронна бібліотека.

Встановлення нового додаткового сервера є значною інвестицією, що потребує значних фінансових витрат, тому буде модернізація старого сервера, який налаштований під роботу тонких клієнтів. Оновлення наявного сервера дозволить не тільки розширити його функціонал, але й забезпечити необхідну підтримку інтерактивного навчання без зайвих витрат. А вже після проведення модернізації буде встановлено веб-сервер, який дозволяє розміщувати веб-програми та надавати доступ до файлів через HTTP.

Програмне забезпечення сервера залишається незмінним. Це Windows Server 2019 - платформа для створення інфраструктури підключених програм, мереж та веб-служб: від робочої групи до центру обробки даних [25].

В таблиці 4.1 наведені характеристики серверу навчального закладу СФКТІ.

Таблиця 4.1 – Характеристики серверу СФКТІ

Характеристика	Деталі
Процесор	Intel Core i7-3770, 4 ядра, 3.4 ГГц
Кількість потоків	8 (з підтримкою Hyper-Threading)
Оперативна пам'ять (RAM)	16 ГБ DDR3 (2 вільні слоти)
Жорсткий диск	HDD 1 ТБ SATA
Швидкість обертання HDD	7200 об/хв
Мережевий інтерфейс	Gigabit Ethernet
Живлення	Одинарний блок живлення 500 Вт
Розмір	Настільний корпус (можливо доопрацювати для стійки)
Операційна система	Windows Server 2019

4.2 Модернізація серверу СФКТІ

В результаті аналізу характеристик було прийнято рішення модернізації. Потрібно збільшити оперативну пам’ять та фізичну пам’ять, додаванням нових HDD та встановленням RAID масиву.

RAID-масив – це технологія, яка об'єднує кілька жорстких дисків або твердотільних накопичувачів (SSD) в єдиний логічний блок з метою підвищення надійності, швидкості або обсягу сховища [26].

Основні режими RAID-масивів:

– RAID 0 – підвищує швидкість доступу до даних за рахунок розподілу даних між дисками, але вихід з ладу одного диска призводить до втрати всіх даних;

– RAID 1 – створює повну копію даних на двох або більше дисках. Має високу надійність, оскільки дані дублюються, сховище дорівнює половині від загального обсягу всіх дисків;

– RAID 5 – потребує мінімум трьох дисків. Дані та контрольні суми розподіляються між усіма дисками, що дозволяє відновити інформацію в разі виходу з ладу одного з них. RAID 5 забезпечує баланс між швидкістю, надійністю та ефективністю використання місця;

– RAID 6 – схожий на RAID 5, але використовує подвійне резервування, дозволяючи зберегти дані навіть при виході з ладу двох дисків одночасно. Це покращує надійність, але потребує більше дисків;

– RAID 10 (1+0) – поєднує RAID 1 і RAID 0. Забезпечує як високу швидкість, так і надійність, але вимагає значних витрат пам’яті, оскільки половина обсягу використовується для дублювання.

В нашому випадку будуть використовуватися саме HDD з RAID масивом 5, а не SSD накопичувачі. Порівняльна характеристика наведена в таблиці 4.2.

Таблиця 4.2 – Порівняльні характеристики HDD і SSD

Характеристика	HDD	SSD
Швидкість читання/запису	Низька (100-200 МБ/с)	Висока (500 МБ/с і більше)
Час доступу до даних	Більший (через механічні компоненти)	Менший (немає рухомих частин)
Стійкість до механічних пошкоджень	Низька (чутливий до ударів)	Висока (немає рухомих частин)
Енергоспоживання	Більше (через рухомі частини)	Менше
Тривалість служби (знос)	Довше при активній роботі	Обмежена кількість циклів перезапису
Шум	Присутній (обертання шпинделя)	Відсутній
Ціна за гігабайт	Нижча	Вища
Обсяг пам'яті	До кількох десятків терабайт	Зазвичай до кількох терабайт

Для створення RAID масиву знадобляться два нових HDD. Було обрано Western Digital Purple 1TB 64MB 5400rpm WD11PURZ з третього розділу. Вони мають підтримку RAID, та ідеально підходять для довгострокової роботи.

Включення RAID 5 показано на рисунку 4.1, після чого обираються диски які потрібно об’єднати в масив та виконується об’єднання.

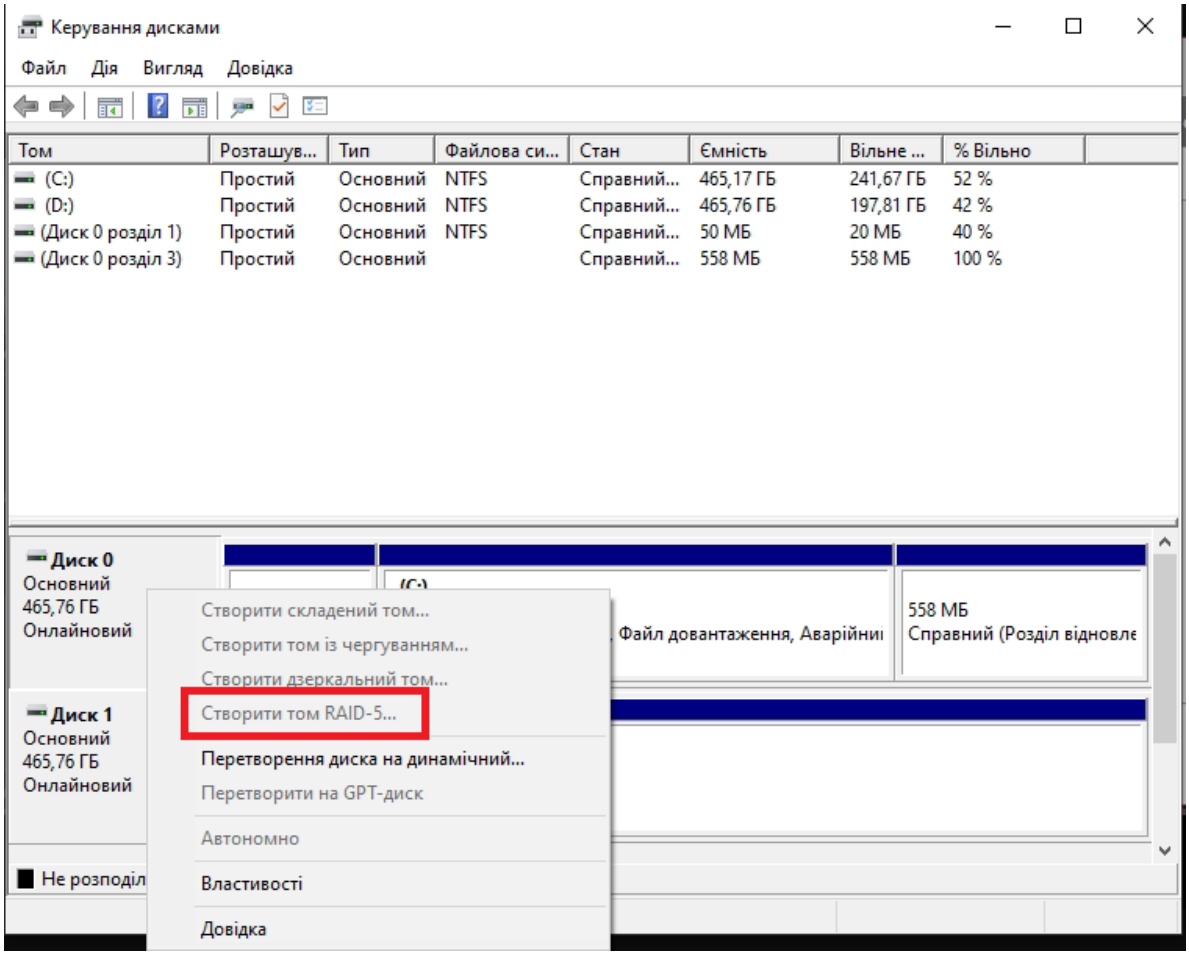

Рисунок 4.1 – Створення масиву RAID 5

Збільшення оперативної пам'яті необхідне для того, щоб сервер мав змогу швидше обробляти великі обсяги даних і витримувати більше навантаження. Чим більше ОЗУ, тим більше запитів і завдань сервер може обробляти одночасно. Якщо пам'яті не вистачає, сервер починає використовувати жорсткий диск як тимчасове сховище, що значно повільніше і може призвести до втрат ККД. Додавання ОЗУ дозволить підготувати сервер до майбутнього зростання

навантаження, забезпечуючи стабільну і безперебійну роботу навіть під час пікових навантажень.

Для модернізації ОЗУ було обрано дві плашки G.Skill DDR3 8GB 1600Mhz (F3-1600C11S-8GNT), це гарний варіант для сервера через свою стабільність, ефективну швидкодію та збалансовану вартість. Ця модель працює на частоті 1600 МГц, що є достатньо швидким показником для DDR3, і забезпечує плавну роботу більшості серверних задач, включаючи багатозадачність [27].

Рисунок 4.2 – G.Skill DDR3 8GB 1600Mhz (F3-1600C11S-8GNT)

4.3 Створення веб-сервера з базою даних

Для встановлення веб-сервера на вже налаштований сервер з тонкими клієнтами потрібно відкрити Server Manager. Server Manager – це головний інструмент для керування ролями та компонентами у середовищі Windows Server. У головному меню Server Manager потрібно натиснути на пункт Add Roles and Features (Додати ролі та компоненти). Це відкриє покроковий майстер, який допоможе додати необхідні функції.

У майстрі потрібно режим Role-based or feature-based installation (Встановлення на основі ролей або компонентів) та виберіть сервер зі списку. У розділі ролей знайдіть і позначте Web Server (IIS). На етапі вибору компонентів переконайтеся, що додані наступні опції:

– Directory Browsing (Дозволяє переглядати вміст каталогів через веб-браузер);

– Basic Authentication (Базова автентифікація для захисту доступу до ресурсу).

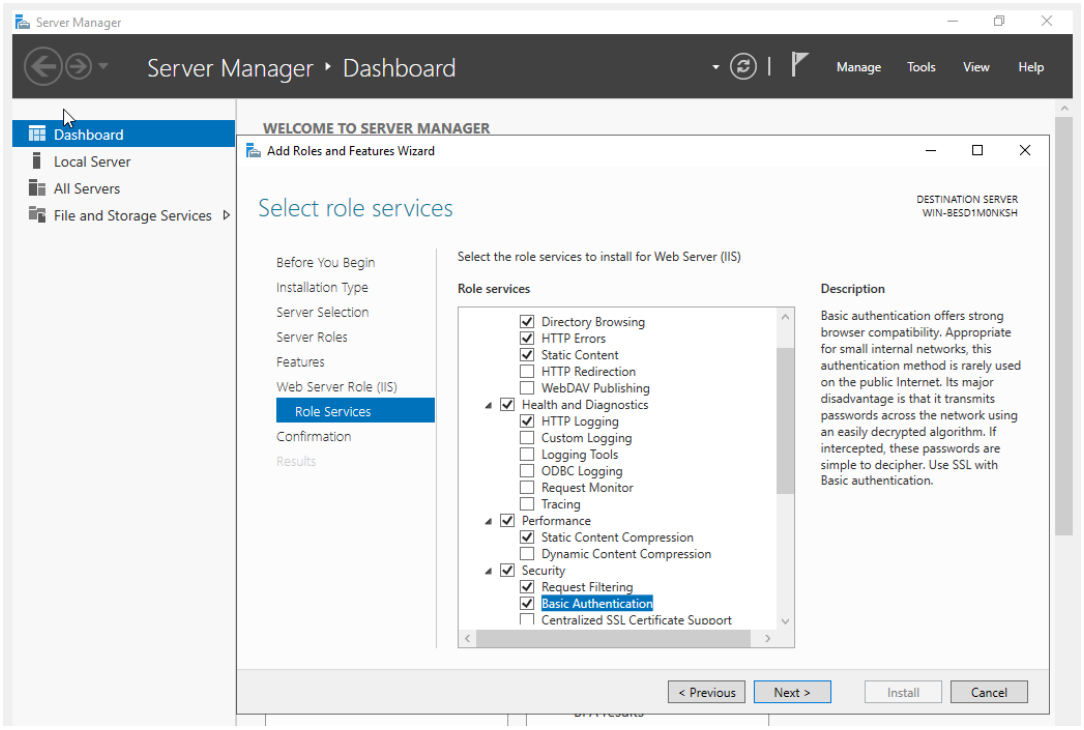

Рисунок 4.3 – Встановлення IIS на Windows Server

Після завершення потрібно перевірити, чи служба IIS успішно запущена.

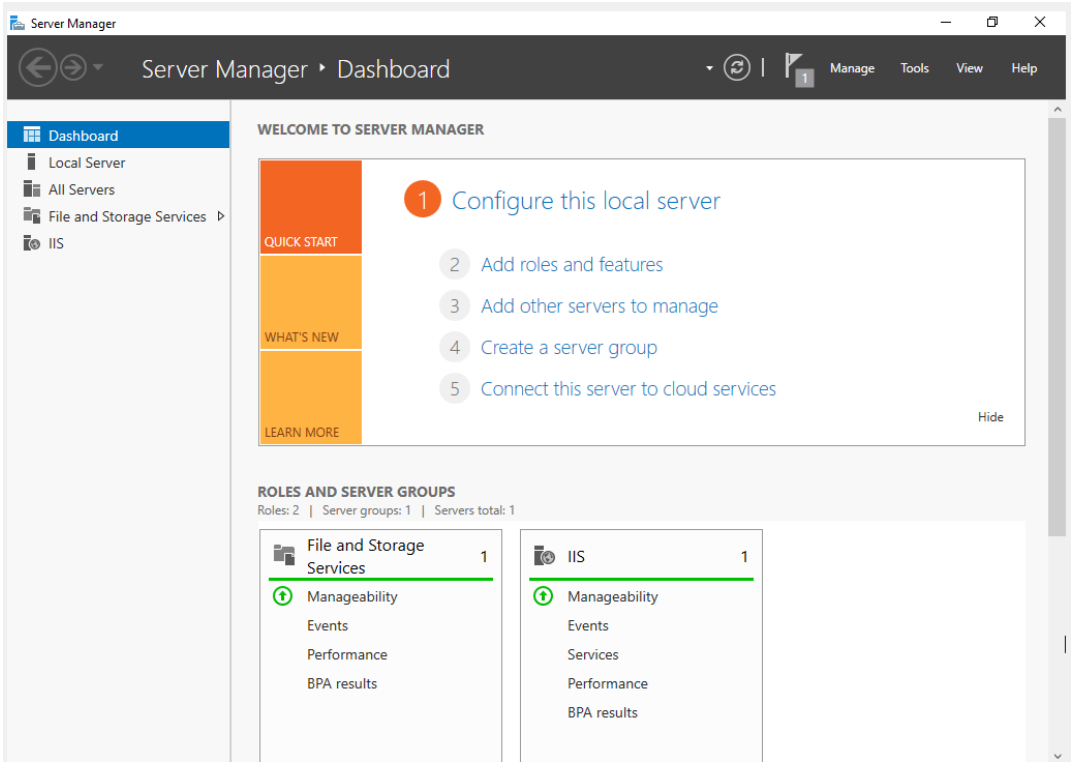

Рисунок 4.4 – Перевірка поточного стану IIS на Windows Server

Наступним кроком є створення локальних користувачів з різними рівнями доступу. Для цього потрібно відкрити Computer Management (Керування комп’ютером). Це можна зробити через меню "Пуск" або команду compmgmt.msc.

У лівій частині вікна переходимо до розділу Local Users and Groups → Users. Тиснемо правою кнопкою миші у вікні користувачів і обираємо New User.

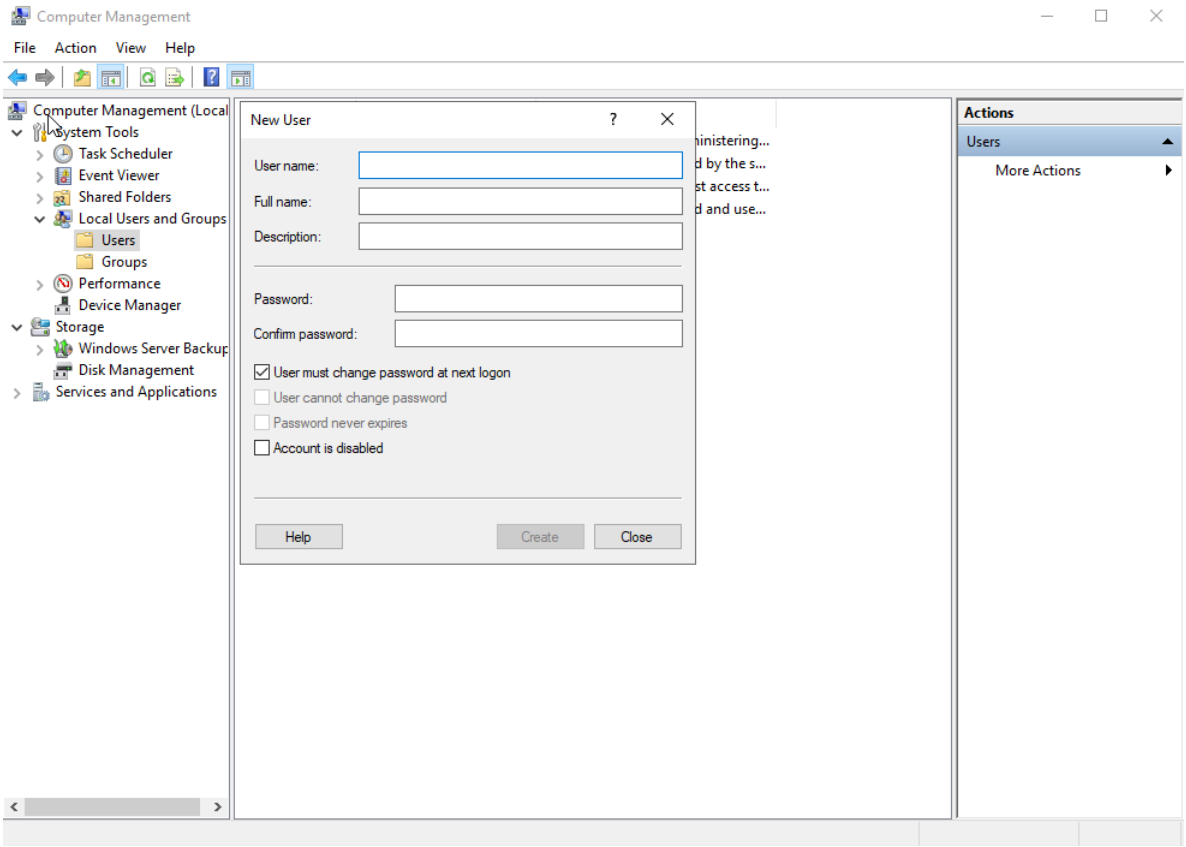

Рисунок 4.5 – Створення нового користувача в Computer Management

Для вчительського доступу необхідно прописати User name, встановити надійний пароль і зняти позначку з опції User must change password at next logon (Користувач має змінити пароль при наступному вході), адже логін та пароль буде однаковий для всіх викладачів. Сервер підтримує мультипідключення, а якщо з’явиться необхідність знайти «саботажника», то це можна зробити через налаштований пул адресів на MikroTik. Він покаже коли підключалися до бібліотеки ті чи інші користувачі корпоративної мережі.

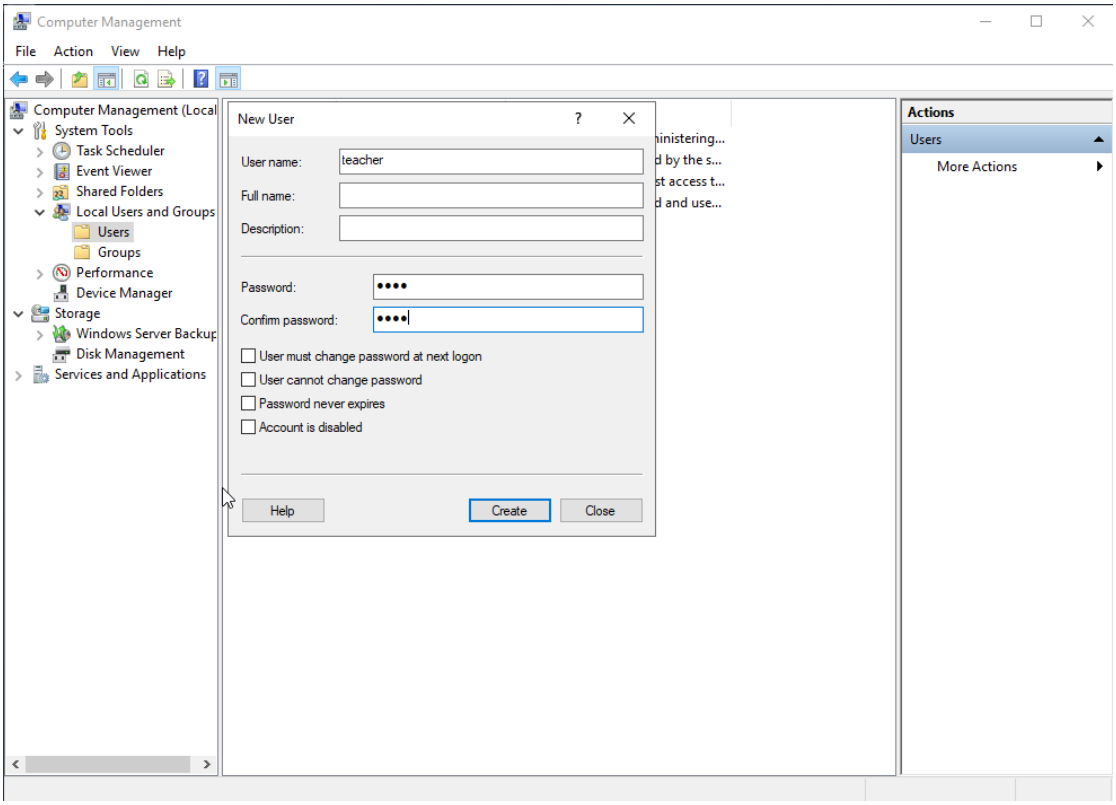

Рисунок 4.6 – Створення користувача teacher

Аналогічно створюється користувач student. Слід зазначити, що користувачі teacher та student мають обмежені права доступу. До локального диску С (налаштування програм та ОС) на сервері має доступ лише адміністратор корпоративної мережі. Бібліотека з журналами, робочими програмами та іншим необхідним матеріалом буде знаходитися на локальному диску D, третій диск E буде зарезервовано у зв'язку з використанням RAID масиву.

Для зберігання файлів, до яких матимуть доступ користувачі, необхідно створити відповідну папку. На локальному диску D необхідно створити папку з назвою Library.

Наступним кроком налаштовуємо права доступу. Тиснемо правою кнопкою миші на папці Library, оберємо Properties (Властивості) і переходимо на вкладку Security (Безпека).

У розділі налаштування доступу додайте створених користувачів:

– Для teachers встановіть рівень доступу Modify (Зміна). Це дозволить викладачам додавати, редагувати та видаляти файли;

– Для students встановіть рівень Read & Execute (Читання та виконання), щоб вони могли лише переглядати файли.

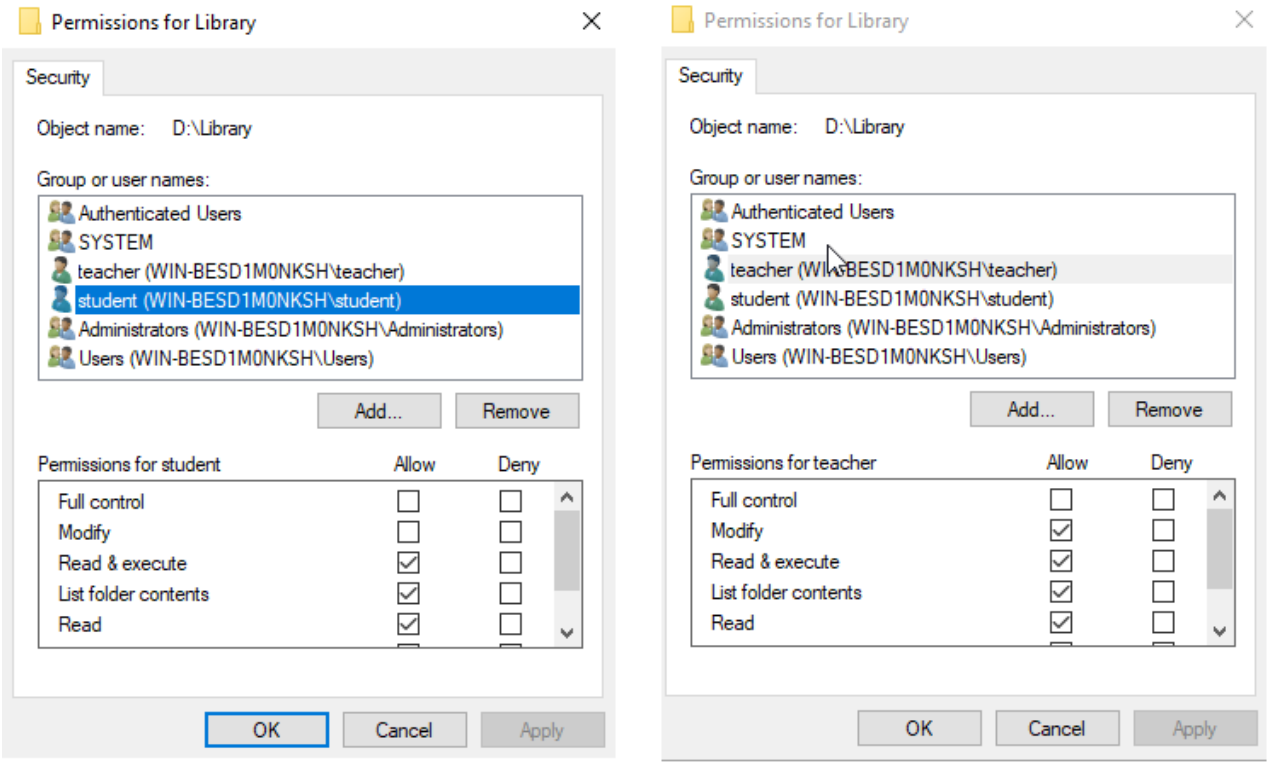

Рисунок 4.7 – Налаштування доступу до папки Library

Наступний крок це налаштування IIS для загального доступу до бібліотеки. Необхідно відкрити IIS Manager через меню "Пуск" або інструмент Server Manager. У дереві сайтів правою кнопкою миші тиснемо на Default Web Site (або інший сайт) і обираємо Add Virtual Directory.

У вікні додавання віртуальної директорії необхідно прописати назву змінної: Library та фізичний шлях до папки: D:\Library.

Після створення потрібно перейти до налаштувань директорії і активувати Directory Browsing. Відкриваємо директорію Library під вкладкою Default Web Site. У розділі Features обираємо опцію Directory Browsing, тиснемо на неї та обираємо Enable [28].

На рисунку 4.8 та 4.9 наведено налаштування IIS для загального доступу до бібліотеки з дозволом відображення директорії Library в веб-браузері.

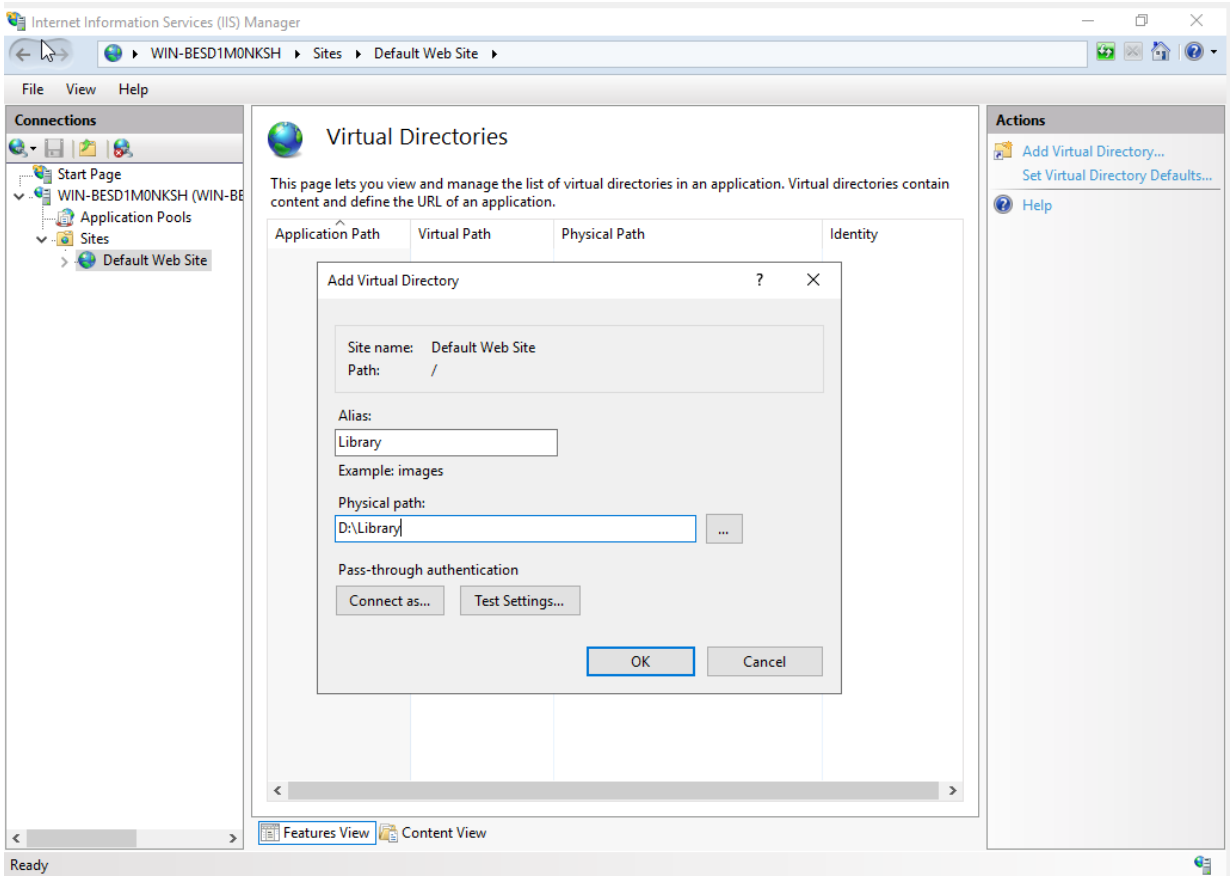

Рисунок 4.8 – Налаштування IIS для загального доступу до бібліотеки

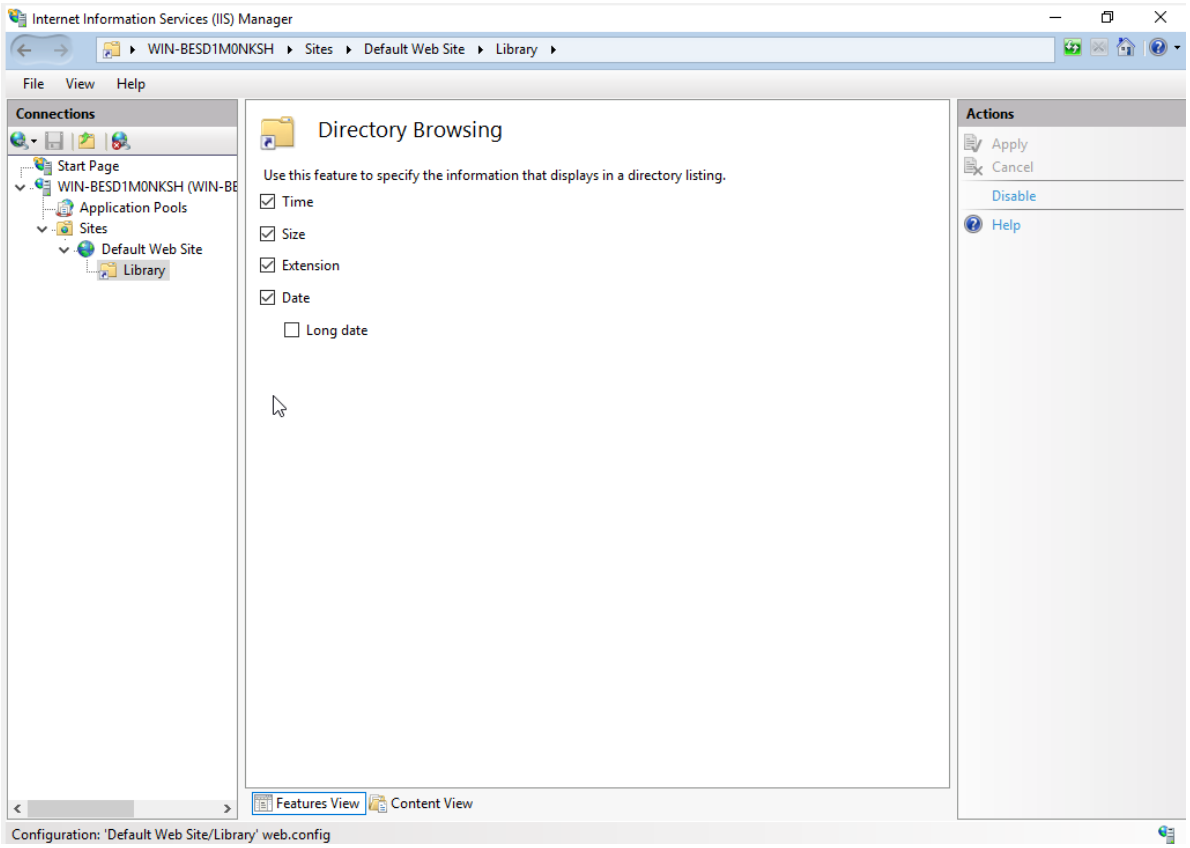

Рисунок 4.9 – Включення опцію Directory Browsing для директорії Library

Коли директорія відкрита для перегляду, необхідно налаштувати автентифікацію. Для цього в IIS Manager потрібно відкрити налаштування Authentication для створеної директорії Library.

Для ввімкнення базової автентифікації потрібно виконати наступні кроки:

– Виділити Basic Authentication і натиснути Enable;

– Anonymous Authentication потрібно вимкнути її натиснувши Disable.

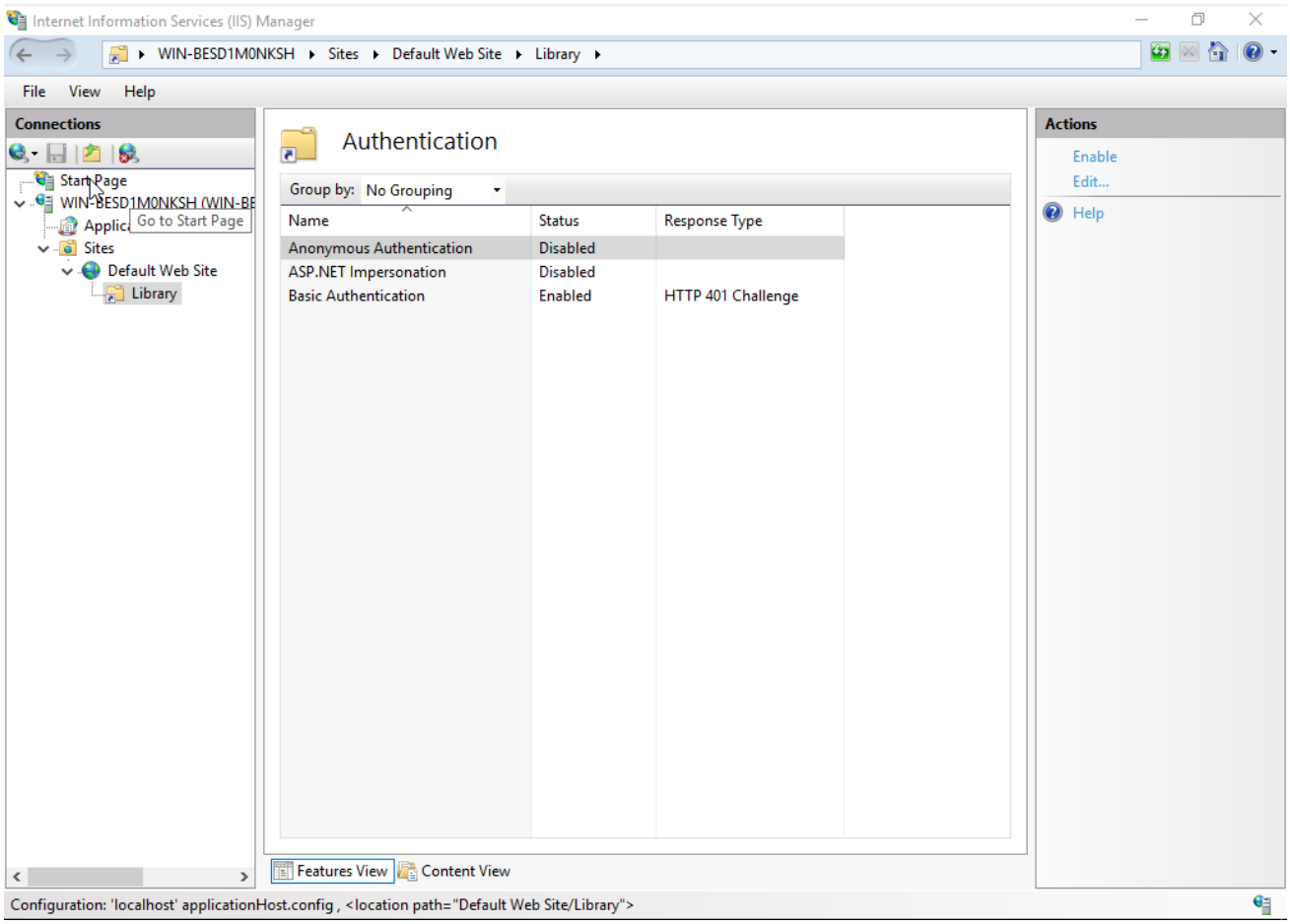

Рисунок 4.10 – Налаштування автентифікації для директорії Library.

Останній крок це перевірка доступу до веб-сервера. На вчительському пристрої в пошукову строку веб-браузера вводимо URL-адресу сервера: http://<IP_адреса_сервера>/Library

Після чого з’явиться віконце з автентифікацією. Вводимо логін та пароль для тестування доступу для вчителів. Результати наведено на рисунку 4.11.

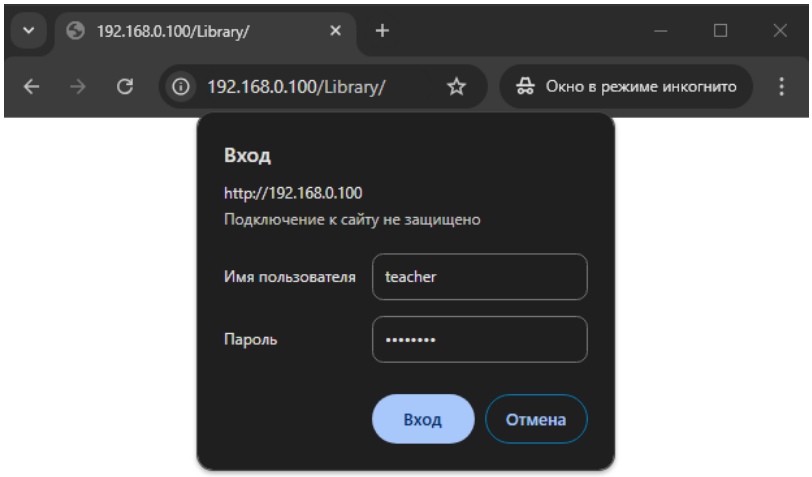

Рисунок 4.11 – Автентифікація користувачів

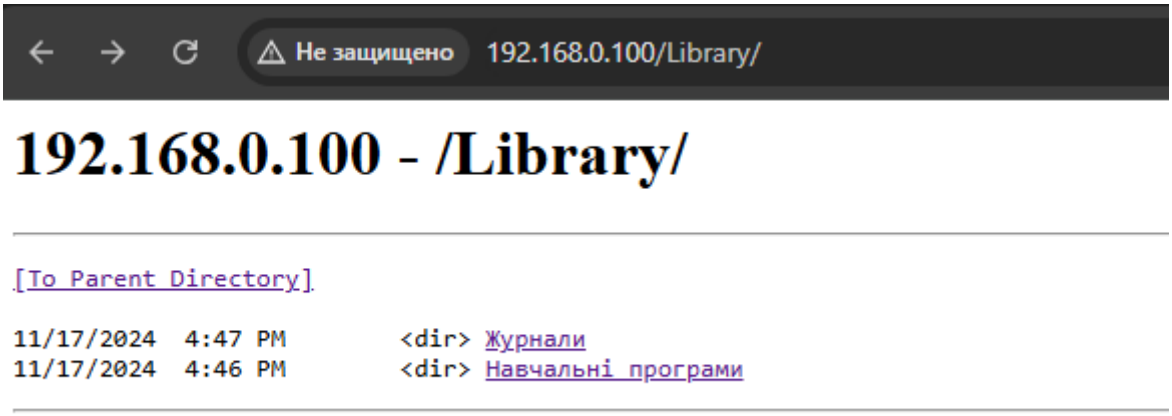

Рисунок 4.12 – Підключення до директорії через веб-браузер

Тепер бібліотека готова до використання. Вчителі та студенти зможуть отримувати доступ до файлів через веб-браузер із відповідними рівнями прав доступу. Слід зазначити, що підключення по RDP зберігається і продовжує функціонувати.

Для використання RDP (Remote Desktop Protocol) потрібно підключитися до серверу через його IP-адресу. Вона закріплюється в таблиці маршрутизації MikroTik в пулі адрес. Налаштування групової політики вже було виконано раніше, тобто студентам та вчителям потрібно ввести IP-адресу серверу в програму «Віддалений робочий стіл» та натиснути «Підключитися».

ВИСНОВКИ

У процесі дослідження корпоративної мережі навчального закладу було розглянуто її загальні особливості. Розглянуто загальні відомості про корпоративні мережі, що дало можливість зрозуміти ключові принципи їх побудови та функціонування. Корпоративна мережа є основою для ефективної взаємодії між пристроями, що дозволяє навчальному закладу використовувати різноманітні ресурси та засоби зв’язку.

Для оцінки поточного стану мережі було використано програмні засоби Wireshark та iPerf, що дозволило переглянути та проаналізувати продуктивність та якістю з'єднання. Ці інструменти допомогли оцінити стан мережі та її продуктивність, що є важливим етапом для визначення напрямів подальшої модернізації. Крім того, була проведена візуалізація структури мережі, яка дозволила отримати чітке уявлення про її фізичну та логічну організацію. Це стало основою для розробки рекомендацій та подальшого вдосконалення.

Особливу увагу було приділено модернізації захисту мережі. Було запропоновано впровадження системи відеоспостереження. Значний акцент зроблено на захисті даних та запобіганні несанкціонованому доступу до ресурсів мережі.

Було організовано веб-сервер з базою даних, який покликаний оптимізувати освітній процес та управління внутрішніми ресурсами навчального закладу. Під час впровадження цього рішення враховувались вартість модернізації та її простота. Це забезпечило швидкий доступ до навчальних матеріалів та створило базу для інтеграції нових функціональних можливостей.

В роботі було змодельовано корпоративну мережу навчального закладу СФКТІ. За допомогою програми Cisco Packet Tracer мережу було модернізовано та перевірено на стабільність до відмов.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В. Г. Компьютерные сети: Принципы, технологии, протоколы. 2005. – 107 с.

2. Хоменко В. Г., Павленко М. П. Комп'ютерні мережі: Навчальний посібник, – Донецьк: ЛАНДОН-ХХІ, 2011. – 86 – 229 с.

3. Жураковський Б. Ю., Зенів І.О. КОМП'ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК, – Київ: КПІ ім. Ігоря Сікорського, 2020. – 117 с.

4. Дудник Г.О., Ляшенко Г.Є., «Управління процесами в корпоративних мережах», Одинадцята міжнародна науково-технічна конференція «Проблеми інформатизації», 2023. – 98 с.

5. Wireshark [Електронний ресурс]. URL: https://www.wireshark.org/faq.html

6. All about packet loss [Електронний ресурс]. URL: https://www.techtarget.com/searchnetworking/definition/packet-loss

7. iPerf [Електронний ресурс]. URL: https://iperf.fr/iperf-doc.php#3doc

8. Cisco Packet Tracer [Електронний ресурс]. URL: https://www.netacad.com/cisco-packet-tracer

9. Visio [Електронний ресурс]. URL: https://www.microsoft.com/uk-ua/microsoft-365/visio/flowchart-software

10. OK-Net FTP кат.5e КППЭ-ВП [Електронний ресурс]. URL: https://e-server.com.ua/vitaja-para-po-metru/vitaja-para-ok-net-ftp-kat-5e-kppje-vp-100-4h2h0-51-1m-detail

11. TL-WR841N V14 [Електронний ресурс]. URL: https://www.tp-link.com/ru/home-networking/wifi-router/tl-wr841n/

12. Mikrotik hAP lite (RB941-2ND) [Електронний ресурс]. URL: https://mikrotik.com/product/RB941-2nD

13.TL-SF1008D [Електронний ресурс]. URL: https://www.tp-link.com/ru/business-networking/unmanaged-switch/tl-sf1008d/

14. TL-SG1016D [Електронний ресурс]. URL: https://www.tp-link.com/ru/business-networking/unmanaged-switch/tl-sg1016d/

15. NVR [Електронний ресурс]. URL: https://control.ua/ua/blog/chto-takoe-nvr.html

16. VMS [Електронний ресурс]. URL: https://www.verna.ua/security-system-cctv/vms-management-video-surveillance

17. PoE [Електронний ресурс]. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-power-over-ethernet.html

18. TL-SF1005P [Електронний ресурс]. URL: https://www.tp-link.com/uk-ua/business-networking/poe-switch/tl-sf1005p/

19. Hikvision DS-2CD1321-I(F) [Електронний ресурс]. URL: https://hikvision.co.ua/ua/hikvision-ds-2cd1321-if-28-mm/

20. TC-R3108 [Електронний ресурс]. URL: https://tiandy.com.ua/tc-r3108-spec-i-b-p8-c-e-l-s/

21. HDD WD11PURZ [Електронний ресурс]. URL: https://www.westerndigital.com/en-ae/products/internal-drives/wd-purple-sata-hdd?sku=WD11PURZ

22. Bluetti EB3A [Електронний ресурс]. URL: https://bluettipower.com.ua/zaryadna-stanciya-bluetti-eb3a-600-vt-268-vtgod-elektrostanciya-dlya-domu-ups-dzhb/

23. Google Drive [Електронний ресурс]. URL: https://workspace.google.com/intl/uk/products/drive/

24. Дудник Г.О., Митцева О.С., «Використання інтерактивних методів у професійній освіті та навчанні», IV Всеукраїнська науково-практична онлайн-конференція «Модернізація змісту професійної освіти в умовах євроінтеграції України – 2024», 2024. – 134 с.

25. Windows Server [Електронний ресурс]. URL: https://www.microsoft.com/uk-ua/windows-server

26. RAID масив [Електронний ресурс]. URL: https://jackmx.net.ua/raid-masiv-shcho-ce-take-i-dlya-chogo-voni-nam-potribni.html

27. G.Skill F3-1600C11S-8GNT [Електронний ресурс]. URL: https://www.gskill.com/product/165/186/1532583825/F3-1600C11S-8GNT

28. Directory Browsing [Електронний ресурс]. URL: https://learn.microsoft.com/ru-ru/iis/configuration/system.webserver/directorybrowse