Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)

Факультет інформаційних технологій
(факультет)

Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи бакалавра

студента Соболевського Івана Олексійовича
(ПІБ)

академічної групи 123-17-1
(шифр)

спеціальності 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему: «Комп'ютерна система IP-відео-нагляду комплексу «Золоті ключі» з опрацюванням передачі відео інформації на базі Raspberry Pi"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Проф. Цвіркун Л.І.			
розділів:				
апаратний розділ	Доц. Ткаченко С.М.			
проектування мережі та захист інформації	Ас. Панферова Я.В.			
програмне забезпечення	Ас. Бешта Л.В.			
Рецензент				
Нормоконтролер	Проф. Цвіркун Л.І.			

Дніпро

2021

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних
технологій та
комп'ютерної інженерії

проф._____ В.В. Гнатушенко
"__" _____ 2021 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту Соболевського І.О. академічної групи 123-17-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему: «Комп'ютерна система IP-відео-нагляду комплексу «Золоті ключі» з опрацюванням передачі відео інформації на базі Raspberry Pi"
(назва за наказом ректора)

затвержена наказом ректора НТУ "Дніпровська політехніка" від 07.06.2021 р. № 317

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	Застосувати звіт з виробничої практики, інших науково-технічних джерел та розробити технічні вимоги до комп'ютерної системи IP-відео-нагляду комплексу «Золоті ключі»	05.05.2021
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи IP-відео-нагляду комплексу «Золоті ключі»	14.05.2021
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи IP-відео-нагляду комплексу «Золоті ключі» з опрацюванням передачі відео інформації на базі Raspberry Pi	31.05.2021
Графічна частина	Графічні результати розробки системи подати у вигляді рисунків електричних схем та інших креслень на 18 арк. формату А4	07.06.2021

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище та ініціали)

Дата видачі 03.02.2021 р.

Дата подання до екзаменаційної комісії 12.06.2021 р.

Прийнято до виконання _____ Соболевський І.О.
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 106 с., 71 рис., 9 табл., 22 джерел, 1 додаток.

Об’єктом розробки являється – комп’ютерна система відеонагляду для котеджного містечка “Золоті ключі”.

Метою роботи являється – підбір та налаштування обладнання для формування мережі підприємства “АН ЗОЛОТІ КЛЮЧІ” та котеджного містечка “Золоті ключі”, розробка та підключення системи відеонагляду на території котеджного містечка “Золоті ключі”. Метою системи являється підвищення рівня безпеки у котеджному містечку.

У розділі «Стан питання і постановка задачі» проаналізована сфера, в якій буде впроваджуватись система, проведено аналіз підприємства “АН ЗОЛОТІ КЛЮЧІ” та котеджного містечка “Золоті ключі”. А також поставлена задача і визначенні можливі путі рішення.

У розділі «Технічні вимоги до комп’ютерної системи» дані технічні вимоги для впровадження системи, сформовані вимоги до видів забезпечення.

У розділі «Розробка апаратної частини комп’ютерної системи» наведено структурну схему технічних заходів підприємства, підібрано апаратні засоби комп’ютерної мережі, розроблена архітектура комп’ютерної мережі та проведені розрахунки вихідного трафіку.

У розділі «Проектування комп’ютерної мережі та перевірка роботи комп’ютерної системи» проведено розрахунок підмереж, та налаштована комп’ютерна мережа підприємства “АН ЗОЛОТІ КЛЮЧІ” та котеджного містечка “Золоті ключі”.

ВІДЕОНАГЛЯД, ОС, RASPBERRYPI, CISCO, СЕРВЕР, WEB.

ЗМІСТ

ВСТУП 7
1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ 8
1.1 Характеристика галузі та умов застосування системи, що проектується 8
1.2 Характеристика котеджного містечка «Золоті ключі» 9
1.3 Організаційна структура підприємства 12
1.4 Характеристика і структура об’єкта впровадження 12
1.5 Системи відеоспостереження 17
1.5.1 Аналогові системи відеоспостереження 18
1.5.2 Цифрові системи відеоспостереження 19
1.5.3 IP системы видео спостереження 21
1.6 Завдання і мета роботи 24
1.7 Визначення можливих напрямків рішення поставлених завдань та обґрунтування вибору. 24
2 ТЕХНІЧНІ ВИМОГИ ДО КОМП’ЮТЕРНОЇ СИСТЕМИ 27
2.1 Вимоги до системи в цілому 27
2.1.1 Структура і функціонування системи 27
2.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи 27
2.1.3 Вимоги до надійності 28
2.1.4 Вимоги до захисту інформації від несанкціонованого доступу 29
2.1.5 Вимоги до патентної чистоти 29
2.2 Вимоги до видів забезпечення 29
2.2.1 Вимоги до інформаційного забезпечення системи 29
2.2.2 Вимоги до технічного забезпечення системи 30
2.2.3 Вимоги до організаційного забезпечення системи 30
3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ 31
3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи 31
3.1.1 Розташування камер на об’єкті відеоспостереження 32
3.1.2 Аналіз входів і виходів 34
3.2 Вибір та характеристики апаратних засобів комп’ютерної мережі 36
3.2.1 Вибір та характеристика обладнання для IP відеоспостереження 36
3.2.2 Вибір та характеристика мережевого обладнання 39

3.2.3 Вибір та характеристика сервера 41
3.3 Розробка архітектури мережі комп’ютерної системи 44
3.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства 46
4 ПРОЕКТУВАННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП’ЮТЕРНОЇ СИСТЕМИ 48
4.1 Розрахунок схеми адресації комп’ютерної мережі 48
4.2 Налаштування та перевірка роботи комп’ютерної системи 52
4.2.1 Базове налаштування конфігурації пристроїв 52
4.2.2 Налаштування маршрутизаторів корпоративної мережі 58
4.2.3 Налаштування роботи Інтернет 59
4.2.4 Налаштування агрегування каналів PAgP 60
4.2.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec 62
4.2.6 Перевірка роботи комп’ютерної системи 64
5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ 68
5.1 Розробка методів для захисту інформації в комп’ютерній системі 68
5.2 Налаштування маршрутизаторів на підтримку служби AAA 68
5.3 Налаштування мереж VLAN 70
5.4 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN 72
5.4.1 Налаштування параметрів безпеки комутаторів 72
5.4.2 Налаштування адресації ПК в мережах VLAN 72
6 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП’ЮТЕРНОЇ СИСТЕМИ 75
6.1 Призначення і область застосування програми 75
6.2 Обґрунтування технічних характеристик програми 75
6.2.1 Обґрунтування вибору платформи для програми 75
6.2.2 Обґрунтування вибору технології ПО 76
6.2.3 Вибір та обґрунтування архітектури додатку 77
6.2.4 Вибір та обґрунтування архітектури компонентів 77
6.2.5 Вибір та обґрунтування структури БД 79
6.3 Підготовка та налаштування пристроїв 80
6.3.1 Встановлення ОС 80
6.3.2 Налаштування WiFi на Raspberry Pi 81

6.3.3 Налаштування SSH на Raspberry Pi 81
6.3.4 Підключення живлення до Raspberry Pi 81
6.3.5 Налаштування мережі для Raspberry Pi 82
6.3.6 Підключення по протоколу SSH до Raspberry Pi 84
6.3.7 Зміна стандартного паролю на Raspberry Pi 85
6.3.8 Налаштування камери PiCam на Raspberry Pi 86
6.3.9 Встановлення програми cvlc 89
6.3.10 Перевірка роботи камери 89
6.3.11 Автозапуск камери, для роботи у live режимі 91
6.4 Опис розробленої програми 92
6.4.1 Загальні відомості 92
6.4.2 Функціональне призначення 92
6.4.3 Опис логічної структури застосунку 93
6.4.3.1 Побудова та запуск застосунку 93
6.4.3.2 Реалізація серверної частини 93
6.4.3.3 Реалізація інтерфейсу користувача 94
6.4.3.4 Використовувані технічні засоби 102
6.4.3.5 Виклик і завантаження застосунку 102
6.4.3.5 Вхідні і вихідні дані 102
ВИСНОВКИ 104
ПЕРЕЛІК ПОСИЛАНЬ 105
ДОДАТОК А ТЕКСТ ПРОГРАМИ 107

ВСТУП

У сучасному світі, системи відеоспостереження являються невід'ємною частиною підтримки безпеки та протидії злочинам. Системи відеоспостереження бувають різних масштабів, від однієї камери для стеження за клієнтами біля каси, до систем міського масштабу, які керують тисячами камер.

На ринку є безліч рішень для реалізації відеоспостереження – для малого бізнесу, для дому, та для великих систем, з купою камер. Головна проблема рішень, які присутні на ринку, це відсутність централізованої системи з розмежуванням доступу до камер та записів.

За завданням, для котеджного містечка “Золоті ключі” потрібно розробити систему відеоспостереження, яка базується на мікрокомп’ютері Raspberry Pi. В системі повинен бути адміністратор, який займається видачею користувачам прав на доступ до камер. Користувачі повинні мати можливість перегляду своїх камер в реальному часі, та запису за заданий адміністратором період.

IP системи відеоспостереження базуються на відеореєстраторах, які являються окремим обладнанням, що накладає ряд проблем на кінцевого користувача.

Першою проблемою являється те, що користувач повинен виконати ряд умов, для доступу до камер. По перше користувач повинен мати білу IP адресу на своєму маршрутизаторі, але не всі провайдери можуть її надати. Якщо в користувача є біла IP адреса, тоді потрібно налаштувати мережеве обладнання, на функції VPN серверу, чи трансляції адрес, але не всі маршрутизатори підтримують даний функціонал.

Метою даної роботи буде розробка хмарного сервісу, який дозволить користувачам отримувати доступ до своїх камер незалежно від мережі, чи геолокації, та розробка мережі підприємства “АН ЗОЛОТІ КЛЮЧІ”, для забезпечення роботи персоналу та системи.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умов застосування системи, що проектується

Котеджні містечка користуються популярністю. Це майже райські куточки, які знаходяться відокремлено від шумної цивілізації. В такому котеджному містечку, як «Золоті ключі», люди можуть купити як готовий дім, так і ділянку, для того, щоб побудувати, в залежності від фантазії архітектора, смаку власника, та наявності матеріальних благ, будівлю мрії.

В таких містечках гостро стоїть питання безпеки, вона завжди повинна стояти на першому плані.

Навіть за наявністю охоронців, проходу та проїзду за пропусками, не можна нехтувати безпекою від внутрішніх загроз, таких як – сусіди, гості, робочі, екскурсанти, люди які тимчасово знімають апартаменти.

Кожен дім повинен бути захищений охоронною системою відеоспостереження, щоб уникнути злочину з найменш очікуваного боку.
Відеонагляд повинен виконувати такі функції:

1) Відеозйомка за зазначений період – завжди повинен бути відеозапис, який буде служити доказом злочину для правоохоронних органів.
2) Показ камер у реальному часі – відеонагляд повинен показувати реальну картину, в реальному часі. Це важлива функція яка може служити для:
    - налаштування, виявлення найкращого кута огляду.
    - перегляду поточної ситуації, наприклад, коли було получено автоматичне оголошення про тривогу.
    - перевірки справності камер.
3) Підтримка режимів охорона та спокій:
    - охорона – режим для виявлення загроз, та оповіщення про них:
        - власника;
        - охоронної фірмі;
        - поліції;

- спокій – режим, коли охоронна сигналізація вимкнена, тому-що, наприклад, в домі є авторизовані люди, та сигналізації немає сенсу працювати

1.2 Характеристика котеджного містечка «Золоті ключі»

"Золоті ключі" – перший в Україні котеджний мікрорайон, створений в рамках комплексного містобудівного рішення.

Рисунок 1.1 – Котеджне містечко «Золоті ключі» на мапі Google Maps

Розташування: Дніпропетровська область, Дніпропетровський район, Слобожанське. Розташування котеджного містечка на карті зображено на рисунку 1.1.

Котеджне містечко “Золоті ключі” розташований в 10 км від Дніпропетровська. На рисунку 1.2 зображено план будівництва, на рисунку 1.3 стан будівництва на даний момент.

Рисунок 1.2 – План будівництва 2004-2009-х років

Рисунок 1.3 – Стан будівництва на 2021-й рік

Забудовник: Міжнародна будівельна компанія (МСК) «Україна-Канада».

Загальна площа забудови: 260 га.

Кількість будинків: близько тисячі.

Площа будинків: від 120 м².

Площа земельних ділянок: від 8 до 15 соток.

Комунікації:

- водопостачання;
- газопостачання;
- каналізація;
- електрика;
- інтернет.

Інфраструктура:

На території КМ Золоті ключі знаходяться фітнес центр, дитячий садок, школа, спортивний магазин, спортивний комплекс, мінімаркет, ресторан. Поруч з котеджне містечком знаходяться будівельний гіпермаркет Епіцентр, торговий центр Metro, супермаркет Фуршет.

Опис:

На сьогоднішній день котеджне селище Золоті ключі є одним з найбільших житлових районів України. Його інфраструктура включає в себе соціальні, технічні та комерційні об'єкти. Селище розташоване в передмісті міста Дніпро і займає площу близько 210 гектарів.

Кожен котедж знаходиться на окремій ділянці і був побудований за індивідуальним проектом. Проектуванням будинків займалися авторитетні архітектори, метою яких було створення максимально затишною і комфортної обстановки.

Котеджі селища мають площею від 80 м² і ціною на рівні трьох, а то і чотирьохкімнатних квартир. При цьому, власники такої нерухомості можуть насолодитися всіма благами приватних житлових будинків. Котеджне містечко було зведено з урахуванням усіх передових технологій будівництва, екологічності, енерго- і водозбереження.

Золоті ключі відмінно поєднують в собі кращі світові будівельні технології та матеріали. Над його спорудженням працювало понад ста українських і зарубіжних компаній. Саме тому котеджне містечко є дуже

комфортабельним, затишним і безпечним. Його територія постійно охороняється. А будинки розташовані по сусідству з парком, природними озерами та іншими благами.

1.3 Організаційна структура підприємства

Організаційна структура підприємства – це склад відділів, служб і підрозділів в апараті управління, системна їх організація, характер підпорядкованості та підзвітності один одному і вищому органу управління, а також набір координаційних і інформаційних зв'язків, порядок розподілу функцій управління по різним рівням і підрозділам управлінської ієрархії.

Організаційна структура є базисом оптимізації функціонування підприємства та використання його виробничо-технологічного потенціалу [1].

Організаційна структура підприємства "АН ЗОЛОТІ КЛЮЧІ" відноситься до класичної структури. Структуру "АН ЗОЛОТІ КЛЮЧІ" вказано на рисунку 1.4.

1.4 Характеристика і структура об'єкта впровадження

Об'єктами, впровадження системи відеоспостереження, являються чотири двоповерхові будівлі, з чотирма кімнатами, які знаходяться на вулиці Полтавська, в котеджному містечку "Золоті Ключі". Фото будівлі зображено на рисунку 1.5. План першого поверху зображено на рисунку 1.6. План другого поверху зображено на рисунку 1.7.

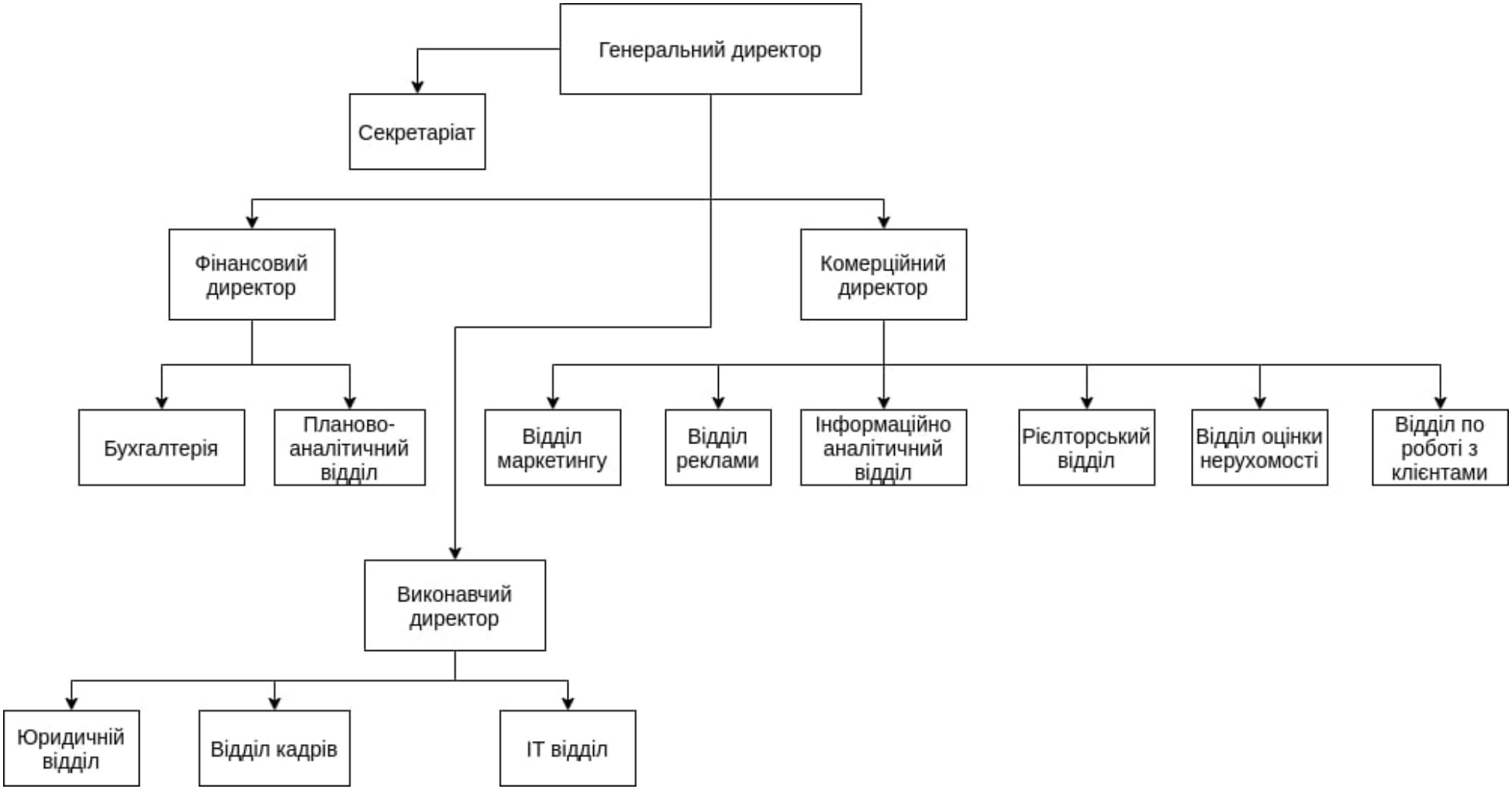

Рисунок 1.4 – Організаційна підприємства “АН ЗОЛОТІ КЛЮЧІ”

Рисунок 1.5 – Фото будівлі

Характеристики:

- 4 кімнати
- 2 поверхи
- Площа 136 м² • 55 м² • 36 м²
- 4.5 сотки
- Стіни з цегли

Перший поверх:

- велика кімната, яка вміщує у себе гостьову та кухню
- коридор зі сходами
- кімната з робочим столом

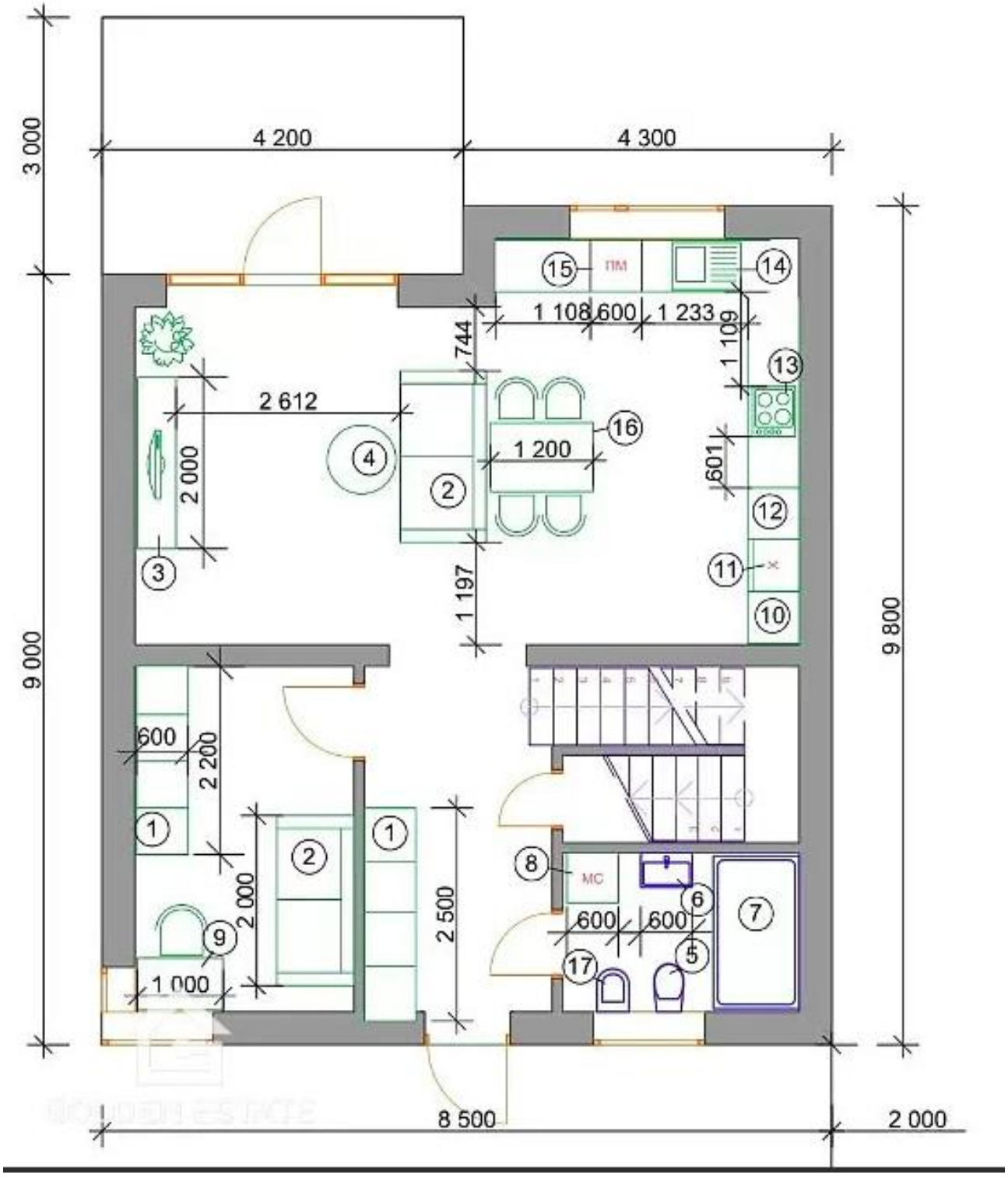

Рисунок 1.6 – План 1-й поверх

- ванна кімната

Інтер'єр:

1 - шкаф-купе

2 - диван

3 - тумба з телевізором

4 - журнальний столик

5 - туалет

6 - раковина

7 - душ

8 - пральна машина

9 - робочий стіл

10 - шафа

11 - холодильник

12 - шафа зі встроєною духовкою і мікрохвильовкою

13 - варильна панель

14 - мийка

15 - посудомийна машина

16 - обіденна зона

17 - біде

Другий поверх:

- дві спальні кімнати;
- кімната з робочим столом;
- ванна кімната;
- коридор зі сходами сходами;
- балкон.

Інтер'єр:

1 - двоспальне ліжко;

2 - телевізор;

3 - шкаф-купе;

4 - туалет;

5 - біде;

6 - диван;

7 - робочий стіл;

8 - раковина;

9 - ванна [2].

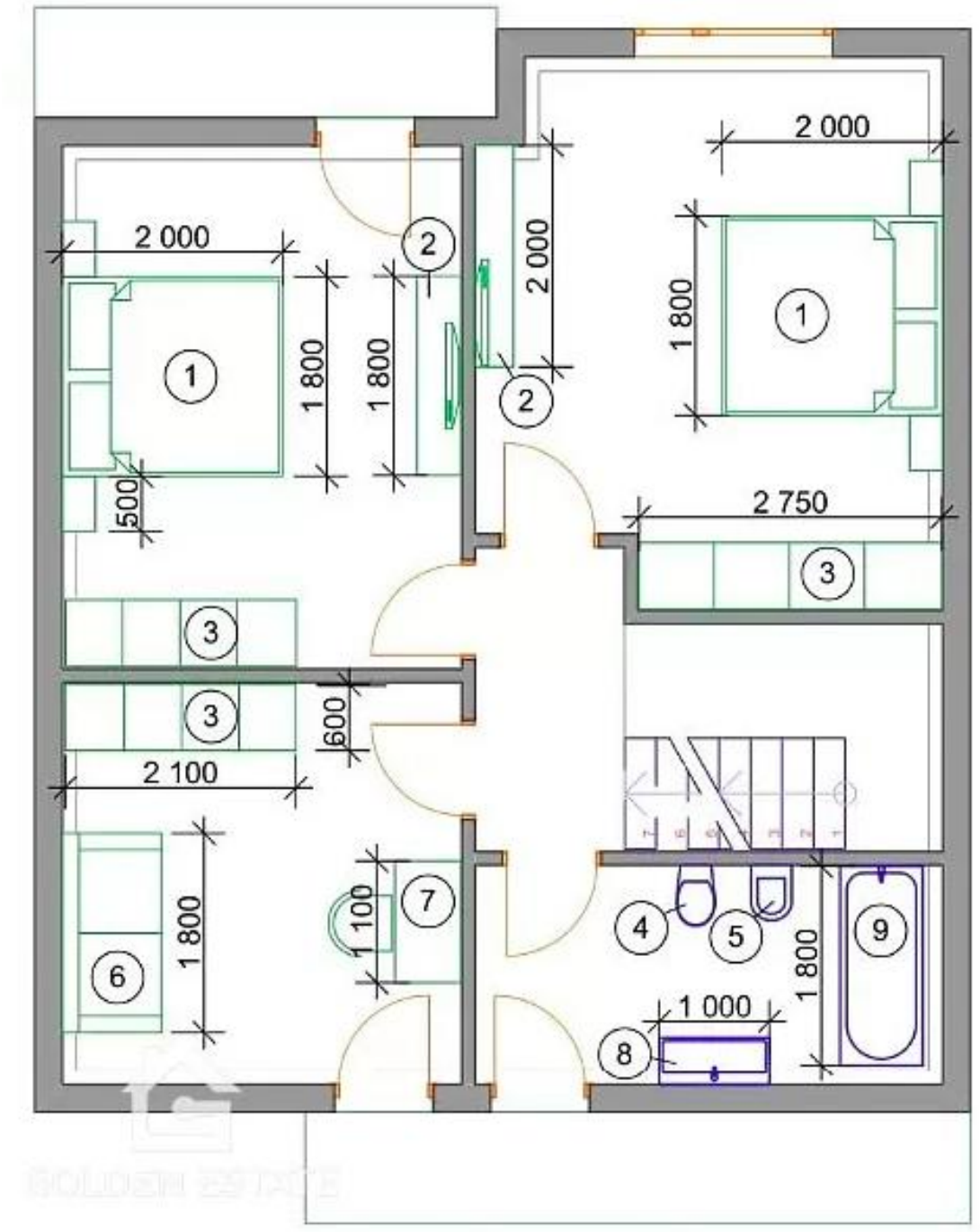

Рисунок 1.7 – План 2-й поверх

1.5 Системи відеоспостереження

Системи відеоспостереження – це програмно-апаратний комплекс, важливий елемент безпеки, який встановлюється в житлових будинках,

офісах, на дворі, та інших місцях, для підтримання під охороною. Вона може бути як простою, так і складною. Проста система відеоспостереження може складатися лише з однієї камери, яка може передавати відеосигнал на монітор. Складна же, може працювати по протоколу IP, та транслювати відео одразу на декілька підключених комп'ютерів. Системи відеоспостереження діляться на аналогові та цифрові [3].

1.5.1 Аналогові системи відеоспостереження

Аналогові системи відеоспостереження побудовані з використанням коаксіального кабелю, дротом за технологією крученої пари або волоконно-оптичної системи. Стандартом відеосигналу в таких системах є телевізійні PAL або NTSC. Вважаються застарілими, тому що цю систему дуже важко масштабувати і автоматизовувати, такі системи застосовуються у місцях, де потрібно встановити відеонагляд за низькою вартістю.

Переваги аналогової системи:

- низька вартість;
- надійність високого рівня;
- проста схема підключення;
- просте налаштування;
- простота користування.

Недоліки аналогової системи:

- потреба постійного обслуговування;
- відсутність можливості збереження даних у цифровому форматі;
- відсутність можливості автоматизації;
- максимальна кількість камер залежить від кількості портів на відеореєстраторі, щоб поставити більше, потрібно ставити другий відеореєстратор на інший монітор, або покупати видеорегистратор с більшою кількістю аналогових портів;
- відсутність можливості шифрування відеосигналу;
- відсутність можливості перегляду через інтернет;

- відсутність можливості керування збільшенням чи рухом;
- для підключення мікрофону потрібен окремий кабель.

Графічний приклад системи відеоспостереження зображен на рисунку 1.8.

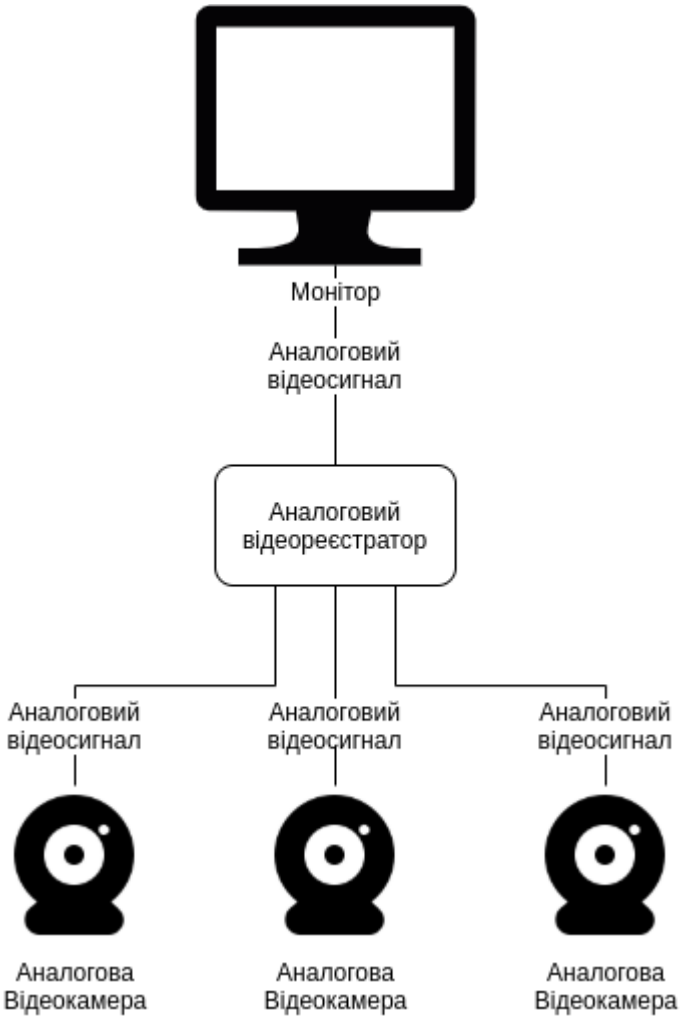

Рисунок 1.8 – Схема підключення аналогового відеоспостереження

1.5.2 Цифрові системи відеоспостереження

Цифрові системи відеоспостереження мають переваги над аналоговими і являються їх сучасним нащадком. Вони доступні у декількох варіантах.

Варіант перший (гібридний) – аналогові камери приєднані до компьютера, який оцифровує сигнал для того, щоб була можливість вивести сигнал від камер в мережу або записувати відеопоток в цифровому формати.

Такі системи зазвичай ставлять в тих місцях, де вже є аналогові камери і буде дешевше їх оцифрувати, ніж повністю замінити.

Варіант другий – технологія HD-SDI (High-Definition Serial Digital Interface), передача відеосигналу через послідовний цифровий інтерфейс для передачі зображення з високою роздільною здатністю. HD-SDI камери це проміжна ланка між аналоговими і IP системами. Цей стандарт перейшов до відеонагляду з телебачення.

HD-SDI виходить з аналогового композитного сигналу, спочатку сигнали розкладаються на складові: яскравість Y, а також цвіторізні сигнали U (або Cr) і V (або Cb). Потім кожна компонента оцифровується і подається на кодер, в якому дані збираються в послідовності, відповідній структурі SDI.

Звук включається в структуру SDI (в проміжках між мітками EAV і SAV) за допомогою спеціальних пристроїв – ембедерів, на приймальні ж боку він знову витягується з сигналу за допомогою де ембедерів. Стандарт SMPTE-292M дає можливість впровадження до 16 каналів цифрового звуку.

Камери HD-SDI використовують стандартизований формат 16 : 9. За дозволом зображення камери високої роздільної здатності діляться на два типи:

1) Камери HDTV 720p, стандарт SMPTE 296M, підтримують дозвіл 1280x720 пікселів, високу точність передачі кольору, формат 16: 9, використовують порядкову розгортку 25/30 Гц, 50/60 Гц.

2) Камери HDTV 1080p, стандарт SMPTE 274M, підтримують дозвіл 1280x720 пікселів, високу точність передачі кольору, формат 16: 9, використовують порядкову розгортку 25/30 Гц, 50/60 Гц [4].

Переваги:

- гарна якість зображення, так як інтерфейс цифровий, зображення не погіршується при передачі на відстань;
- відсутність затримок, так як кожна камера має виділену лінію зв'язку з відеореєстратором;
- швидке налаштування.

Недоліки:

- дальність передачі (максимально 150 метрів по коаксіальному кабелю);
- вартість обладнання вище ніж в аналогових системах.

1.5.3 IP системы видео спостереження

Internet Protocol (IP) це протокол, який об’єднав окремі комп'ютерні мережі у всесвітню мережу Інтернет. До світу відеонагляду IP протокол добрався з початком 2000-х років. Цифрові камери почали оснащувати портами Ethernet з RS-45, та під’єднувати їх до мережі. Доступ до таких камер можна получити як з локальної мережі, так і з Інтернету [5].

IP система відеонагляду – це цифрова система, в якої камери працюють по протоколу IP та можуть передавати свій відеосигнал через мережу до відеореєстратору для перегляду та запису, або працювати обособленно, в такому випадку користувач може приєднатись до кожної камери окремо. На данный момент IP камери можуть працювати як по кабелю, так і по WiFi, що дає можливість встановлення IP камер бездротовим підключенням. Приклад IP відеоспостереження зображено на рисунку 1.9.

IP система відеонагляду дає значні переваги для користувача та являється проривом у охоронній та науковій областях.

IP камера представляє собою маленький комп’ютер, в якому є центральний процесор, керуючий відеокамерою, мережевим інтерфейсом та модулями мікрофону або тривожними виходами, процессор також керує стисненням відеопотоку. Як і у будь якого комп’ютера в IP-камері стоїть операційна система, зазвичай це урізаний за функціоналом дистрибутив Linux, з розгорнутим веб-сервером для приєднання за HTTP протоколом користувача. Зазвичай IP камера використовує протоколи HTTP, RTSP, RTP.

RTSP (Real Time Streaming protocol) – це основний протокол, по якому відбувається передача відеопотоку. Протокол RTSP може працювати як через

TCP, так і через UDP, в залежності від швидкості та/або стабільності мережі [6–8].

HTTP (HyperText Transfer Protocol) – по цьому протоколу працювали застарілі моделі відеокамер, в яких відеопотік розкладався на фрейми в форматі JPEG і викладався на сервері відеокамери, клієнт тим часом забирав їх з певною частотою для відновлення кадру. Зараз HTTP в основному забезпечує для віддачі користувачу веб-сторінок, на яких відображається відео, або налаштування камери [9].

RTP (Real Time Transport Protocol) – цей протокол використовується для передачі даних в реальному часі. RTP працює, як правило, поверх UDP і не використовує зарезервовані порти, як RTSP (це може стати проблемою, якщо знадобиться відправити відеопоток за міжмережевий екран) [10; 11].

Крім класичних камер відеоспостереження, можуть бути задіяні тепловізійні IP-камери, вони можуть використовуватись в одній системі з класичними. Тепловізійні відеокамери застосовуються для контролю за інженерними об’єктами, для спостереження за периметром та для виявлення людей з підвищеною температурою тіла.

Стиснення зображення, дуже важливе в мережі з IP-камерами. Стиснення відбувається в самій IP-камері, для зниження кількості трафіка в мережі, так як ширина каналу в IP мережі не завжди максимальна, потрібно стискати трафік, щоб не забивати мережевий канал. Існує два основні підходи до стиснення: всередині кадра і між кадрами:

а) стиснення всередині кадра виконується тільки в одному кадрі, а не між кадрами (MJPEG);

б) стиснення між кадрами виконується всередині кадрів і в окремих кадрах (H.264, H.265, MPEG-4).

На даний момент кодек H.264 найбільш поширений в IP-обладнанні.

Переваги:

- віддалений доступ до камер в режимі online;
- користування камерами з різних пристроїв одночасно;

– можливо настроїти програмний відео аналіз, наприклад зчитування знаків автомобілів, виявлення рухомих об’єктів або аналіз настрою людей;
– масштабування системи;
– можливо бездротове підключення;
– шифрування відео трафіку.

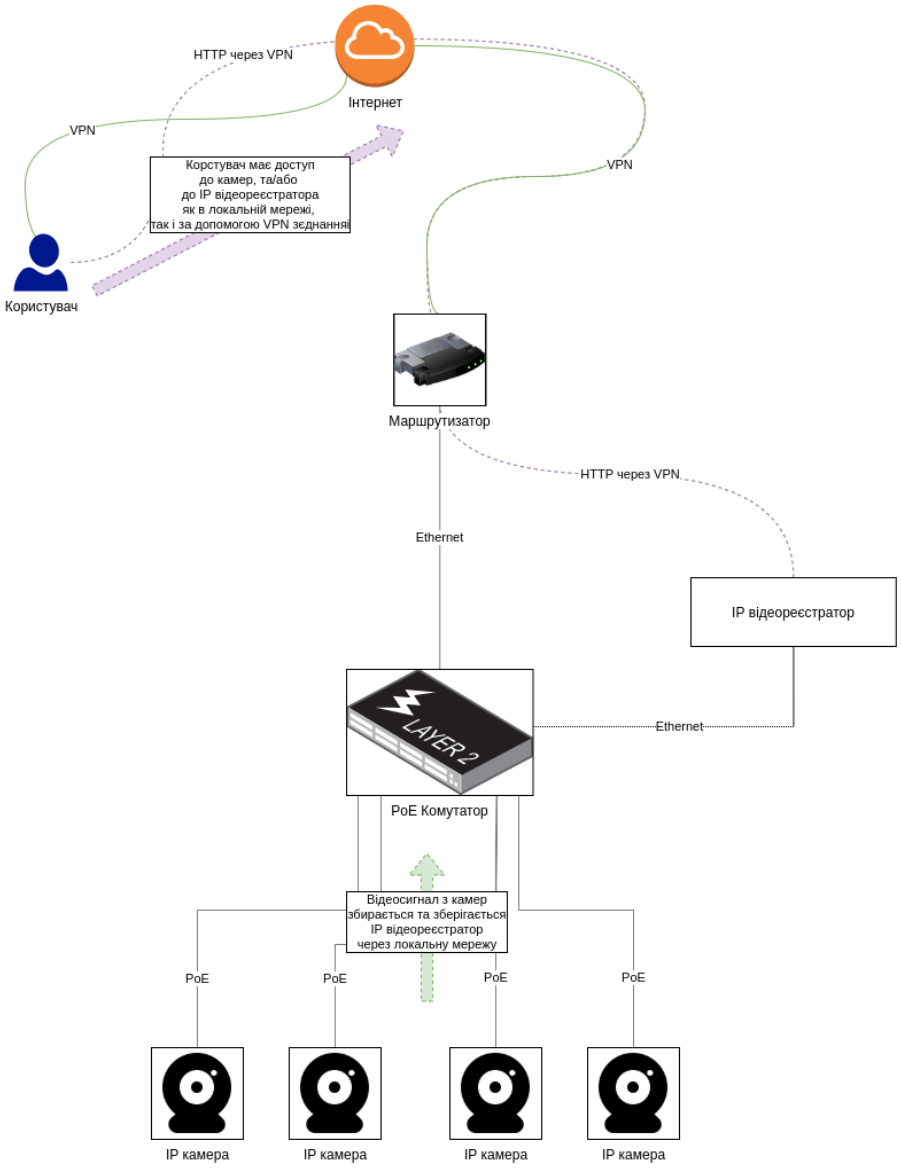

Рисунок 1.9 – Схема підключення цифрового відеоспостереження з IP відеореєстратором

Недоліки:

- ціна. IP відеоспостереження дорожче за інші аналоги, та потребує покупку та налаштування мережі для передачі даних;
- для гарної якості картинки повинна бути гарна пропускна здатність мережі;
- стан мережі впливає на відеонагляд, несправність мережі може позначитися на роботі системи відеоспостереження.

1.6 Завдання і мета роботи

Підвищення рівня безпеки будинку за рахунок встановлення системи відеоспостереження. Створення програмного забезпечення для централізованого перегляду трансляцій реального часу з відеокамер, запис та можливість доступу до місця зберігання відеофайлів, видалення старих записів за вказаний користувачем період. Забезпечення користувача зручним доступом до трансляції та оптимізація системи для коректного функціонування. Провести аналіз інформаційних джерел для покращення роботи системи.

Для досягнення мети необхідно вирішити такі завдання:

а) провести аналіз існуючих систем відеоспостереження;

б) побудувати схему розташування відеокамер на плані будівлі;

в) розробка програмного забезпечення керування даними;

г) створити схему мережі для найбільш ефективної передачі відео;

д) провести аналіз джерел інформації.

1.7 Визначення можливих напрямків рішення поставлених завдань та обґрунтування вибору.

Комп'ютерна система відеонагляду буде побудована на базі одноплатного компьютеру Raspberry Pi, який зображено на рисунку 1.10, з модулем камери , зображено а рисунку 1.11. Raspberry Pi являється ідеальною можливістю для побудови не складної системи чи прототипу завдяки безлічі модулів. Згідно з

завданням, можна використати модуль PiCam та програмну мову Python з бібліотекою picamera, для зчитування зображення з камери.

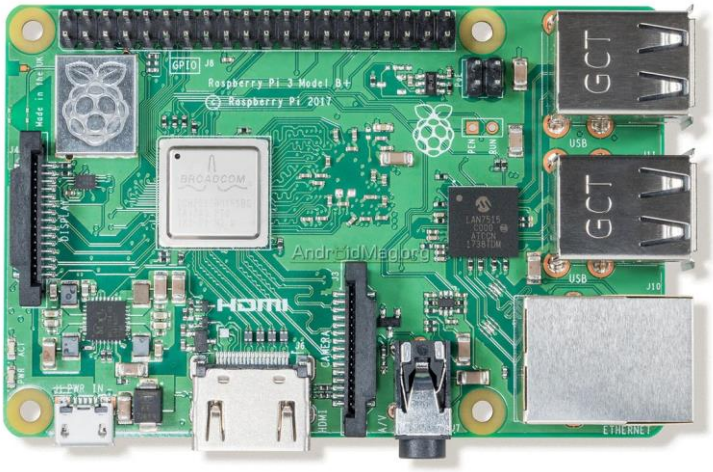

Рисунок 1.10 – Одноплатний комп’ютер Raspberry Pi

Рисунок 1.11 – Модуль камери для Raspberry Pi

При побудові мережі буде використана топологія – “зірка”. Зірка – це єдина топологія мережі з явно виділеним центром, до якого підключаються всі інші абоненти. Обмін інформацією йде винятково через центральний комп'ютер, на який лягає більше навантаження, тому нічим іншим, крім мережі, він, як правило, займатися не може. Зрозуміло, що мережне устаткування центрального абонента повинно бути істотно складнішим, чим устаткування периферійних абонентів. Про рівноправність всіх абонентів (як у шині) у цьому випадку говорити не доводиться. Звичайно центральний комп'ютер найпотужніший, саме на нього покладають всі функції по керуванню обміном. Ніякі конфлікти в мережі з

топологією зірка в принципі не можливі, тому що керування повністю централізоване [12].

Зробивши аналіз ринку мережевого обладнання було обрано обладнання компанії Cisco Systems, Inc. Компанія Cisco це світовий лідер в області мережевого обладнання. Обладнання Cisco має ряд переваг, таких як:

- надійність обладнання;
- гарантія;
- підтримка;
- гнучке програмне забезпечення.

Для моделювання системи буде використовуватися програмний застосунок Packet Tracer від компанії Cisco. Packet Tracer – це інструмент візуального моделювання між платформами, розроблений Cisco Systems, який дозволяє користувачам створювати топології мережі та імітувати сучасні комп'ютерні мережі. Програмне забезпечення дозволяє користувачам моделювати конфігурацію маршрутизаторів і комутаторів Cisco за допомогою модельованого інтерфейсу командного рядка. Packet Tracer використовує користувальницький інтерфейс перетягування, що дозволяє користувачам додавати та видаляти змодельовані мережеві пристрої, як їм зручно. Програмне забезпечення в основному орієнтоване на сертифікованих студентів Академії Cisco Network Associate Academy як навчальний інструмент, який допомагає їм вивчати основні концепції CCNA [13; 14].

Для написання програмного забезпечення буде використовуватись мова JavaScript. Серед основних її переваг – написання на одній мові як клієнтської аплікації, так і серверного ПО. Мова JavaScript являється асинхронною. Цей підхід служить для того, щоб не перегружати ресурси сервера при великій кількості запитів від користувачів. Запити виконуються в паралельному режимі, але обробляються у одному потоці, тому операцій ставляться у чергу і поки програма робить запит, який потребує очікування, в цей момент стартує обробка наступного в черзі. Таким чином операцій виконуються асинхронно і це являється дуже ефективним способом обробки запитів та економії ресурсів [15].

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

2.1.1 Структура і функціонування системи

Комп'ютерна система повинна виконувати наступні функції:

Збір інформації. Інформація, в цьому випадку, – відео поток з камер. Відео дані повинні передаватися мережею з IP камер для подальшого аналізу та обробки.

Аналіз та обробка інформації. Дані з камер повинні попадати до інтерфейсу користувача, для нагляду за об'єктом впровадження. Інтерфейс користувача повинен бути доступним як з локальної мережі, так і завдяки VPN з'єднанню.

Зберігання інформації. Камери повинні записувати відеопотік на сервер FTP, за необхідністю, користувач повинен мати доступ до перегляду відеозапису. Відео повинне зберігатися за встановлений користувачем період, для оптимізації місця на FTP сервері. Камери повинні фіксувати час, для того, щоб, при перегляді запису, можна було встановити дату та час записаної події.

Комп'ютерна система повинна мати такі параметри – гнучкість, масштабованість, віддалений доступ, можливість адміністрування.

2.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи

Комп'ютерну систему повинні обслуговувати:

І. Мережевий інженер – відповідає за коректну роботу мережевого обладнання, займається моніторингом основних частин мережі, при необхідності, налаштовує нове мережеве обладнання.

1) Кількість – дві людини.

2) Графік роботи:

а) з 9 до 18 понеділок-п'ятниця;

б) вихідні та празники, тільки за умови робот, з відновлення коректної роботи системи.

II. Експерт з техпідтримки – людина що за працює з клієнтами, відповідає на заявки користувачів за технічними питаннями, передає інформацію о некоректній роботі системи до інженерів.

1) Кількість – 6-ть експертів.
2) Графік роботи:

а) робота у три зміни, по 8-м годин кожна;

б) понеділок-п’ятниця:

- 6:00 - 14:00 – 1-а людина;
- 14:00 - 22:00 – 2-і людини;
- 22:00 - 6:00 – 1-а людина;

в) субота-неділя:

- 6:00 - 14:00 – 1-а людина;
- 14:00 - 22:00 – 1-а людина;
- 22:00 - 6:00 – 1-а людина;

г) техпідтримка 24/7.

III. Адміністратор відеонагляду – відповідає за коректну роботу системи відеоспостереження.

1) Кількість – дві людини.
2) Графік роботи:

а) з 9 до 18 понеділок-п’ятниця;

б) вихідні та празники, тільки за умови робот, з відновлення коректної роботи системи.

2.1.3 Вимоги до надійності

Система повинна забезпечувати можливість заміни окремих компонентів обладнання, при виході і строю. Система має бути захищена від перебоїв електроживлення, аварії не повинні сказитися на працездатності

обладнання. Дані повинні бути захищені від втрати чи спотворень, за допомогою резервного копіювання.

2.1.4 Вимоги до захисту інформації від несанкціонованого доступу

Інформація повинна бути доступна тільки авторизованим користувачам. Усі елементи системи повинні обмежувати несанкціонований доступ завдяки надійним логінами і паролям чи ключам шифрування. Інформація має бути захищена від перегляду, підміни, модифікації, знищення не авторизованим користувачем. Також усі пристрої в системі повинні бути подібні з метою безпеки. На обладнанні повинна стояти операційна система з активною підтримкою розробників, які гарантують регулярні виходи патчів безпеки та захист від нових експлойтів. Безпека комп’ютерної системи повинна захищати власників та користувачів обладнання від втручання в особистий простір, завдяки камерам відеонагляду. Мережа повинна блокувати зовнішні підключення до елементів управління.

2.1.5 Вимоги до патентної чистоти

Комп’ютерна система повинна використовувати ліцензійне програмне забезпечення. Елементи системи повинні бути сертифікованими для використання на території України.

2.2 Вимоги до видів забезпечення

2.2.1 Вимоги до інформаційного забезпечення системи

Камери повинні транслювати свій відеопотік, який буде записуватися сервером і зберігатися у виді файлів, за заданий адміністратором період.

Алгоритми шифрування та дешифрування даних, і програмне забезпечення, яке їх реалізує, повинні пройти контроль та бути сертифікованими уповноваженими організаціями

Технічні засоби, які використовуються для зберігання інформації, повинні використовувати надійні, сучасні методи та технології, для забезпечення кращого рівня надійності збереження даних та швидку заміну обладнання.

2.2.2 Вимоги до технічного забезпечення системи

Головний маршрутизатор повинен підтримувати мережеві технології – DHCP, NAT, VPN, Firewall.

Всі мережеві пристрої, повинні підтримувати технологію VLAN. Комутатори повинні забезпечувати швидкість передачі до 100 Мбіт/с.

В цілях полегшення найму обслуговуючого персоналу та збільшення надійності системи, всі маршрутизатори в корпоративній мережі повинні бути від компанії Cisco.

Камери відеонагляду повинні базуватися на мікрокомп’ютері Raspberry Pi 3 та модулю Pi Camera.

FTP сервер для зберігання відеозаписів повинен мати такі параметри:

- об’єм диска 500 ГБ, з можливістю розширення;
- 4-х ядерний процесор з тактовою частотою не менш 2 ГГц;
- 32 ГБ оперативної пам’яті.

2.2.3 Вимоги до організаційного забезпечення системи

Система повинна розмежувати доступ користувачів до інформації. Кожен окремий користувач повинен мати доступ тільки до тої інформації, до якої йому було надано головним адміністратором.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Структура комплексу технічних засобів комп'ютерної системи включає в себе:

- систему відеонагляду в будівлях містечка "Золоті Ключі";
- мережа будівель містечка "Золоті Ключі";
- мережа фінансового відділу "АН ЗОЛОТІ КЛЮЧІ";
- мережа секретаріату "АН ЗОЛОТІ КЛЮЧІ";
- мережа ІТ відділу "АН ЗОЛОТІ КЛЮЧІ";
- мережа комерційного відділу "АН ЗОЛОТІ КЛЮЧІ";
- мережа юридичного відділу "АН ЗОЛОТІ КЛЮЧІ";
- веб сервер;
- FTP сервер.

До структурної схемі входить цілий програмно апаратний комплекс, який базується на мережі. До складу технічних засобів відносяться мережеве обладнання, а саме, маршрутизатори, комутатори, комутаційне обладнання, відносяться серверне обладнання, робочі станції та елементи системи відеоспостереження, такі як камери, чи відеореєстратор.

Виділяються наступні рівні комп'ютерної системи:

1) Рівень ядра – це рівень, який відповідає за маршрутизацію трафіку, рівень ядра поєднує локальні мережі, надає їм доступ одна до одної та пов'язує мережу підприємства з глобальною мережею Інтернет. Також на цьому рівні реалізується поєднання віддалених офісів у одну мережу завдяки VPN.
2) Рівень доступу – це рівень, який формує локальні підмережі LAN, до яких підключені кінцеві пристрої, вони підключаються до

комутаторів, які відповідають як за передачу даних від клієнтів всередині мережі, так і за відправку до інших мереж через рівень ядра. На цьому рівні реалізується мережа VLAN, яка ділить під мережу на сегменти, та протокол PAgP, який служить для .

3) Кінцеві пристрої – кінцеві пристрої, це робочі станції, сервера та камери відеонагляду. Це прилади, з якими взаємодіє користувач фізично, чи через мережу. Також, кінцеві прилади можуть взаємодіяти з один-з-одним без прямого втручання користувача, наприклад в системі “АН ЗОЛОТІ КЛЮЧІ” це сбір відеопотоку з камер, для розташування відеозаписів на сервері FTP.

Проаналізувавши інформацію о технічних заходах було сформовано структурну схеми комплексу технічних засобів комп’ютерної системи. Структурну схему зображено на рисунку 3.1.

3.1.1 Розташування камер на об’єкті відеоспостереження

На даний момент відеонагляд планується встановити у 4-х однотипних будівлях котеджного містечка “Золоті Ключі”.

Камери можуть бути розташовані як надворі, так і всередині будівлі. Всередині будівлі має сенс охороняти лише перший поверх, але ця можливість лише опція, так як це приватна власність, відеозйомка буде заважати життю власників дому і камери всередині будуть встановлюватись тільки за їх бажанням. Надворі, зйомка практично обов’язкова, для запобігання злочину. План будівель з встановленими камерами відеоспостереження зображено на рисунку 3.2

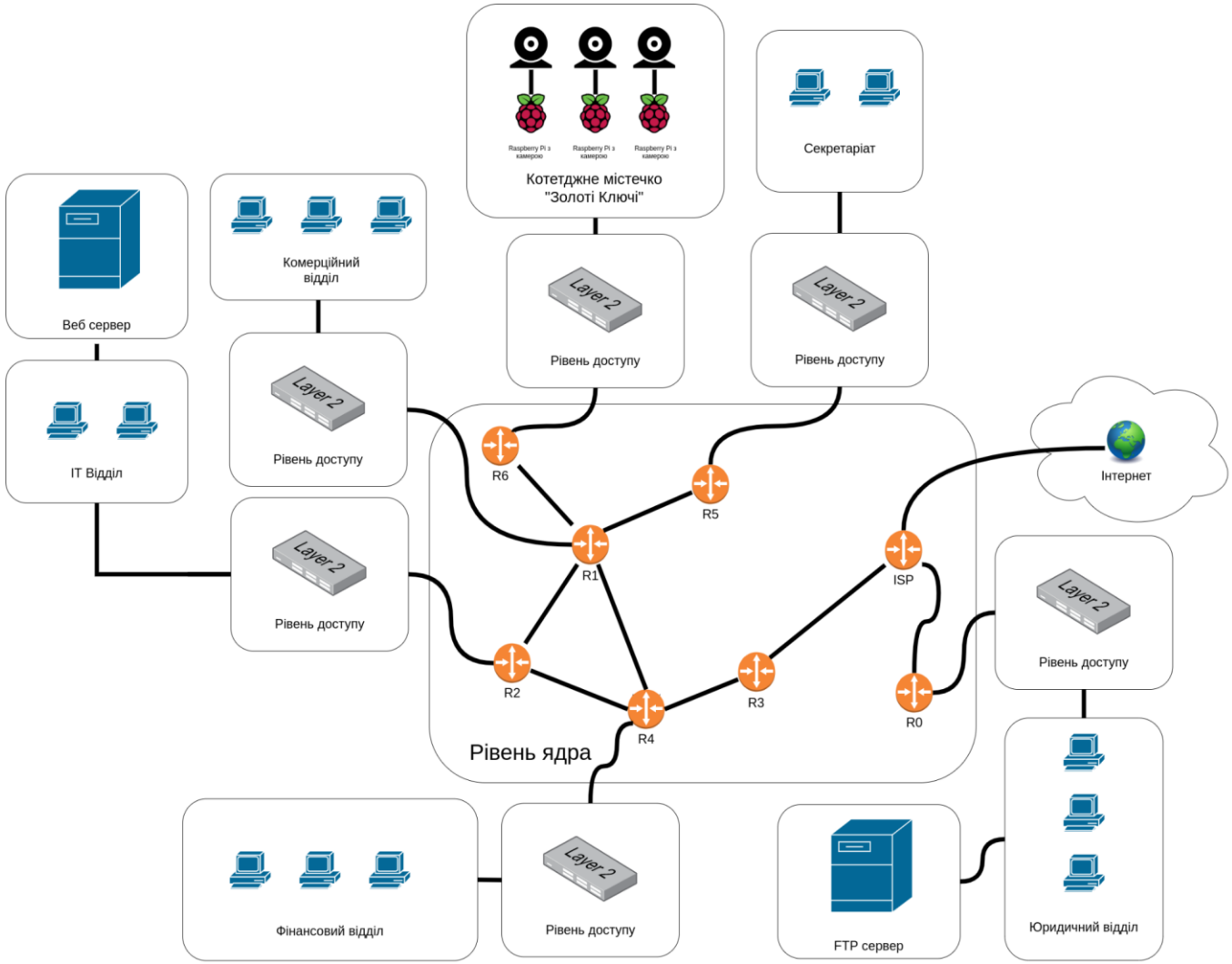

Рисунок 3.1 – Структурна схема комплексу технічних заходів “АН ЗОЛОТІ КЛЮЧІ”

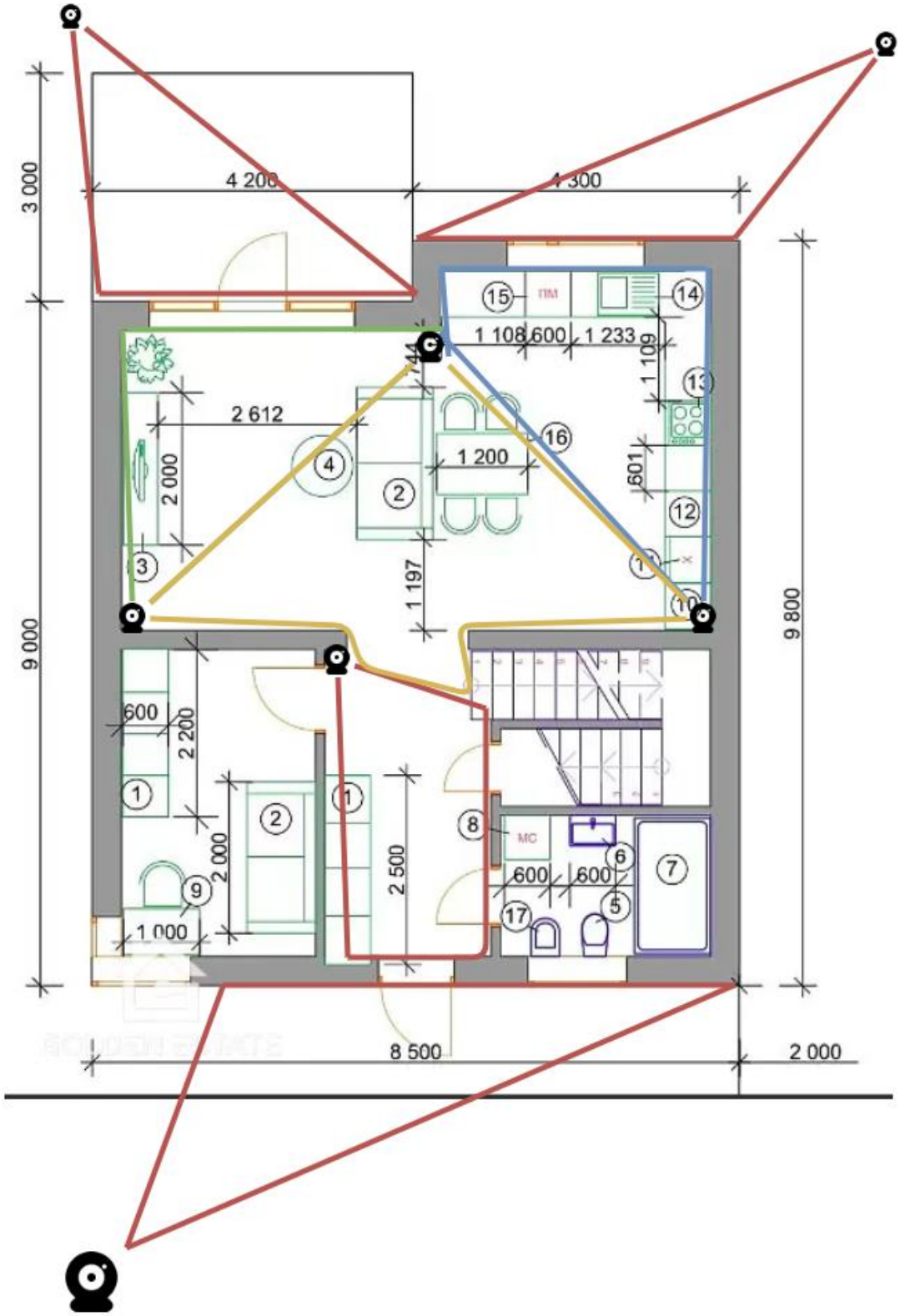

Рисунок 3.2 – План розташування камер у будівлі (перший поверх)

3.1.2 Аналіз входів і виходів

Для вибору та налаштування апаратних засобів потрібно проаналізувати входи та виходи. Було сформовано таблицю 3.1

Таблиця 3.1 – Входи та виходи

Тип	Назва	Функціональне значення
Вхід	Камера (задні двері, двір)	Знаходиться зовні. Знімає задні двері та транслює відеопоток в мережу.
Вхід	Камера (передні двері, двір)	Знаходиться зовні. Знімає передні двері та транслює відеопоток в мережу.
Вхід	Камера (переднє вікно, двір)	Знаходиться зовні. Знімає переднє вікно будівлі та транслює відеопоток в мережу.
Вхід	Камера (коридор, будівля)	Знаходиться всередині. Знімає задні двері та коридор, біля сходів. Транслює відеопоток в мережу.
Вхід	Камера (передні двері, вітальня)	Знаходиться всередині. Знімає передні двері та вітальню. Транслює відеопоток в мережу.
Вхід	Камера (вітальня, коридор)	Знаходиться всередині. Знімає вітальню і коридор. Транслює відеопоток в мережу.
Вхід	Камера (кухня, вікно)	Знаходиться всередині. Знімає кухню та вікно. Транслює відеопоток в мережу.
Вхід	Сервіс приймання відеопотоку	Сервіс займається опросом камер та конвертуванням відеопотоку
Вихід	Сервіс видачі відеопотоку	Сервіс видає зображення з обраної користувачем камери
Вихід	WEB сервер	Надає доступ користувачам до WEB сторінки.
Вихід	FTP сервер	Місце складування записів з камер
Вихід	Кінцевий прилад користувача	Цей прилад користувач використовує для перегляду відеопотоку з камер

3.2 Вибір та характеристики апаратних засобів комп’ютерної мережі

3.2.1 Вибір та характеристика обладнання для IP відеоспостереження

Як вказано у вимогах до системи, для IP відеоспостереження повинен використовуватись мікрокомп'ютер Raspberry Pi. Серед актуального модельного ряду можна виділити моделі вказані у таблиці 3.2.

Таблиця 3.2 – Характеристика модельного ряду Raspberry Pi

Модель	Рік випуску	Процессор	Відеочіп	Тактова частота процесора	Оперативна пам’ять
Pi 3 A+	2018	Broadcom BCM2837B0	Video Core IV 400 МГц	4x1.4 ГГц	512 Мб
Pi 3 B	2016	Broadcom BCM2837	Video Core IV 400 МГц	4x1.2 ГГц	1 Гб
Pi 3 B+	2018	Broadcom BCM2837B0	Video Core IV 400 МГц	4x1.4 ГГц	1 Гб
Pi 4 B	2019	Broadcom BCM2711	Video Core VI	4x1.5 ГГц	1 Гб 2 Гб 4 Гб
Pi Zero W	2017	Broadcom BCM2835	Video Core IV	1x1 ГГц	512 Мб

Передачі відеопотоку по мережі потребує злагодженої роботи відеочіпа та процесора. При обробки зображення навантаження буде падати на відеоядро, а для підтримки каналу та передачі зображення підключеним клієнтам буде працювати процесор. Експериментальним методом було виявлено, що одноядерний процесор, не підійде, тому, що його буде мало для

обслуговування клієнтів при безперервної передачі відеопотоку. Тому Pi Zero W не підходить для вирішення поставленого завдання.

Серед моделей третьої лінійки, а саме – PI 3 A+, PI 3 B та Pi 3 B+, кращим за характеристиками являється PI 3 B+. В моделі PI 3 B+ зібрані найкращі черти моделей PI 3 A+ та Pi 3 B, від PI 3 A+ частота процесора до 1.4 ГГц, а від Pi 3 B більш малий формфактор та об’єм оперативної пам’яті в 1ГБ.

Якщо вибирати між Pi 3 B+ та Pi 4 B, то остаточним рішенням являється Pi 3 B+ в силу меншою ціни та більшої поширеності на ринку. Тому обрано модель Pi 3 B+ , який зображено на рисунку 3.3.

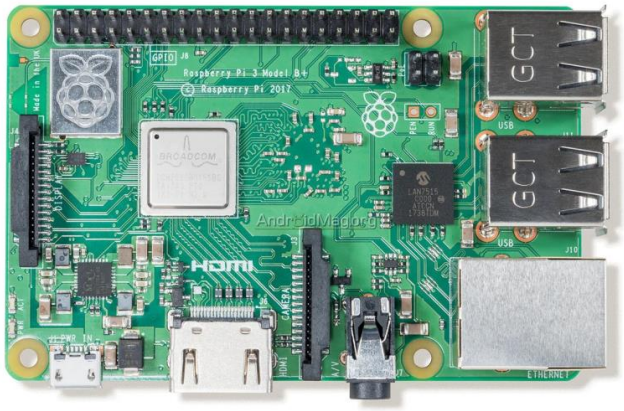

Рисунок 3.3 – модель Pi 3 B+

Також для відеонагляду потрібно придбати модуль камери на Raspberry Pi.

Було обрано модуль Raspberry Pi Camera Module, який зображено на рисунку 3.4, завдяки тому, що ця камера являється ліцензованою розробниками Raspberry Pi, тому являється надійним рішенням для системи.

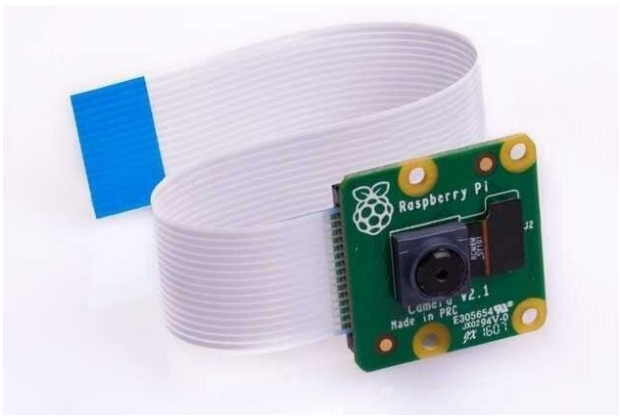

Рисунок 3.4 – Raspberry Pi Camera Module v2.

Характеристики камери:

- максимальний розмір зображення фото: 3280 x 2464 пікселів;
- запис відео з роздільною здатністю: 1080p30, 720p60 та 640x480p90;
- датчик зображення: Sony IMX219.

Для мікрокомп’ютера Raspberry Pi було обрано PoE стандарту 802.3af, як основне джерело живлення. Цей стандарт було обрано в цілях зменшення витрат на монтаж, так як завдяки PoE живлення може бути реалізовано через виту пару. Для реалізації цього виду живлення на Raspberry Pi було обрано модуль POE_BOARD, який зображено на рисунку 3.5.

Характеристика модуля PoE для Raspberry Pi POE_BARD:

- сумісність: Raspberry Pi 4 B та Raspberry Pi 3 B+;
- стандарт: 802.3 af PoE;
- вхідна напруга: від 36В до 56В;
- вихідна напруга: 5В;
- максимальний вихідний струм: 2,5 А;
- керування охолодженням: мікроконтролерне [16].

Рисунок 3.5 – Модуль PoE живлення POE_BOARD

3.2.2 Вибір та характеристика мережевого обладнання

Для реалізації PoE живлення для камер, на стороні мережевого обладнання, було обрано комутатор Mikrotik CRS112-8P-4S-IN, який зображено на рисунку 3.6. Цей комутатор має 8 LAN інтерфейсів з PoE, а також 4 SFP входів.

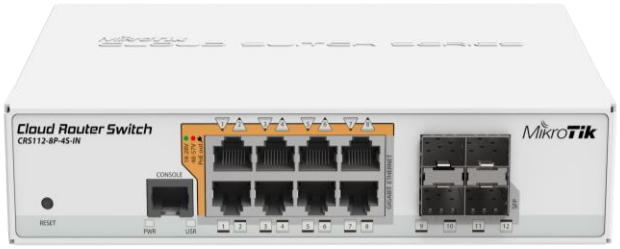

Рисунок 3.6 – Коммутатор Mikrotik CRS112-8P-4S-IN

Характеристики Mikrotik CRS112-8P-4S-IN:

- кількість портів: 13;
- інтерфейси: SFP, Gigabit Ethernet;
- середовище передачі даних: 100BASE-TX: неекранована вита пара категорії 5, оптичний кабель, 10BASE-T: неекранована вита пара катерогій 3, 4, 5, 100BASE-TX / 1000Base-T: неекранована вита пара категорій 5;
- можливість віддаленого управління: керований;
- комутаційна здатність: 24 Гбіт/с;
- швидкість перенаправлення 64-байтних пакетів: 17.86 Mpps;
- стандарт PoE: 802.3af, 802.3at [17].

Для реалізації рівня ядра мережі важливо підібрати маршрутизатори, в яких встановлено SFP інтерфейси для підключення оптики, апаратна підтримка модулів EHWIC, а також програмна підтримка VPN site-to-site. Важливо, щоб маршрутизатор підтримував апаратне шифрування IPSEC.

Найкращим вибором, з даних характеристик, будуть маршрутизатори Cisco 2900, серед яких було обрано маршрутизатор Cisco 2901-SEC/K9, який зображено рисунку 3.7. Особливостями цього маршрутизатора являються – гігабітні Ethernet порти, наявність інтерфейсів SFP, слоти розширення EHWIC.

Харакатеристики:

- Інтерфейси:

  WAN: 2 x 10Base-T / 100Base-TX / 1000Base-T - RJ-45.

  Управління: 1 x консоль - RJ-45.

  Управління: 1 x консоль - mini-USB Type B.

  Управління: 1 x допоміжне - RJ-45.

  Периферія: 2 x високошвидкісний USB - 4-контактний USB типу A.
- Форм-фактор: Монтаж в стійку - модульний - 1U.
- Протокол передачі даних: Ethernet, Fast Ethernet, Gigabit Ethernet.
- Протокол маршрутизації: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, статична маршрутизація IPv4, статична маршрутизація IPv6, маршрутизація на основі політики (PBR).
- Відповідні стандарти: IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag.
- Пам'ять DRAM: 2 ГБ (встановлено) / 2 ГБ (макс.).
- Флеш-пам'ять: 8 ГБ (макс.).
- Потрібна напруга: 120/230 В змінного струму (50/60 Гц).
- Особливості: Захист Firewall, апаратне шифрування IPSEC, підтримка VPN, підтримка MPLS, підтримка системного журналу, фільтрація вмісту, підтримка IPv6, зважена чесна черга на основі класів (CBWFQ), зважена випадкова рання детекція; (WRED), динамічна багатоточкова VPN (DMVPN) [18].

Рисунок 3.7 – Маршрутизатор Cisco 2901-SEC/K9

В якості комутаторів було обрано Cisco SB SF200-24FP, який зображено на рисунку 3.8, так яка цей комутатор підтримує протокол PAgP, для агрегування каналів, якій необхідно застосувати. Комутатор Cisco SB SF200-24FP має 24 інтерфейсів Fast Ethernet, та 2 інтерфейсу Gigabit Ethernet.

Рисунок 3.8 – Коммутатор Cisco SB SF200-24FP

Стандарти: IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100Base-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3E STE, 802.3x IEEE 802.1Q / p VLAN, IEEE 802.1w RSTP, IEEE 802.1X.

Живлення: 100-240В змінного струму, 50-60 Гц.

Пропускна здатність пересилки: 6,55 млн. пакети в секунду.

Загальна кількість мережевих портів: 24 [19].

3.2.3 Вибір та характеристика сервера

За заданими характеристиками, з вимог до комп’ютерної системи, серверне обладнання повинно мати:

– об’єм диска 500 ГБ, з можливістю розширення;

– 4-х ядерний процесор з тактовою частотою не менш 2 ГГц;

– 32 ГБ оперативної пам’яті.

Для виконання цієї задачі було проведено аналіз сучасного серверного обладнання. Висновком цього аналізу являється, що на ринку серверів лідируючу позицію займає фірма DELL. Компанія DELL дає можливість обрати комплектацію серверу під свої нужди. Лінійка R720 дає право на модифікацію комплектації. Для виконання поставлених вимог було обрано сервер Dell R720, який зображено на рисунку 3.9. Базову комплектацію прийшлось модифікувати, сервер укомплектовано – з процесором Xeon E5-2630v2 з 2.6-3.10 ГГц, оперативною пам'яттю 32 Гб, чотирма жорсткими дисками, по 600 Гб кожний, та рейд контролером DELL Perc H710 для забезпечення цілісності інформації, завдяки реалізації 5-го рейд масиву.

Рисунок 3.9 – Сервер Dell R720

Для забезпечення цілісності інформації на сервері, було прийнято рішення включити у список необхідного обладнання – джерело безперебійного живлення. Було проведено аналіз, завдяки якому було обрано фірму APC, завдяки її надійності та гарантії якості. Серед модельного ряду для серверного обладнання було обрано APC Smart-UPS 3000VA LCD, який зображено на рисунок 3.10 з вихідною потужністю в 2700 Вт. Цей ДБЖ гарантує коректне вимкнення серверного обладнання та 17-ть хвилин роботи при навантаженні в 1350 Вт, що являється задовільним для збереження даних та коректного завершення роботи сервера.

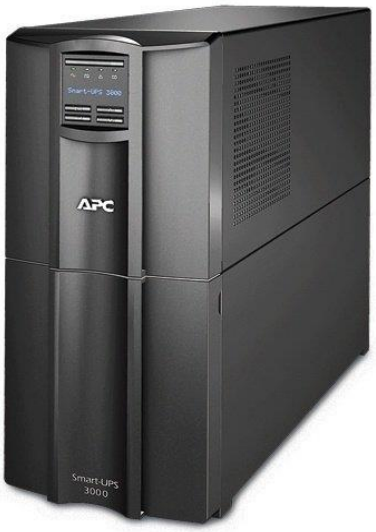

Рисунок 3.10 – APC Smart-UPS 3000VA LCD

Таблиця 3.2 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість
1	2	3	4	5
1	Raspberry Pi 3 B+	мікрокомп’ютер, raspberry pi, raspberry_pi_x	шт	28
2	Raspberry Pi Camera Module v2	камера, pi camera, pi_camera_x	шт	28
3	Коммутатор Mikrotik CRS112-8P-4S-IN	маршрутизатор, mikrotik	шт	4
4	Маршрутизатор Cisco 2901-SEC/K9	маршрутизатор, cisco	шт	6
5	Коммутатор Cisco SB SF200-24FP	коммутатор, cisco	шт	9
6	Сервер Dell R720	сервер, dell	шт	2
7	ДБЖ APC Smart-UPS 3000VA LCD	дбж, apc	шт	2

3.3 Розробка архітектури мережі комп’ютерної системи

Розробка архітектури мережі це один з найголовніших етапів розробки комп’ютерної системи. Архітектура мережі складається з наступних елементів:

- топологія;
- мережеве обладнання;
- протоколи мережі;
- кабельна інфраструктура.

Архітектура мережі “АН ЗОЛОТІ КЛЮЧІ” базується на дворівневій ієрархічній моделі мережі, яка включає в себе рівні – рівень ядра та рівень доступу. Рівень ядра буде базуватись на маршрутизаторах, а рівень доступу на комутаторах.

Всього в топології буде сім маршрутизаторів, та Інтернет провайдер. Шість маршрутизаторів будуть знаходитись на території містечка “Золоті Ключі”, один з яких повинен забезпечувати роботу відеонагляду в будівлях котеджного містечка, а інші п’ять знаходяться в офісній будівлі, їх задача відповідати за роботу підприємства “АН ЗОЛОТІ КЛЮЧІ”. Також в підприємстві є віддалений офіс, в якому працюють юристи, він знаходиться в окремій будівлі, та буде під’єднаний до мережі підприємства завдяки side-to-side VPN. Для забезпечення маршрутизації буде використано протокол динамічної маршрутизації EIGRP.

Виділяється п'ять підмереж кінцевих пристроїв для підприємства “АН ЗОЛОТІ КЛЮЧІ” та ще дві додаткові для котеджного містечка “Золоті Ключі”.

ІТ відділ потребує підвищення швидкості передачі даних та рівня надійності на рівні доступу, так як там буде стояти WEB сервер для перегляду відеокамер, тому було прийнято рішення застосувати технологію агрегації каналів PAgP.

Підмережа комерційного відділу буде розбита на чотири віртуальні підмережі VLAN30 (для маркетингу) , VLAN40 (для реклами), VLAN50 (для ріелторів) та VLAN99 для керування мережевими пристроями. Також на VLAN буде розбита підмережа для домівок в котеджному містечку. Будуть використані наступні VLAN для будівель – VLAN10, VLAN11, VLAN12, VLAN13. Для доступу до мережевого обладнання буде використано VLAN99.

В віддаленому офісі юридичного відділу буде стояти FTP сервер. В головному офісі підприємства “АН ЗОЛОТІ КЛЮЧІ” в наявності є два сервера, які потрібно буде застосувати як RADIUS та DNS. RADIUS сервер буде стояти в підмережі секретаріату, а DNS сервер буде поставлений в віртуальній підмережі комерційного відділу під тегом VLAN50.

З прийнятих рішень, які базуються на заданих вимогах, було розроблено топологічну схему архітектури мережі “АН ЗОЛОТІ КЛЮЧІ” , як зображена на рисунку 3.11.

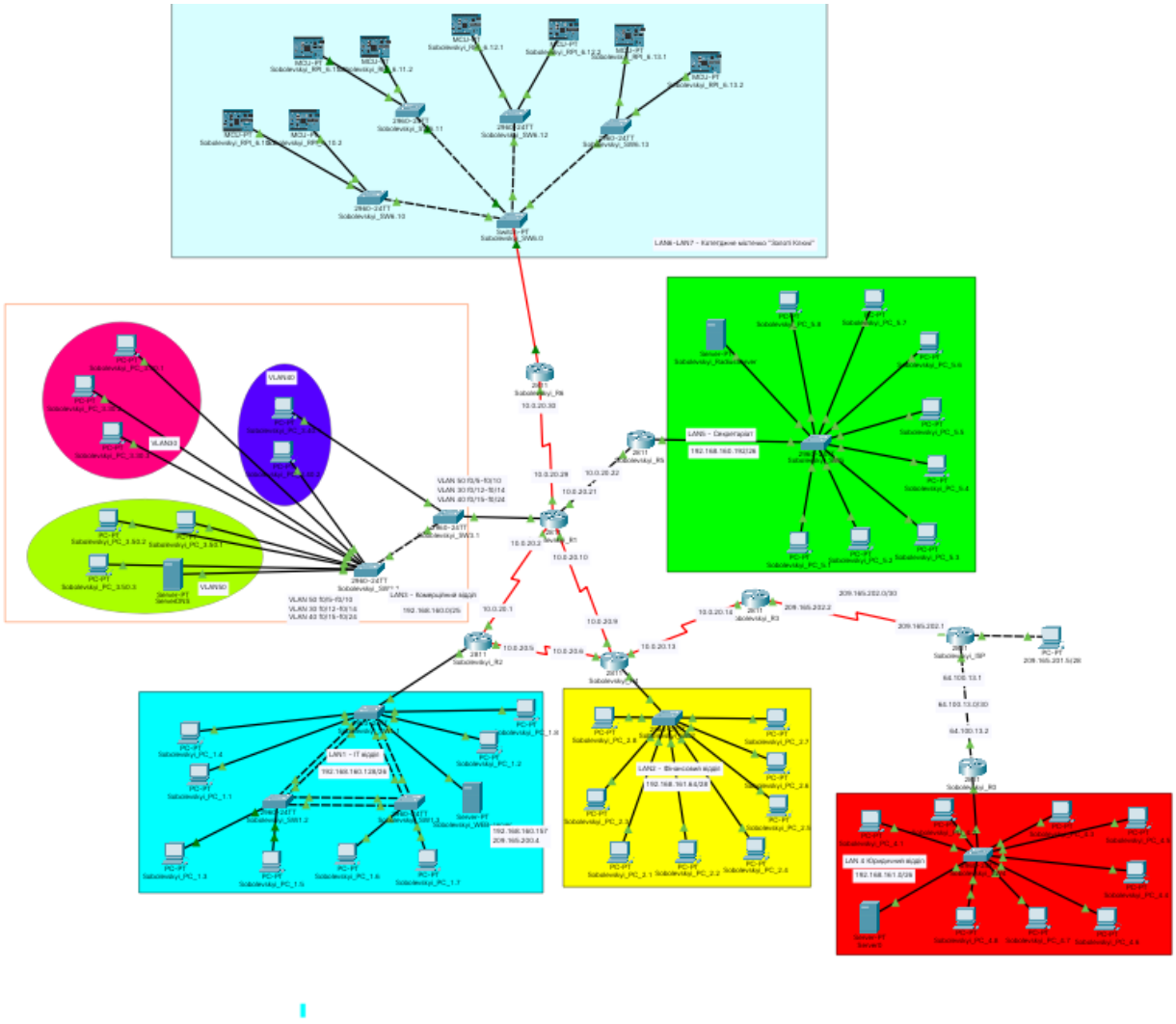

Рисунок 3.11 – Архітектура мережі “АН ЗОЛОТІ КЛЮЧІ”

3.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Для розрахунку інтенсивності трафіку дано:

- Кількість вузлів в найбільшій мережі: 86;
- Середня інтенсивність трафіку: μ=103 (кадрів/с);
- Середня довжина повідомлення: l=650 байт;
- Вимоги до затримки передачі пакету – ≤6 мс.

Рішення:

Для початку, треба розрахувати пропускну здатність мережі. Розрахунок для рівню доступу:

$Pp.p=\mu \cdot l \cdot n \cdot 8=103 \cdot 650 \cdot 24 \cdot 8/1000000=12.85$ (Мбіт/с)

n=24 (кількість портів комутатора)

Розрахунок загального навантаження на коммутатор при підключенні через лінію 100 Мбіт/с:

$\mu_{вих}=100\ 000\ 000/(650 \cdot 8)=19230$ (пакетів/с)

Так як, середня інтенсивність трафіку μ=103, то до комутатора рівня розподілу можна приєднати максимум:

N=19230/103=186 вузлів.

Для мережі з кількістю вузлів 86, це є більш ніж задовільно.

Розрахунок інтенсивності трафіку від всіх користувачів:

$\lambda=n \cdot \mu=86 \cdot 103=8858$ (пакетів/с).

Розрахунок коефіцієнту затримки на рівні розподілу:

$\rho=\lambda/\mu_{вих}=8858/19230=0,46$

Розрахунок коефіцієнту зайнятості комутатора, на рівні розподілу:

$r=\rho/(1-\rho)=0,46/(1-0,46)=0,85$

Розрахунок середньої затримки кадру:

$T=1/((\mu_{вих}-\lambda))=1/(19230-8858)=9,64*10^{-5}$ с

Розрахунок середньої довжини черги:

$L_{черги}=\rho\text{^}2/(1-\rho)=(0,46^2/(1-0,46)=0,39$

Розрахунок середнього часу перебування пакета в черзі:

$T_{очік}=L_{черги}/\lambda=0,39/8858=0.044028$ мс.

Значення $T_{очік}$ менше ніж задане у вимогах (6 мс). Вимоги вважаються виконаними.

Розрахунок пропускної здатності каналу:

$\lambda=b/l$

$b=\lambda \cdot l=(8858 \cdot 650 \cdot 8) \cdot 10^{-6}=46$ Мбіт/с

Пропускна здатність каналу задовольняє вихідний канал 100Мбіт/с.

4 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ

4.1 Розрахунок схеми адресації комп'ютерної мережі

Для перевірки комп'ютерної системи, необхідно спроектувати комп'ютерну мережу, згідно заданої структури, рисунок 3.12,+ в програмі Packet Tracer. Для розробки мережі виділений блок адрес з підмережі 192.168.160.0/21.

Кількість вузлів приведена в таблиці 4.1. Паролі на пристрої приведені в таблиці 4.2.

Таблиця 4.1 – Кількість вузлів у підмережах

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6 (додатково)	LAN 7 (додатково)
55	12	86	40	50	70	24

LAN 1 – IT відділ

LAN 2 – Фінансовий відділ

LAN 3 – Комерційний відділ

LAN 4 – Юридичний відділ

LAN 5 – Секретаріат

LAN 6 – Житлові будинки з відеонаглядом

LAN 7 – Управління мережевим обладнанням в котеджному містечку

Таблиця 4.2 – Паролі на пристрої

Консоль і vty	Привілейований режим	Користувач
cisco	class	12317_Sobolevskyi

Для комп’ютерної мережі було видано блок IP адрес 192.168.160.0/21. Цей блок потрібно розбити на п’ять підмереж, які являються різними за розміром. Розміри підмереж вказані в таблиці 4.1.

Для з’єднання маршрутизаторів використовується окрема адресація з підмережі 10.1.20.0/24. Такі підмережі будуть містити в собі лише два хоста, тому, для них, буде найкращим рішенням використовувати маску 255.255.255.252.

Розрахунок підмереж з різною кількістю вузлів найкраще всього буде вести методом VLSM, який передбачає під собою розбивання великої підмережі на менші, до тих пір поки кількість хостів не буде задовільною. Цей метод дозволяє створювати підмережі різних розмірів, для використовування VLSM потрібно знати необхідну кількість вузлів для кожної підмережі.

Блок адрес 192.168.160.0/21 може містити в собі 2046 пристроїв, але для потреб комп’ютерної системи потрібно лише 243 вузла. Для того, щоб порахувати кількість виділяємих адрес, потрібно відсортувати адреси у порядку вибування. Порядок вибування – LAN 3 (86 вузлів), LAN 1 (55 вузлів), LAN 5 (50 вузлів), LAN 4 (40 вузлів), LAN 2 (12 вузлів). Блоки адрес LAN 6 та 7 будуть обчислюватись окремо.

1) LAN 3 (86 вузлів) – найближча кількість адресів 128, префікс 25, мережа 192.168.160.0/25.
2) LAN 1 (55 вузлів) – найближча кількість адресів 64, префікс 26, мережа 192.168.160.128/26.
3) LAN 5 (50 вузлів) – найближча кількість адресів 64, префікс 26, мережа 192.168.160.192/26.
4) LAN 4 (40 вузлів) – найближча кількість адресів 64, префікс 26, мережа 192.168.161.0/26.
5) LAN 2 (12 вузлів)– найближча кількість адресів 16, префікс 28, мережа 192.168.161.64/28.

   Мережа LAN 1 (55 вузлів):

   – мережа: 192.168.160.128/26;

- маска: 255.255.255.192;
- діапазон: 192.168.160.129 – 192.168.160.190;
- кількість вузлів: 62;
- широкомовна адреса: 192.168.160.191.

В мережі LAN1 адресою шлюза буде IP 192.168.160.129. В мережі LAN1 зайнятий простір вузлів – 55, доступний, за вирахуванням маршрутизатора, – 61, тобто в запасі остається 6 адресів.

Мережа LAN 2 (12 вузлів):

- мережа: 192.168.161.64/28;
- маска: 255.255.255.240;
- діапазон: 192.168.161.65 – 192.168.161.78;
- кількість вузлів: 14;
- широкомовна адреса: 192.168.161.79.

Мережа LAN 3 (86 вузлів):

- мережа: 192.168.160.0/25;
- маска: 255.255.255.128;
- діапазон: 192.168.160.1 – 192.168.160.126;
- кількість вузлів: 126;
- широкомовна адреса: 192.168.160.127.

Мережа LAN 4 (40 вузлів):

- мережа: 192.168.161.0/26;
- маска: 255.255.255.192;
- діапазон: 192.168.161.1 – 192.168.161.62;
- кількість вузлів: 62;
- широкомовна адреса: 192.168.161.63.

Мережа LAN 5 (50 вузлів):

- мережа: 192.168.160.192/26;
- маска: 255.255.255.192;
- діапазон: 192.168.160.193 – 192.168.160.254;

– кількість вузлів: 62;

– широкомовна адреса: 192.168.160.255.

Мережа LAN 6 буде використовуватись під домівки в житловому містечку, а мережа LAN 7 буде використовуватись під доступ по мережевих пристроїв.

Мережа LAN 6 (70 вузлів):

– мережа: 192.168.161.128/25;

– маска: 255.255.255.128;

– діапазон: 192.168.165.129 – 192.168.165.254;

– кількість вузлів: 126;

– широкомовна адреса: 192.168.165.127.

Мережа LAN 7 (24 вузла):

– мережа: 192.168.161.96/27;

– маска: 255.255.255.224;

– діапазон: 192.168.161.97 – 192.168.165.126;

– кількість вузлів: 30;

– широкомовна адреса: 192.168.165.127.

Схема адресації мережі вказана в таблиці 4.3.

Таблиця 4.3 − Схема адресації мережі

Назва мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
1	2	3	4	5	6
LAN 1	55	192.168.160.128	255.255.255.192	192.168.160.129	192.168.160.190
LAN 2	12	192.168.161.64	255.255.255.240	192.168.161.65	192.168.161.78
LAN 3	86	192.168.160.0	255.255.255.128	192.168.160.1	192.168.160.126
LAN 4	40	192.168.161.0	255.255.255.192	192.168.161.1	192.168.161.62

Продовження таблиці 4.3

1	2	3	4	5	6
LAN 5	50	192.168.160.192	255.255.255.192	192.168.160.193	192.168.160.254
LAN 6	70	192.168.161.128	255.255.255.128	192.168.161.129	192.168.165.254
LAN 7	24	192.168.161.96	255.255.255.224	192.168.161.97	192.168.165.126
WAN 1	2	10.0.20.0	255.255.255.252	10.0.20.1	10.0.20.2
WAN 2	2	10.0.20.4	255.255.255.252	10.0.20.5	10.0.20.6
WAN 3	2	10.0.20.8	255.255.255.252	10.0.20.9	10.0.20.10
WAN 4	2	10.0.20.12	255.255.255.252	10.0.20.13	10.0.20.14
WAN 5	2	10.0.20.16	255.255.255.252	10.0.20.17	10.0.20.18
WAN 6	2	10.0.20.20	255.255.255.252	10.0.20.21	10.0.20.22
WAN 7	2	10.0.20.24	255.255.255.252	10.0.20.25	10.0.20.26
WAN 8	2	10.0.20.28	255.255.255.252	10.0.20.29	10.0.20.30

Схема адресації пристроїв вказана в таблиці 4.4.

4.2 Налаштування та перевірка роботи комп’ютерної системи

4.2.1 Базове налаштування конфігурації пристроїв

Згідно до вимог, була налаштована базова конфігурація пристроїв комп'ютерної системи.

Базова конфігурація пристроїв включає в себе:

- встановлення назв пристроям
- встановлення паролів для входу vty та консоль;
- встановлення паролів для входу в привілейований режим;
- шифрація паролів, які зберігаються у відкритому вигляді;
- налаштування банеру MOTD;

Таблиця 4.4 − Схема адресації пристроїв

Пристрій	Інерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
1	2	3	4	5	6	7
Sobolevskyi_R0	F0/0	64.100.13.2	255.255.255.252	-	-	F0/0
	F0/1	192.168.161.1	255.255.255.192	192.168.161.1	-	F0/1
Sobolevsky_SW4	Vlan1	192.168.161.2	255.255.255.192	-	1	-
Sobolevskyi_R1	F0/0	10.0.20.21	255.255.255.252	-	-	F0/0
	S0/1/0	10.0.20.29	255.255.255.252	-	-	S0/3/0
	S0/2/0	10.0.20.10	255.255.255.252	-	-	S0/3/0
	S0/3/0	10.0.20.2	255.255.255.252	-	-	S0/3/0
	F0/1.30	192.168.160.97	255.255.255.224	-	30	-
	F0/1.40	192.168.160.33	255.255.255.224	-	40	-
	F0/1.50	192.168.160.65	255.255.255.224	-	50	-

Продовження таблиці 4.3

1	2	3	4	5	6	7
	F0/1.99	192.168.160.1	255.255.255.224	-	99	-
Sobolevskyi_SW3.1	Vlan99	192.168.160.2	255.255.255.224	192.168.160.1	99	-
Sobolevskyi_SW3.2	Vlan99	192.168.160.3	255.255.255.224	192.168.160.1	99	-
Sobolevskyi_R2	S0/1/0	10.0.20.5	255.255.255.252	-	-	S0/2/0
	S0/3/0	10.0.20.1	255.255.255.252	-	-	S0/3/0
	F0/0	192.168.160.129	255.255.255.192	-	-	F0/24
Sobolevskyi_SW1.1	Vlan1	192.168.160.130	255.255.255.192	192.168.160.129	1	-
Sobolevskyi_SW1.2	Vlan1	192.168.160.131	255.255.255.192	192.168.160.129	1	-
Sobolevskyi_SW1.3	Vlan1	192.168.160.132	255.255.255.192	192.168.160.129	1	-
Sobolevskyi_R3	S0/2/0	10.0.20.14	255.255.255.252	-	-	S0/1/0
	S0/3/0	209.165.202.2	255.255.255.252	-	-	S0/2/0

Продовження таблиці 4.3

1	2	3	4	5	6	7
Sobolevskyi_R4	S0/1/0	10.0.20.13	255.255.255.252	-	-	S0/2/0
	S0/2/0	10.0.20.6	255.255.255.252	-	-	S0/1/0
	F0/0	192.168.161.65	255.255.255.240	-	-	F0/1
Sobolevskyi_SW2	Vlan1	192.168.161.66	255.255.255.240	192.168.161.65	1	-
Sobolevskyi_R5	F0/0	10.0.20.22	255.255.255.252	-	-	F0/0
	F0/1	192.168.160.193	255.255.255.192	-	-	F0/1
Sobolevskyi_SW2	Vlan1	192.168.160.194	255.255.255.192	192.168.160.193	1	-
Sobolevskyi_R6	G0/2/0	-	-	-	-	G9/1
	G0/2/0.10	192.168.161.129	255.255.255.224	-	10	-
	G0/2/0.11	192.168.161.161	255.255.255.224	-	11	-
	G0/2/0.12	192.168.161.193	255.255.255.224	-	12	-

Кінець таблиці 4.3

	G0/2/0.13	192.168.161.225	255.255.255.224	-	13	-
	G0/2/0.100	192.168.161.97	255.255.255.224	-	100	-
Sobolevskyi_SW6.0	Vlan100	192.168.161.98	255.255.255.224	192.168.161.97	100	-
Sobolevskyi_SW6.10	Vlan10	192.168.161.130	255.255.255.224	192.168.161.97	100	-
Sobolevskyi_SW6.11	Vlan11	192.168.161.162	255.255.255.224	192.168.161.161	100	-
Sobolevskyi_SW6.12	Vlan12	192.168.161.130	255.255.255.224	192.168.161.97	100	-
Sobolevsyi_SW6.13	Vlan13	192.168.161.130	255.255.255.224	192.168.161.97	100	-

- назначити на усіх лініях vty використання протоколу ssh;
- налаштування в якості імені домена − ім’я пристрою;
- для шифрування даних створити ключ RSA завдовжки 1024 біт;
- на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000;

Приклад налаштування базової конфігурації на маршрутизаторі Sobolevskyi_R1:

Вхід в привілейований режим:

Router>enable

Вхід в режим конфігурації:

Router#configure terminal

Налаштування назви пристрою:

Router(config)#hostname Sobolevskyi_R1

Встановлення паролю на привілейований режим:

Sobolevskyi_R1(config)#enable password class

Створення користувача:

Sobolevskyi_R1(config)#username 12317_Sobolevskyi password cisco

Встановлення доменного ім’я:

Sobolevskyi_R1(config)#ip domain-name Sobolevskyi_R1

Встановлення банеру:

Sobolevskyi_R1(config)#banner motd # 123-17-1 Sobolevskyi WELCOME #

Генерація ключа шифрування RSA:

Sobolevskyi_R1(config)#*crypto key generate rsa general-keys modulus 1024*

Встановлення паролю на консоль:

Sobolevskyi_R1(config)#line con 0

Sobolevskyi_R1(config-line)#password cisco

Sobolevskyi_R1(config-line)#login

Встановлення паролю на лінії vty:

Sobolevskyi_R1(config-line)#line vty 0 4

Sobolevskyi_R1(config-line)#password cisco

Sobolevskyi_R1(config-line)#login

Налаштування SSH:

Sobolevskyi_R1(config-line)#transport input ssh

Sobolevskyi_R1(config-line)#line vty 5 15

Sobolevskyi_R1(config-line)#password cisco

Sobolevskyi_R1(config-line)#login

Sobolevskyi_R1(config-line)#transport input ssh

Налаштування шифрування паролів:

Sobolevskyi_R1(config-line)#service password-encryption

Перенесення конфігурації у постійну пам’ять:

Sobolevskyi_R1#copy running-config startup-config

4.2.2 Налаштування маршрутизаторів корпоративної мережі

За технічними вимогами мережа підприємства “АН ЗОЛОТІ КЛЮЧІ” повинна базуватись на динамічній маршрутизації. Як протокол динамічної маршрутизації було обрано EIGRP. Мережа буде базуватись на розрахунках, які приведено у таблиці 4.3. Головною перевагою протоколу EIGRP являється висока масштабованість мережі.

Для налаштування протоколу EIGRP на маршрутизаторах треба оголосити безпосередньо підключенні мережі та встановити оновлення маршрутизації.

Приклад налаштування маршрутизації на Sobolevskyi_R5 (рисунок 4.1):

Sobolevskyi_R5(config)#router eigrp 20

Sobolevskyi_R5(config-router)#network 192.168.160.192 0.0.0.63

Sobolevskyi_R5(config-router)#network 10.0.20.20 0.0.0.3

Sobolevskyi_R5(config-router)#network 10.0.20.20 0.0.0.3

За вимогами потребується налаштування пропускної спроможності на serial-інтерфейсах 128 Кб/с. Приклад Sobolevskyi_R1:

Sobolevskyi_R1(config)#interface Serial0/2/0

Sobolevskyi_R1(config-if)#bandwidth 128

```
Gateway of last resort is 10.0.20.14 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
D       10.0.20.0/30 [90/21024000] via 10.0.20.5, 01:59:03, Serial0/2/0
                     [90/21024000] via 10.0.20.10, 01:59:02, Serial0/3/0
C       10.0.20.4/30 is directly connected, Serial0/2/0
L       10.0.20.6/32 is directly connected, Serial0/2/0
C       10.0.20.8/30 is directly connected, Serial0/3/0
L       10.0.20.9/32 is directly connected, Serial0/3/0
C       10.0.20.12/30 is directly connected, Serial0/1/0
L       10.0.20.13/32 is directly connected, Serial0/1/0
D       10.0.20.20/30 [90/20514560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       10.0.20.24/30 [90/27392000] via 10.0.20.14, 01:59:02, Serial0/1/0
D       10.0.20.28/30 [90/21024000] via 10.0.20.10, 01:59:02, Serial0/3/0
     192.168.160.0/24 is variably subnetted, 6 subnets, 2 masks
D       192.168.160.0/27 [90/20514560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.160.32/27 [90/20514560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.160.64/27 [90/20514560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.160.96/27 [90/20514560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.160.128/26 [90/20514560] via 10.0.20.5, 01:59:04, Serial0/2/0
D       192.168.160.192/26 [90/20517120] via 10.0.20.10, 01:59:02, Serial0/3/0
     192.168.161.0/24 is variably subnetted, 7 subnets, 4 masks
D EX    192.168.161.0/26 [170/20768000] via 10.0.20.14, 01:59:02, Serial0/1/0
C       192.168.161.64/28 is directly connected, FastEthernet0/0
L       192.168.161.65/32 is directly connected, FastEthernet0/0
D       192.168.161.128/27 [90/21026560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.161.160/27 [90/21026560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.161.192/27 [90/21026560] via 10.0.20.10, 01:59:02, Serial0/3/0
D       192.168.161.224/27 [90/21026560] via 10.0.20.10, 01:59:02, Serial0/3/0
D*EX 0.0.0.0/0 [170/20768000] via 10.0.20.14, 01:59:02, Serial0/1/0
```

Рисунок 4.1 – Маршрути до всіх підмережей налаштовано

4.2.3 Налаштування роботи Інтернет

Для підключення мережі інтернет було обрано провайдера DTS. Цей провайдер виконує підключення корпоративних клієнтів та гарантує якість техпідтримки.

Для налаштування доступу в мережу Інтернет потрібно налаштувати NAT. Вимоги для налаштування NAT:

- ім’я пула: Internet;
- пул адресів: 209.165.200.5 по 209.165.200.30;
- номер списку доступу 20;
- внутрішня адреса HTTP сервера: 209.165.200.4;
- зовнішня адреса HTTP сервера: 209.165.200.4.

Налаштування динамічного NAT на маршрутизаторі *Sobolevskyi_R3*:

Sobolevskyi_R3(config)#access-list 20 permit 192.168.160.0 0.0.7.255

Sobolevskyi_R3(config)#ip nat inside source list 20 pool Internet

Налаштування статичного nat для WEB сервера на маршрутизаторі *Sobolevskyi_R3*:

Sobolevskyi_R3(config)#ip nat inside source static 192.168.160.157 209.165.200.4

4.2.4 Налаштування агрегування каналів PAgP

Пропріетарний протокол компанії CISCO – PAgP потрібен для агрегування каналів. Цей протокол агрегує фізичні інтерфейси в один, для збільшення пропускної здатності та посилення надійності каналу.

Налаштування PAgp буде виконуватися на комутаторах Sobolevskyi_SW1.1, Sobolevskyi_SW1.2 та Sobolevskyi_SW1.3.

Налаштування PAgP Port-channel 1 на Sobolevskyi_SW1.1:

Sobolevskyi_SW1.1(config)#interface range f0/1-2
Sobolevskyi_SW1.1(config-if-range)#switchport mode trunk
Sobolevskyi_SW1.1(config-if-range)#channel-group 1 mode auto
Sobolevskyi_SW1.1(config-if-range)#interface Port-channel 1
Sobolevskyi_SW1.1(config-if)#switchport mode trunk

Налаштування PAgP Port-channel 3 на Sobolevskyi_SW1.1:

Sobolevskyi_SW1.1(config)#interface range f0/5-6
Sobolevskyi_SW1.1(config-if-range)#switchport mode trunk
Sobolevskyi_SW1.1(config-if-range)#channel-group 3 mode auto
Sobolevskyi_SW1.1(config-if-range)#interface Port-channel 3
Sobolevskyi_SW1.1(config-if)#switchport mode trunk

Налаштування PAgP Port-channel 1 на Sobolevskyi_SW1.2:

Sobolevskyi_SW1.2(config-if)#interface range f0/1-2
Sobolevskyi_SW1.2(config-if-range)#channel-group 1 mode desirable
Sobolevskyi_SW1.2(config-if-range)#interface Port-channel 1
Sobolevskyi_SW1.2(config-if)#switchport mode trunk

Налаштування PAgP Port-channel 2 на Sobolevskyi_SW1.2:

Sobolevskyi_SW1.2(config)#interface range f0/3-4

Sobolevskyi_SW1.2(config-if-range)#channel-group 2 mode desirable

Sobolevskyi_SW1.2(config)#interface Port-channel 2

Sobolevskyi_SW1.2(config-if)#switchport mode trunk

Налаштування PAgP Port-channel 2 на Sobolevskyi_SW1.3:

Sobolevskyi_SW1.3(config-if)#interface range f0/3-4

Sobolevskyi_SW1.3(config-if-range)#channel-group 2 mode auto

Sobolevskyi_SW1.3(config-if-range)#interface Port-channel 2

Sobolevskyi_SW1.3(config-if)#switchport mode trunk

Налаштування PAgP Port-channel 3 на Sobolevskyi_SW1.3:

Sobolevskyi_SW1.3(config)#interface range f0/5-6

Sobolevskyi_SW1.3(config-if-range)#channel-group 3 mode desirable

Sobolevskyi_SW1.3(config)#interface Port-channel 3

Sobolevskyi_SW1.3(config-if)#switchport mode trunk

Для перевірки налаштування потрібно ввести команду:

Sobolevskyi_SW1.1#show etherchannel summary

Вивід команди (рисунок 4.2) повинен показувати протокол PAgP, порти, які входять до груп та статуси активних каналів SU - активний канал L2, SD - зарезервований канал L2. Налаштований протокол PAgP в Packet Tracer (рисунок 4.3).

```
Sobolevskyi_SW1.1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Po1(SD)         PAgP   Fa0/1(P) Fa0/2(P)
3      Po3(SU)         PAgP   Fa0/5(P) Fa0/6(P)
Sobolevskyi_SW1.1#
```

Рисунок 4.2 – Перевірка налаштування PAgP

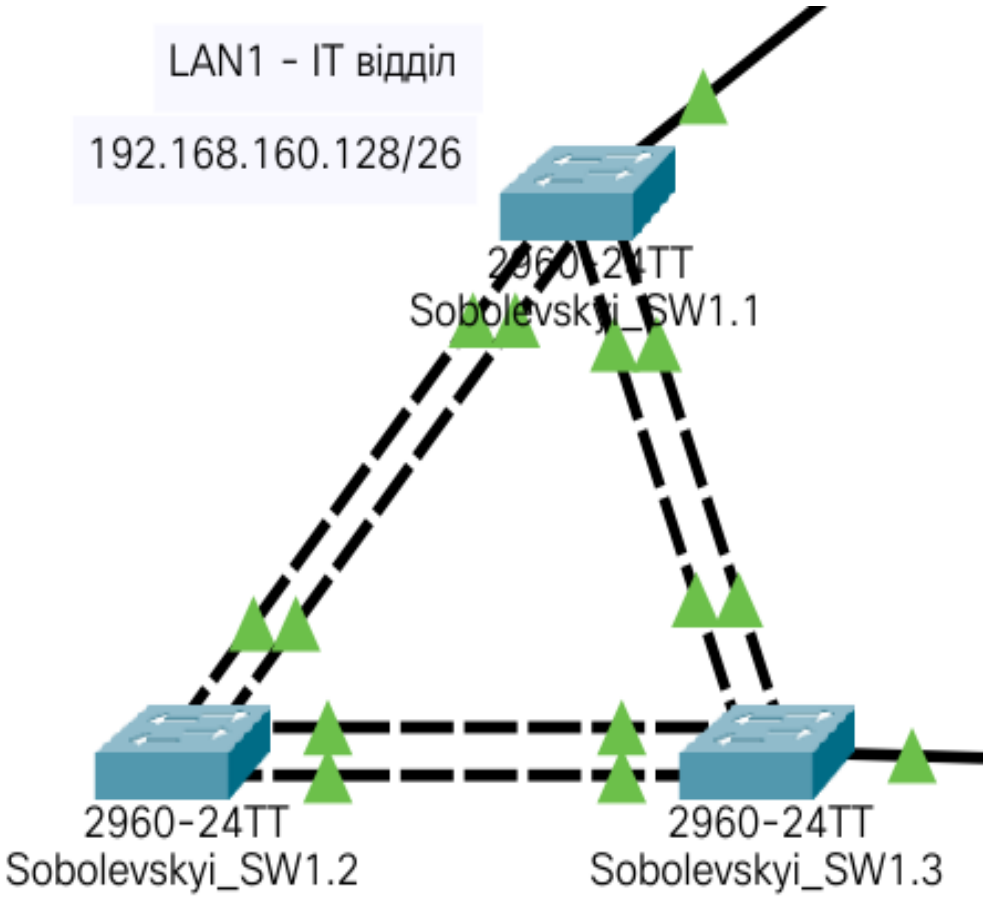

Рисунок 4.3 – Налаштований протокол PAgP

4.2.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Для налаштування side-to-side VPN мережі буде використовуватись протокол GRE, який буде зашифровано IPSEC ключом.

Налаштування gre side-to-side vpn Sobolevskyi_R0:

Sobolevskyi_R0(config)#interface Tunnel0

Sobolevskyi_R0(config-if)#ip address 10.0.20.26 255.255.255.252

Sobolevskyi_R0(config-if)#tunnel destination 209.165.202.2

Sobolevskyi_R0(config-if)#tunnel source FastEthernet 0/0

Sobolevskyi_R3(config)# access-list 130 permit gre host 64.100.13.2 host 209.165.202.2

Sobolevskyi_R0(config)#crypto isakmp policy 1

Sobolevskyi_R0(config-isakmp)#authentication pre-share

Sobolevskyi_R0(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0

Sobolevskyi_R0(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac

Sobolevskyi_R0(config)# mode transport

Sobolevskyi_R0(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

Sobolevskyi_R0(config)#crypto map vpn 10 ipsec-isakmp

Sobolevskyi_R0(config-crypto-map)#set peer 209.165.202.2

Sobolevskyi_R0(config-crypto-map)#set transform-set strong

Sobolevskyi_R0(config-crypto-map)#match address 130

Налаштування gre side-to-side vpn Sobolevskyi_R3:

Sobolevskyi_R3(config)#interface Tunnel0

Sobolevskyi_R3(config-if)#ip address 10.0.20.25 255.255.255.252

Sobolevskyi_R3(config-if)#tunnel destination 64.100.13.2

Sobolevskyi_R3(config-if)#tunnel source Se0/3/0

Sobolevskyi_R3(config)# access-list 130 permit gre host 209.165.202.2 host 64.100.13.2

Sobolevskyi_R3(config)#crypto isakmp policy 1

Sobolevskyi_R3(config-isakmp)# authentication pre-share

Sobolevskyi_R3(config-isakmp)#crypto isakmp key cisco123 address 0.0.0.0

Sobolevskyi_R3(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac

Sobolevskyi_R3(config)#mode transport

Sobolevskyi_R0(config)#crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

Sobolevskyi_R3(config)#crypto map vpn 10 ipsec-isakmp

Sobolevskyi_R3(config-crypto-map)#set peer 64.100.13.2

Sobolevskyi_R3(config-crypto-map)#set transform-set strong

Sobolevskyi_R3(config-crypto-map)# match address 130

Для перевірки ipsec шифрування в тунелю GRE потрібно ввести команду *show crypto ipsec sa* (рисунок 4.4).

```
Sobolevskyi_R3#show crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: CMAP, local addr 209.165.202.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.160.128/255.255.255.192/0/0)
   remote  ident (addr/mask/prot/port): (192.168.161.0/255.255.255.192/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.202.2, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0x0(0)
```

Рисунок 4.4 – Налаштований протокол PAgP

4.2.6 Перевірка роботи комп’ютерної системи

Для перевірки комп’ютерної системи потрібно провести діагностику завдяки програмі ping на комп’ютерах підприємства, та використати встроєні методи Packet Tracer для діагностики трафіку.

Для перевірки буде використовуватись хост Sobolevskyi_PC_5.7, з якого буде виконуватись команда ping у мережі LAN. Спочатку потрібно перевірити доступність серверів. Результат перевірки FTP серверу в юридичному відділі наведено на рисунок 4.5. Результат перевірки WEB серверу в IT відділі наведено на рисунок 4.6. Результат перевірки RADIUS серверу в мережі секретаріату наведено на рисунок 4.7. Результат перевірки DNS серверу в мережі комерційного відділу, з тегом VLAN50 наведено на рисунок 4.8.

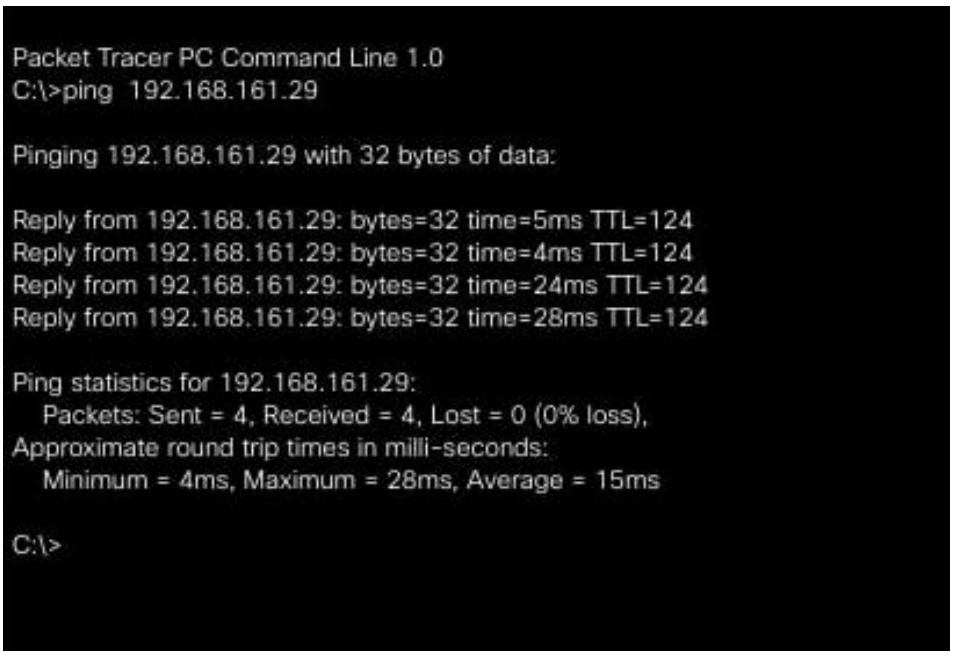

Рисунок 4.5 – Результат перевірки FTP серверу

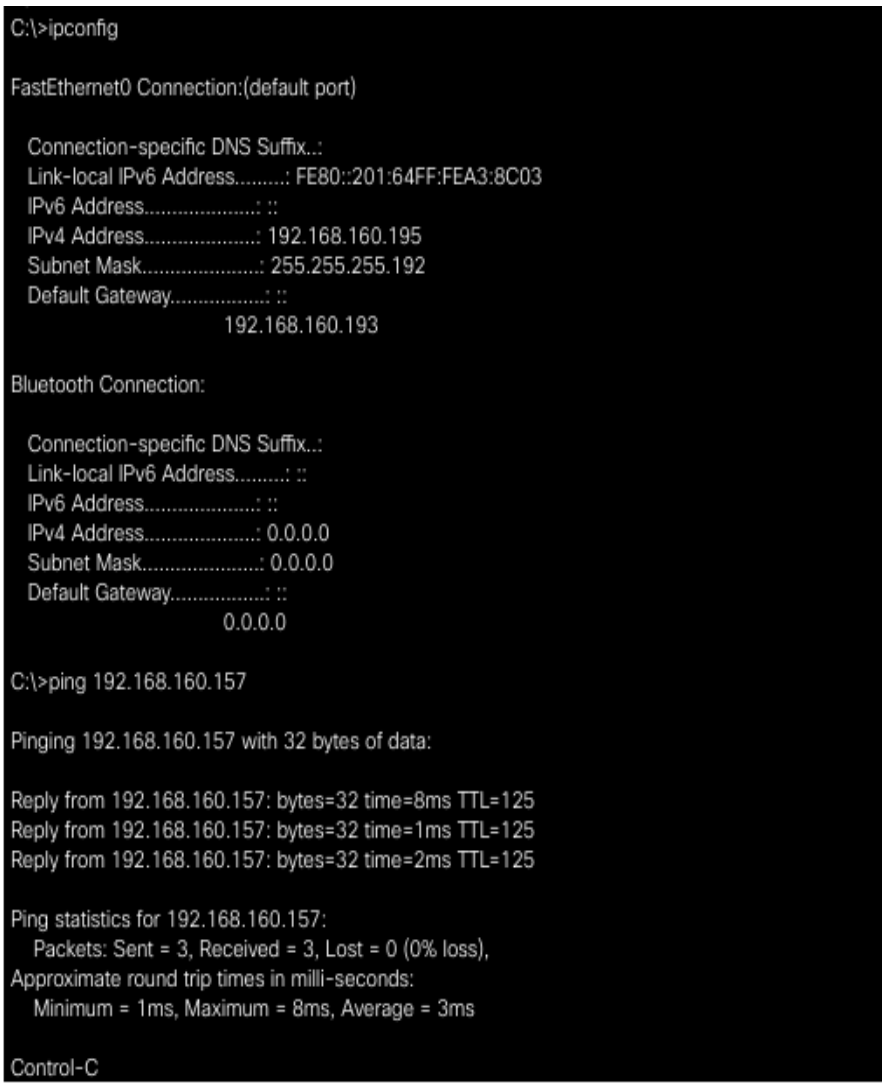

Рисунок 4.6 – Перевірка WEB сервера

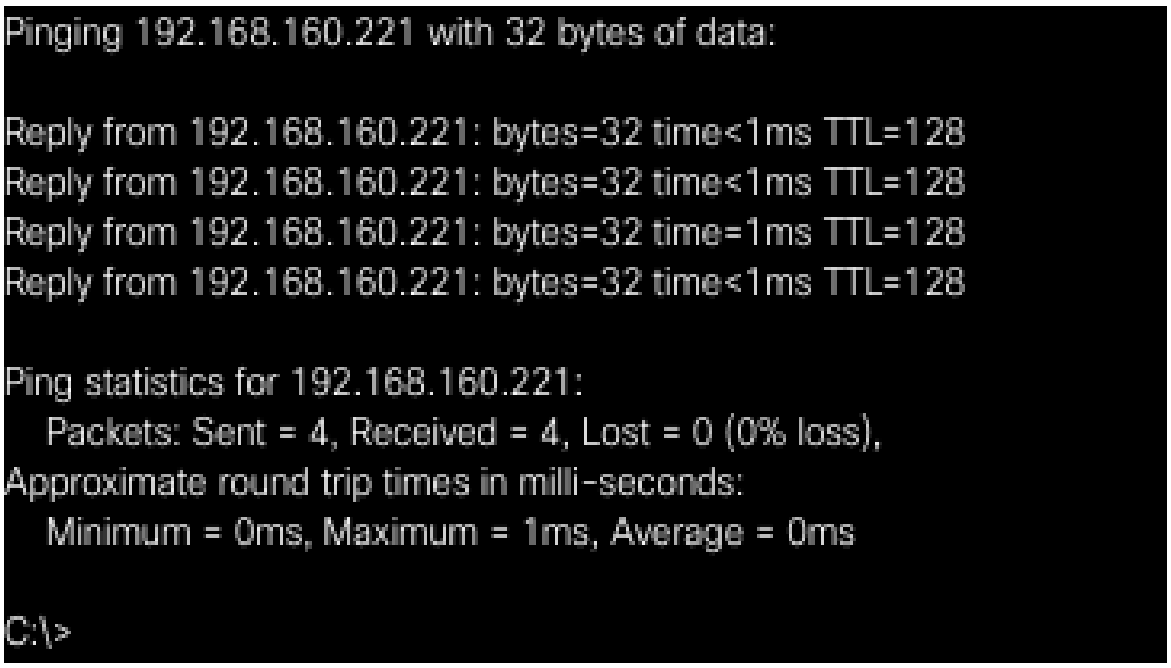

Рисунок 4.7 – Перевірка RADIUS сервера

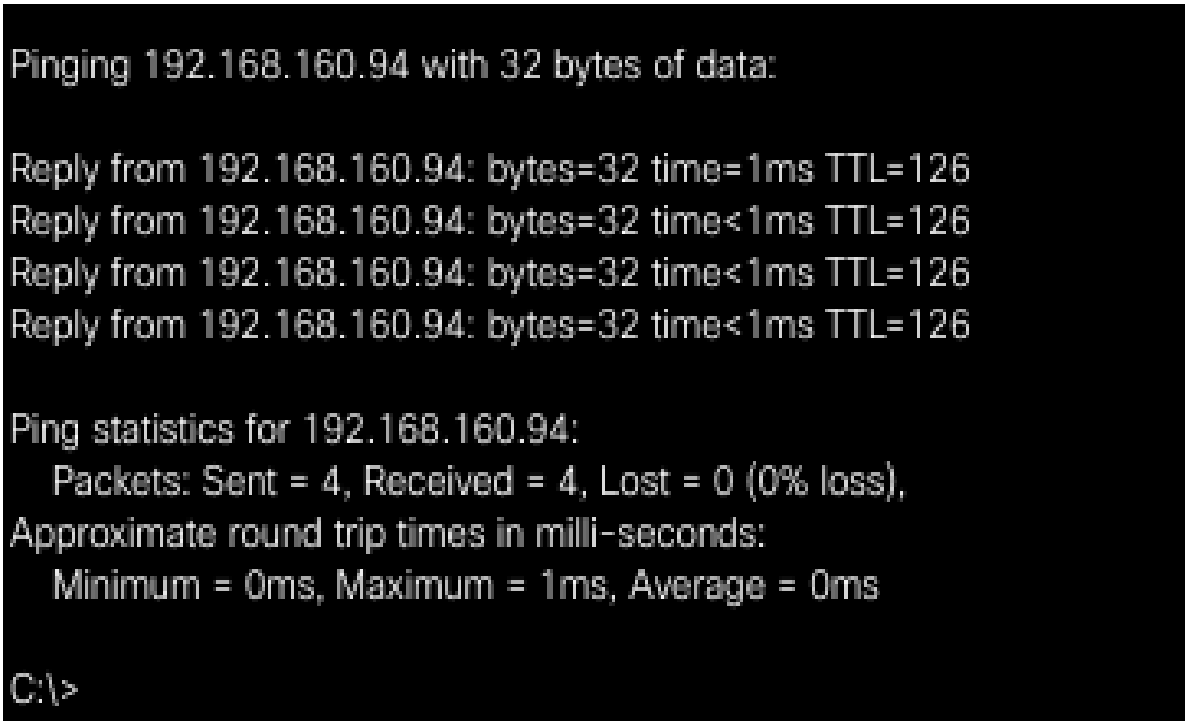

Рисунок 4.8 – Перевірка DNS сервера

Також для перевірки доступу, була застосована генерація трафіку в Packet Tracer. Згенерований трафік відображено в виді пакетів на рисунку 4.9.

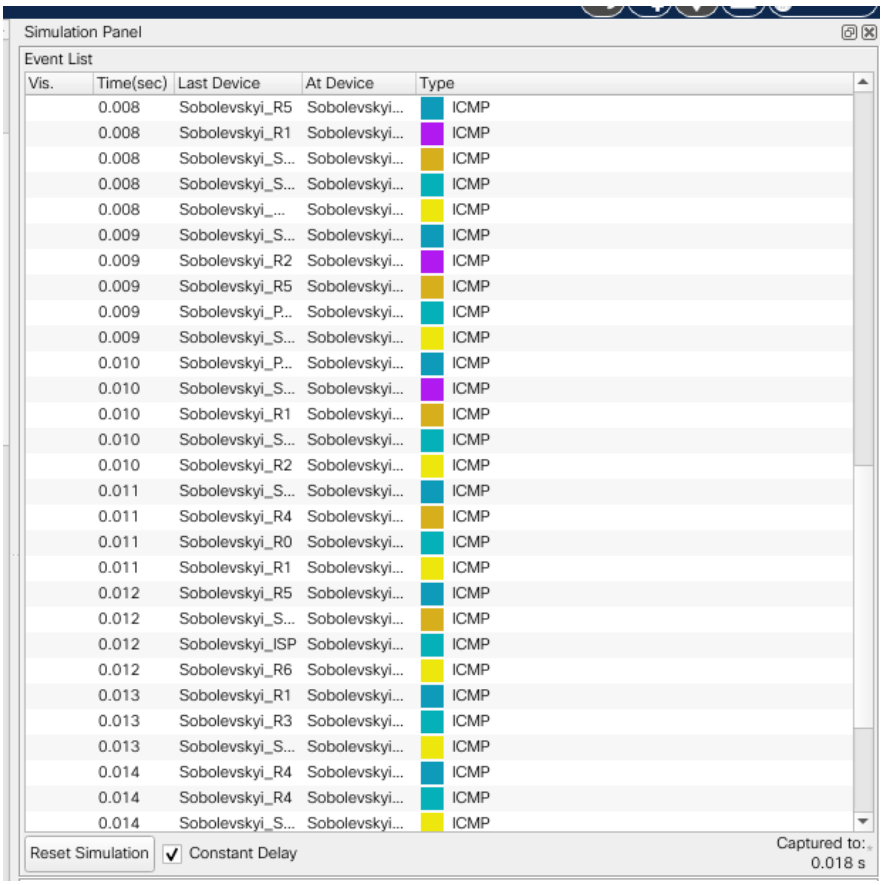

Рисунок 4.9 – Перевірка трафіку в Packet Tracer, перелік пакетів

Для перевірки роботи SSH на маршрутизаторах та коммутаторах, потрібно виконати на комп’ютері команду ssh -l <Login> <IP>. Результат перевірки – успішний (рисунок 4.10).

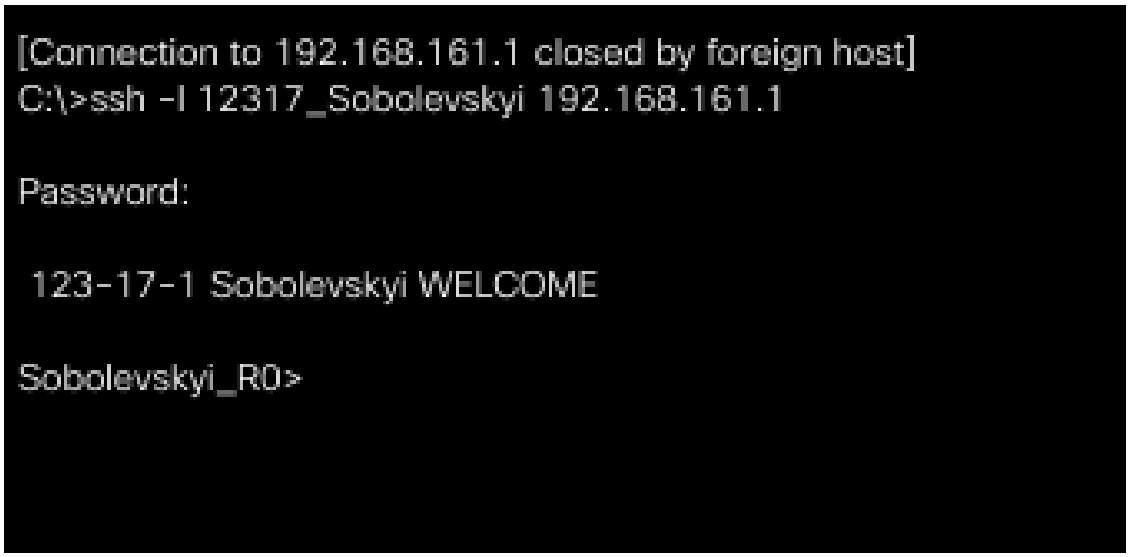

Рисунок 4.10 – Перевірка під'єднання до SSH серверу на Sobolevskiy_R0

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп’ютерній системі

В комп’ютерній системі будуть використовуватись наступні методи захисту інформації:

- VLAN;
- служба AAA з RADIUS сервером;
- безпека портів на комутаторах.

Ці методи являються необхідними, для забезпечення необхідного рівня безпеки в комп’ютерній системі.

5.2 Налаштування маршрутизаторів на підтримку служби AAA

Служба AAA потрібна для авторизації користувачів до мережевих пристроїв.

Перед налаштуванням AAA, потрібно налаштувати RADIUS сервер. Налаштування RADIUS сервера приведене на рисунку 5.1.

Налаштування AAA через RADIUS сервер на маршрутизаторі Sobolevskyi_R5:

Sobolevskyi_R5(config)#aaa
Sobolevskyi_R5(config)#aaa new-model
Sobolevskyi_R5(config)#radius-server host 192.168.160.221 key radius123
Sobolevskyi_R5(config)#aaa authentication login default group radius local
Sobolevskyi_R5(config)#line vty 0 5
Sobolevskyi_R5(config-line)#login authentication default

Перевірка роботи AAA приведена на рисунку 5.2. Для входу в систему тепер потрібно ввести логін та пароль з RADIUS сервера.

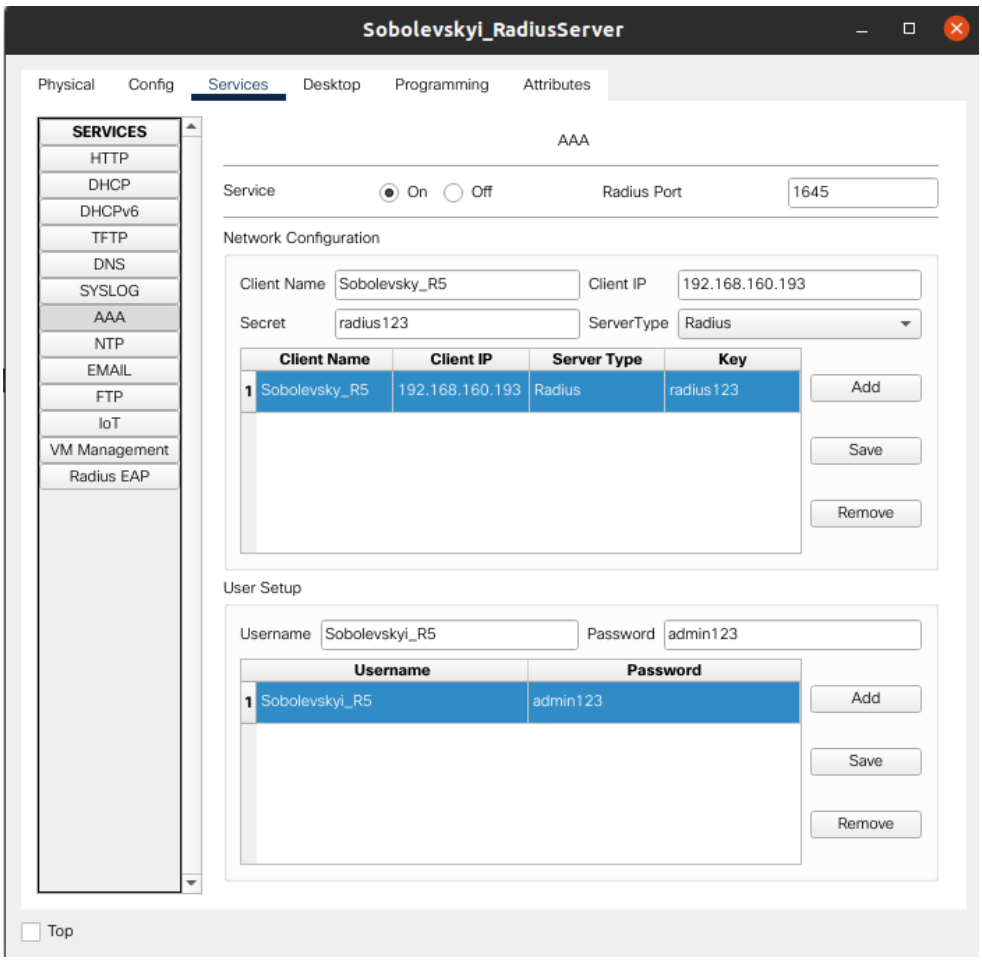

Рисунок 5.1 – Налаштування RADIUS сервера

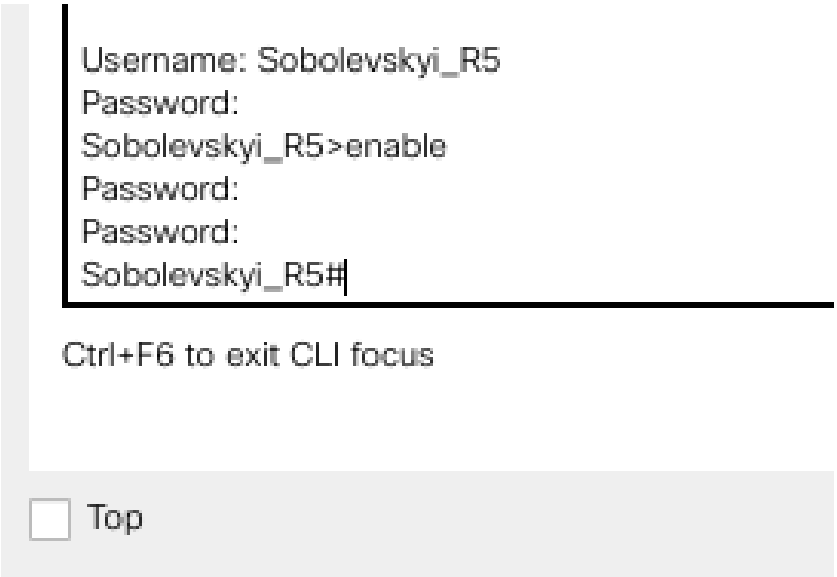

Рисунок 5.2 – Вхід на маршрутизатор через логін та пароль з RADIUS сервера

5.3 Налаштування мереж VLAN

Для налаштувань мереж VLAN було складено таблицю 5.1 та таблицю 5.2, в яких вказані необхідні теги VLAN, та призначення кожної мережі.

Таблиця 5.1 – Назви VLAN для комерційного відділу

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
30	Marketing	Для маркетингу
40	Advertising	Для реклами
50	Realtor	Для рієлторів
99	Management	Для управління пристроями
100	Native	Власна мережа

Налаштування VLAN тегів Sobolevskyi_SW3.1:

Sobolevskyi_SW3.1(config-vlan)#vlan 30

Sobolevskyi_SW3.1(config-vlan)#name Marketing

Sobolevskyi_SW3.1(config-vlan)#vlan 40

Sobolevskyi_SW3.1(config-vlan)#name Advertising

Sobolevskyi_SW3.1(config-vlan)#vlan 50

Sobolevskyi_SW3.1(config-vlan)#name Realtor

Sobolevskyi_SW3.1(config-vlan)#vlan 99

Sobolevskyi_SW3.1(config-vlan)#name Management

Sobolevskyi_SW3.1(config-vlan)#vlan 100

Sobolevskyi_SW3.1(config-vlan)#name Native

Налаштування транкових портів Sobolevskyi_SW3.1 FastEthernet 0/1-2:

Sobolevskyi_SW3.1(config)#interface range f0/1-2

Sobolevskyi_SW3.1(config-if-range)#switchport trunk native vlan 100

Sobolevskyi_SW3.1(config-if-range)#switchport mode trunk

Налаштування транкових портів Sobolevskyi_SW3.1 FastEthernet 0/5-10:

Sobolevskyi_SW3.1(config)#interface range f0/5-10

Sobolevskyi_SW3.1(config-if-range)#switchport mode access

Sobolevskyi_SW3.1(config-if-range)#switchport access vlan 50

Налаштування транкових портів Sobolevskyi_SW3.1 FastEthernet 0/12-14:

Sobolevskyi_SW3.1(config)#interface range f0/12-14

Sobolevskyi_SW3.1(config-if-range)#switchport mode access

Sobolevskyi_SW3.1(config-if-range)#switchport access vlan 30

Налаштування транкових портів Sobolevskyi_SW3.1 FastEthernet 0/15-24:

Sobolevskyi_SW3.1(config)#interface range f0/15-24

Sobolevskyi_SW3.1(config-if-range)#switchport mode access

Sobolevskyi_SW3.1(config-if-range)#switchport access vlan 40

Налаштування SVI інтерфейс:

Sobolevskyi_SW3.1(config)#interface vlan 99

Sobolevskyi_SW3.1(config-if)#ip address 192.168.160.2 255.255.255.128

Таблиця 5.2 – Налаштування VLAN для котеджного містечка “Золоті ключі”.

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
10	house	Дім
11	house1	Дім1
12	house2	Дім2
100	house3	Дім3

5.4 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

5.4.1 Налаштування параметрів безпеки комутаторів

Комутатори, до яких підключене серверне обладнання, потребують додаткового захисту. Для цього було прийнято рішення, налаштувати функцію безпеки портів, яка налаштована таким чином, щоб давати доступ тільки дозволеному MAC адресу. Якщо до порту буде підключено прилад, з іншим MAC адресом, то порт буде виключено.

Налаштування безпеки портів на комутаторі Sobolevskyi_SW1.1:

Sobolevskyi_SW1.1(config)#interface fastEthernet 0/23
Sobolevskyi_SW1.1(config-if)#switchport mode access
Sobolevskyi_SW1.1(config-if)#switchport port-security
Sobolevskyi_SW1.1(config-if)#switchport port-security maximum 2
Sobolevskyi_SW1.1(config-if)#switchport port-security mac-address 000C.CF83.57EE

5.4.2 Налаштування адресації ПК в мережах VLAN

На головному маршрутизаторі комерційного відділу потрібно налаштувати dot1Q інкапсуляцію, для того, щоб прилади бачили маршрутизатор. Налаштування dot1Q на маршрутизаторі Sobolevskyi_R1:

VLAN 99:

Sobolevskyi_R1(config)#interface fastEthernet 0/1.99
Sobolevskyi_R1(config-subif)#encapsulation dot1Q 99
Sobolevskyi_R1(config-subif)#ip address 192.168.160.1 255.255.255.224

VLAN 30:

Sobolevskyi_R1(config)#iinterface FastEthernet0/1.30
Sobolevskyi_R1(config-subif)#encapsulation dot1Q 30
Sobolevskyi_R1(config-subif)#ip address 192.168.160.97 255.255.255.224

VLAN 40:

Sobolevskyi_R1(config-if)#interface FastEthernet0/1.40

Sobolevskyi_R1(config-subif)#encapsulation dot1Q 40

Sobolevskyi_R1(config-subif)#ip address 192.168.160.33 255.255.255.224

VLAN 50:

Sobolevskyi_R1(config-if)#interface FastEthernet0/1.50

Sobolevskyi_R1(config-subif)#encapsulation dot1Q 50

Sobolevskyi_R1(config-subif)#ip address 192.168.160.65 255.255.255.224

Для забезпечення безпеки в котеджному містечку "Золоті Ключі" потрібно налаштувати ACL списки. Приклад налаштування:

Sobolevskyi_R6(config)#access-list 25 permit ip 192.168.161.0 255.255.255.224 192.168.160.157 0.0.0.255

Sobolevskyi_R6(config)#access-list 102 deny ip 192.168.161.0 255.255.255.224 any

Для автоматичної видачі IP адрес у мережах VLAN потрібно налаштувати DHCP сервер. Налаштування DHCP на маршрутизаторі Sobolevskyi_R1:

Виключення адресів маршрутизаторів та комутаторів з пулів DHCP:

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.97

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.1

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.33

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.65

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.2

Sobolevskyi_R1(config)#ip dhcp excluded-address 192.168.160.3

Налаштування DHCP VLAN 30:

Sobolevskyi_R1(config)#ip dhcp pool Vlan30

Sobolevskyi_R1(dhcp-config)#network 192.168.160.96 255.255.255.224

Sobolevskyi_R1(dhcp-config)#default-router 192.168.160.97

Sobolevskyi_R1(dhcp-config)#dns-server 192.168.160.94

Налаштування DHCP VLAN 40:

Sobolevskyi_R1(config)#ip dhcp pool Vlan40

Sobolevskyi_R1(dhcp-config)#default-router 192.168.160.33

Sobolevskyi_R1(dhcp-config)#network 192.168.160.32 255.255.255.224

Sobolevskyi_R1(dhcp-config)#dns-server 192.168.160.94

Налаштування DHCP VLAN 50:

Sobolevskyi_R1(config)#ip dhcp pool Vlan50

Sobolevskyi_R1(dhcp-config)#network 192.168.160.64 255.255.255.224

Sobolevskyi_R1(dhcp-config)#default-router 192.168.160.65

Sobolevskyi_R1(dhcp-config)#dns-server 192.168.160.94

Для того, щоб отримати адресу по DHCP потрібно зайти на комп'ютер, в налаштування IP, та підтвердити отримання адреси по DHCP. Налаштування DHCP приведено на рисунку 5.3.

Рисунок 5.3 – Налаштування на DHCP

6 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ

6.1 Призначення і область застосування програми

Призначенням програми являється – перегляд відеокамер встановлених на приватних ділянках з метою підвищення рівня безпеки в житловому містечку "Золоті ключі". Камери доступні як в режимі онлайн, так і є можливість подивитися запис.

6.2 Обґрунтування технічних характеристик програми

6.2.1 Обґрунтування вибору платформи для програми

Платформою застосунка для перегляду відео з камер може являтись як нативне середовище, так і платформа веб.

Нативне середовище прив'язане до використання на одній платформі, під яку було написано застосунок. Тобто якщо писати застосунок під платформу Windows, то він не буде працювати на операційній системі Linux, або на мобільних платформах. Є фреймворки, такі, як QT, які дозволяють писати кросплатформні нативні застосунки, але якщо розробка ведеться маленькою командою з обмеженим фінансуванням, то знайти всі виниклі баги на підтримуваних операційних системах буде важко, так як це потребує команди QA інженерів.

Особливість веб застосунків – платформою являється не операційна система, а браузер. В цьому можуть бути як плюси, так і мінуси. Застосунок, який написано під браузер може виконувати, лише дозволені браузерним середовищем, системні виклики. Це обмежує можливий функціонал, порівняно з нативним застосунком, але відкриває ряд можливостей, такі як кросплатформність із коробки, тобто, якщо застосунок було написано під платформу браузер, то на будь якому пристрої, на якому є браузер, цей застосунок буде працювати.

Проаналізувавши цю інформацію, було обрано веб застосунок з платформою браузер. Веб застосунок буде найкращим вибором, так як, в браузері є всі необхідні системні виклики для виконання вимог застосунком, а нативний застосунок буде обмежувати кількість підтримуваних пристроїв.

6.2.2 Обґрунтування вибору технології ПО

Для реалізації додатку було обрано мову програмування JavaScript, як для серверної, так і для клієнтської частини. Мова програмування JavaScript може запускатися як в браузері користувач, що ідеально для веб додатку, так і на сервері, який обслуговує клієнта.

Для реалізації клієнтської частини, прийнято рішення використовувати бібліотеку React. React являється сучасною бібліотекою для розробки реактивних веб додатків, ця бібліотека вирішує проблеми часткового оновлення вмісту веб сторінки, що дозволяє ефективно писати багатофункціональні веб додатки [21].

Для реалізації серверної частини буде використовуватись NodeJS, який являється платформою для написання високонавантажених мережевих додатків, які пишуться мовою JavaScript. Головна перевага використовування NodeJS на серверній частині – ефективна обробка запитів користувача, та потоку даних. Це реалізується завдяки асинхронним запитам, що економить ресурси сервера [22].

Для реалізації порталу адміністратора було обрано HCMS Strapi. Strapi являється системою управління вмістом, яка базується на API запитах, та генерує веб портал адміністратора в залежності від заданої структури БД.

Обробка даних відеопотоку від камер буде реалізовано завдяки програмі з відкритим кодом ffmpeg. Ця програма може збирати відеопотік по протоколу RTSP та конвертувати його в формат mpeg, який можна декодувати на веб сторінці користувача, завдяки декодеру JsMpeg, та відобразити у елементі сторінки canvas.

6.2.3 Вибір та обґрунтування архітектури додатку

Для архітектури веб додатку було обрано мікросервісну архітектуру, ця архітектура базується на принципі – програма повинна мати невеликий функціонал, але заложений виконувати якомога ефективніше. Цей принцип будування ПО виник з потрібності удосконалення командної роботи розробників, для оптимізації виконання поставлених завдань. ПО ділиться на мікросервіси, які виконують обмежену функціональність, таким чином розробка кожного мікросервісу, при належному плануванні, може віддаватися, як окреме завдання, для розробника чи команди розробників. Так, як за кожен мікросервіс відповідає обмежена кількість людей, цей процес легше контролювати, а розробка ведеться ефективніше, завдяки розпаралелювання завдань. Також плюсом являється – ізоляція коду кожного мікросервісу, це означає, що код взаємодіє між мікросервісами в рамках виділених точок API, що прискорює тестування та знаходження багів.

6.2.4 Вибір та обґрунтування архітектури компонентів

В додатку виділяються такі мікросервіси (рисунок 6.1):

1) база Даних – сервіс, який являється головним сховищем даних по користувачах та камерах;
2) панель адміністратора – цей сервіс безпосередньо звертається до БД, модифікує дані. Також, він генерує панель адміністратора в залежності від структури БД. До цього сервісу звертаються інші сервіси по API для отримання інформації;
3) обробник відеопотоку з камер – цей сервіс повинен брати з сервісу панелі адміністратора інформацію о камерах, а точніше IP адресу, порт та протокол підключення до камери, під'єднуватися до неї, збирати відеопоток, записувати та видавати його клієнту за протоколом WebSocket;

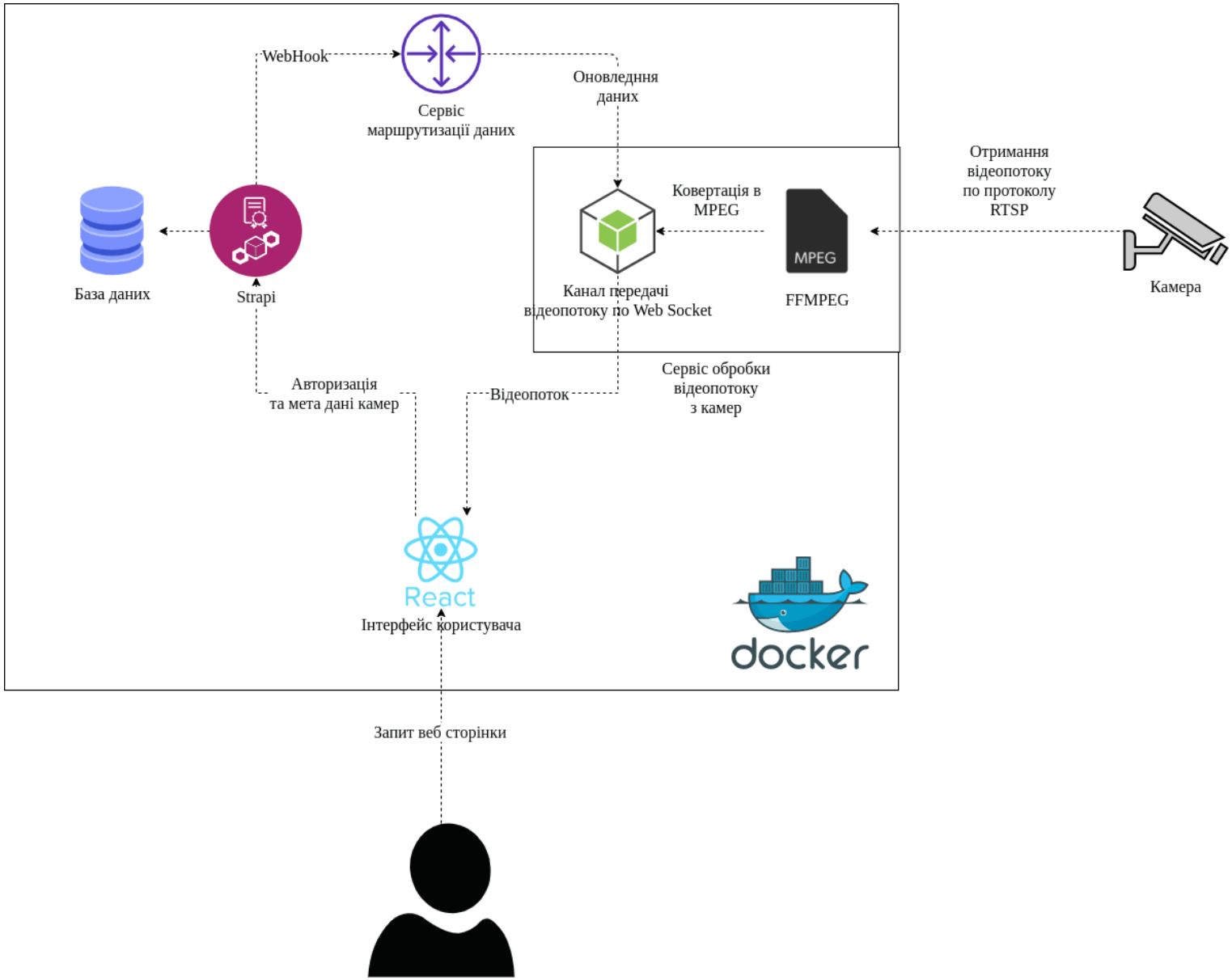

Рисунок 6.1 – Візуалізація архітектури додатку

4) інтерфейс користувача – цей сервіс потрібен для показу користувачеві, призначених адміністратором камер. Користувач повинен авторизуватись у системі, після чого приєднатися до відеопотоку, який видає обробник камер;
5) сервіс маршрутизації даних – цей сервіс відповідає за реагування на зміну даних в адмін панелі. Являється проміжною ланкою, між сервісом адмін панелі та іншими мікросервісами.

6.2.5 Вибір та обґрунтування структури БД

Для структури БД, що відображена на рисунку 6.2, потрібні таблиці:

1) Користувач – ця таблиця містить в собі інформацію про користувача та дані для входу.
2) Роль – користувачі діляться на адмінів та авторизованих користувачів, адміни мають доступ в адмін панель, авторизовані користувачі, мають доступ для перегляду камер.
3) Камера – ця таблиця містить в собі назву, посилання на відеопотік, та порт, який відкривається для трансляції користувачам на веб сторінку.
4) Камера-Користувач – ця таблиця призначена для того, щоб з’єднати сутності користувачів та камер у зв’язку багато до багатьох.

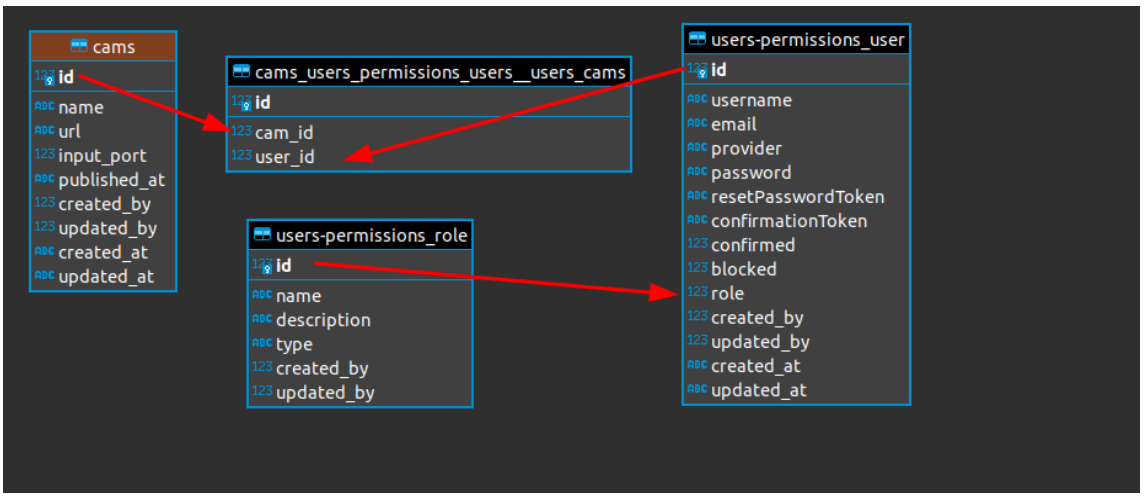

Рисунок 6.2 – Візуалізація БД

Так як архітектура бази даних невелика, та немає великої кількості складних зв'язків, було обрано базу даних SQLite, яка виділяється своєю легкістю та переносимістю.

6.3 Підготовка та налаштування пристроїв

Для налаштування Raspberry Pi потрібно скачати з офіційного сайту образ ОС Raspbian https://www.raspberrypi.org/software/operating-systems/. Ця Unix-подібна ОС базується на ядрі Linux та являється форком дистрибутива Debian. Рекомендується встановити Lite версію ОС, в неї немає робочого стола, та програм, якім необхідно GUI.

6.3.1 Встановлення ОС

Необхідно приготувати карту microSD, її потрібно відформатувати в файлову систему FAT32. Після чого потрібно скачати утиліту balenaEtcher (зображена на рисунку 6.3) з офіційного сайту https://www.balena.io/etcher/.

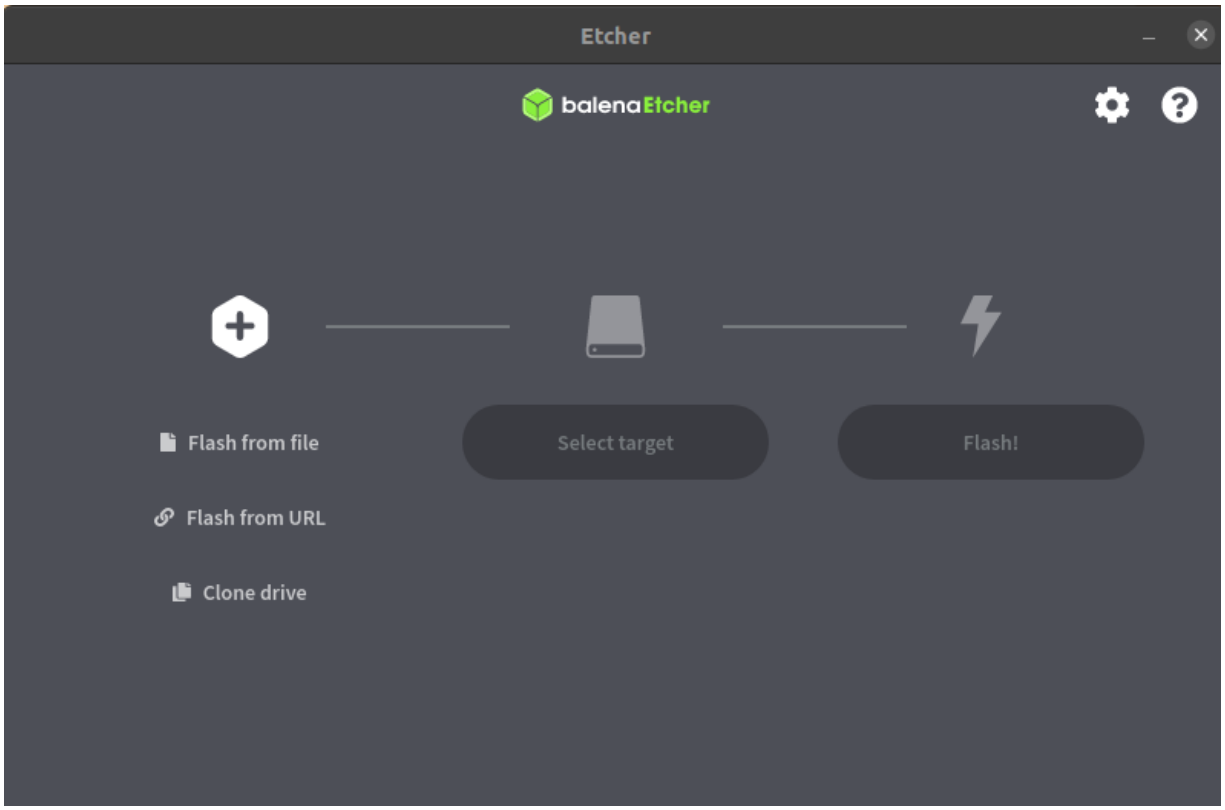

Рисунок 6.3 – Інтерфейс програми balenaEtcher

В програмі balenaEtcher потрібно:

1) Вибрати файл для прошивки.
2) Вибрати microSD карту, як ціль прошивки.
3) Нажати кнопку “Flash!”.

6.3.2 Налаштування WiFi на Raspberry Pi

Якщо користувач вважає необхідним, щоб Raspberry Pi приєднався до мережі через WiFi, потрібно, після того як завантажаться файли до microSD картки, зайти на сектор “boot” та створити файл “wpa_supplicant.conf” у корень сектора [20]. У файлі потрібно написати SSID та пароль у форматі поданому на рисунку 6.4.

```
network={
    ssid="testing"
    psk="testingPassword"
}
```

Рисунок 6.4 – формат підключення WiFi у файлі wpa_supplicant.conf

6.3.3 Налаштування SSH на Raspberry Pi

Для подальшого доступу до терміналу, найбільш зручним та захищеним способом буде використовувати протокол SSH. Для налаштування SSH серверу на Raspberry Pi потрібно зайти на сектор “boot” та створити файл “ssh” у корень сектора [20].

6.3.4 Підключення живлення до Raspberry Pi

Після процессу установки, потрібно вставити картку microSD у Raspberry Pi. Для запуску операційної системи потрібно вставити живлення в Raspberry Pi, потрібно дати 5V, 2A по кабелю microUSB (зображено на рисунку 6.5).

Рисунок 6.5 – підключення живлення Raspberry Pi по порту microUSB

6.3.5 Налаштування мережі для Raspberry Pi

Після підключення, Raspberry Pi повинен завантажити ОС і, якщо він підключенний до мережі з активним DHCP сервером, повинен получити IP адресу, яку можна дізнатися на маршрутизаторі, чи приєднати монітор і клавіатуру до Raspberry Pi та дізнатися IP адреси завдяки програмі “ifconfig”[20]. Приклад приклад виведення команди “ifconfig” зображено на рисунку 6.6.

```
pi@raspberrypi:~ $ sudo ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:27:eb:73:1f:e7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3972  bytes 198600 (193.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3972  bytes 198600 (193.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.128.112  netmask 255.255.255.0  broadcast 192.168.128.255
        inet6 fe80::76b3:267:3d34:ada  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:26:4a:b2  txqueuelen 1000  (Ethernet)
        RX packets 947  bytes 96644 (94.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 257  bytes 39494 (38.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberrypi:~ $
```

Рисунок 6.6 – приклад виведення команди “ifconfig”.

IP адресу обов’язково потрібно зробити статично, задати її можна на маршрутизаторі (рисунок 6.7) або на самому Raspberry Pi в файлі “/etc/dhcpcd.conf” (рисунок 6.8).

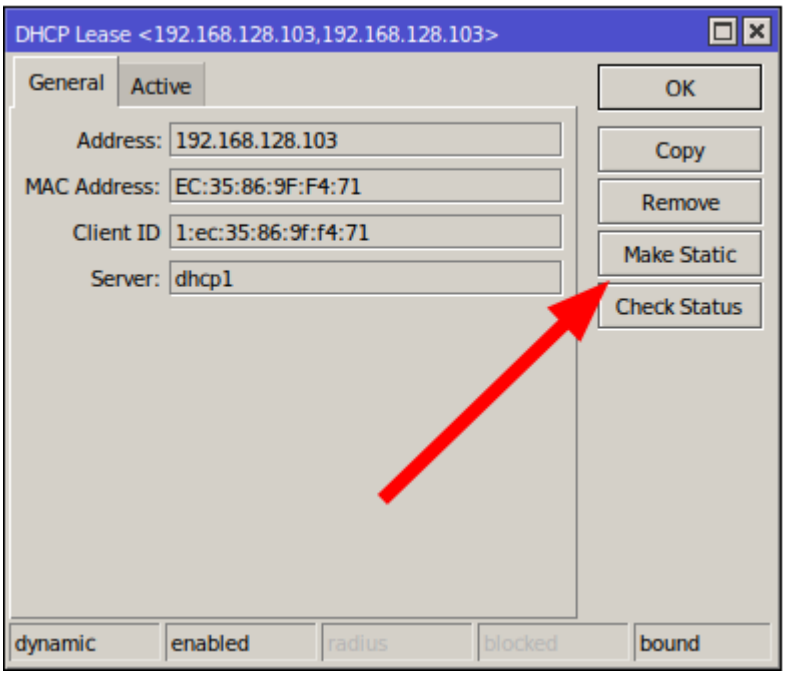

Рисунок 6.7 – Приклад налаштування статичного адресу в DHCP на маршрутизаторі MikroTik

```
# Example static IP configuration:
interface eth0
static ip_address=192.168.128.112/24
static routers=192.168.128.1

# It is possible to fall back to a static I
# define static profile
#profile static_eth0
#static ip_address=192.168.1.23/24
#static routers=192.168.1.1
#static domain_name_servers=192.168.1.1

# fallback to static profile on eth0
#interface eth0
#fallback static_eth0
```

Рисунок 6.8 – Приклад налаштування статичного адресу на Raspberry Pi в файлі /etc/dhcpcd.conf

6.3.6 Підключення по протоколу SSH до Raspberry Pi

На комп’ютері користувача повинен бути встановлений SSH клієнт. Для користувачів ОС Windows це може бути Putty, або Openssh в Powershell. Linux та MacOS користувачі, як правило, мають вже встановлений Openssh, який можна використовувати в терміналі [20].

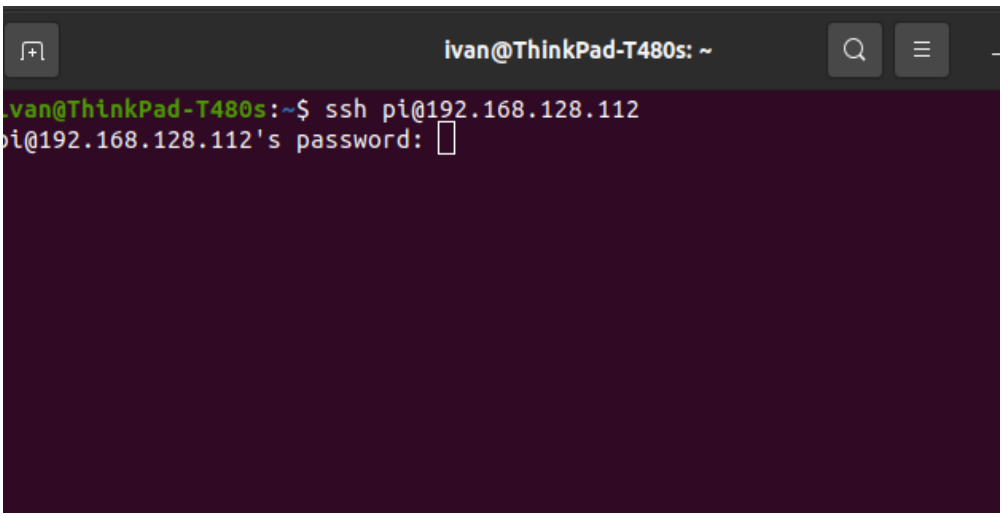

Рисунок 6.9 – Приклад підключення до Raspberry Pi з терміналу Linux.

Для підключення потрібно ввести логін та пароль, при першому запуску логін буде – pi, пароль – raspberry (рисунок 6.10).

```
ivan@ThinkPad-T480s:~$ ssh pi@192.168.128.112
pi@192.168.128.112's password:
Linux raspberrypi 5.4.51-v7+ #1333 SMP Mon Aug 10 16:45:19 BST 2020 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 14:48:36 2021 from 192.168.128.113

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
 a new password.
```

Рисунок 6.10 – Успішне підключення до SSH серверу.

6.3.7 Зміна стандартного паролю на Raspberry Pi

Щоб змінити стандартний пароль на Raspberry Pi, потрібно ввести команду “sudo raspi-config” (рисунок 6.11, рисунок 6.12).

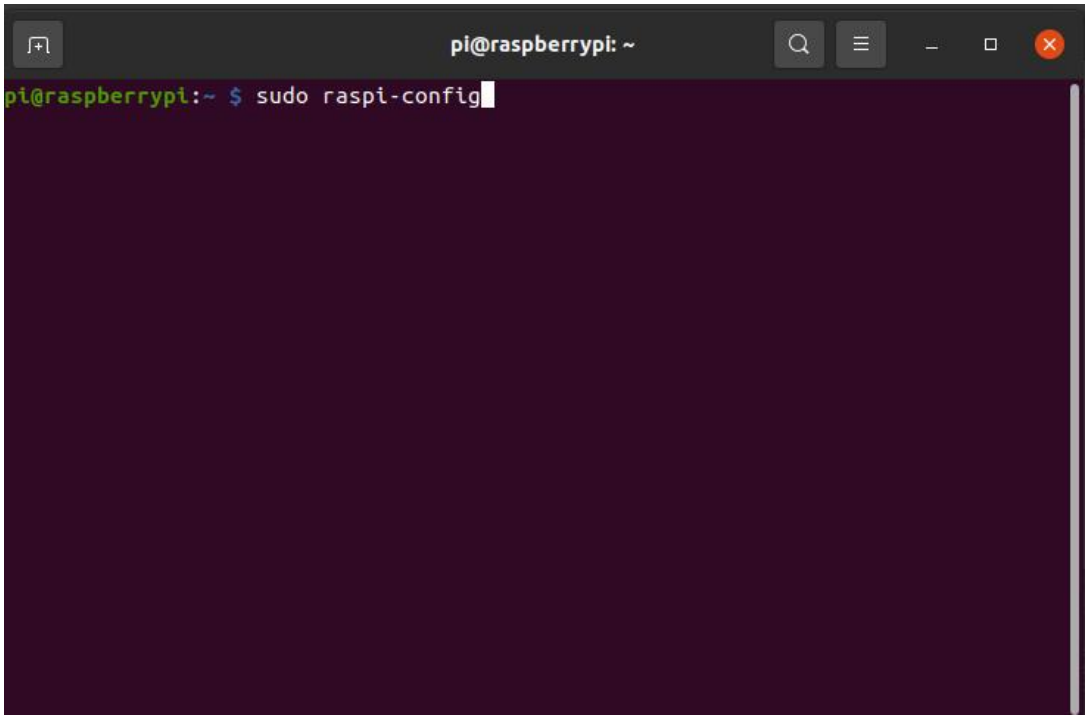

Рисунок 6.11 – Команда raspi-config

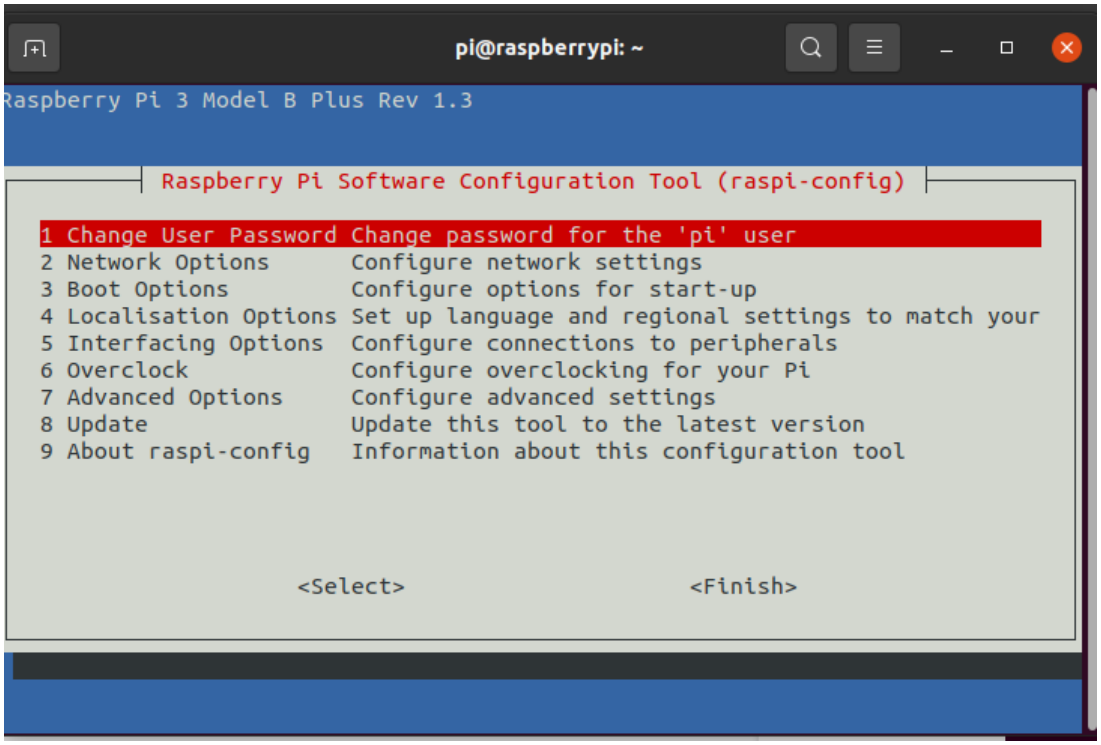

Рисунок 6.12 – Вивід команди raspi-config.

Після того, як була виконана команда “sudo raspi-config”, потрібно вибрати пункт “Change User Password”, нажати “Enter”, та підтвердити вибір. Програма запитає ввести новий пароль для користувача (рисунок 6.13). Після підтвердження нового паролю, потрібно натиснути – “Finish” [20].

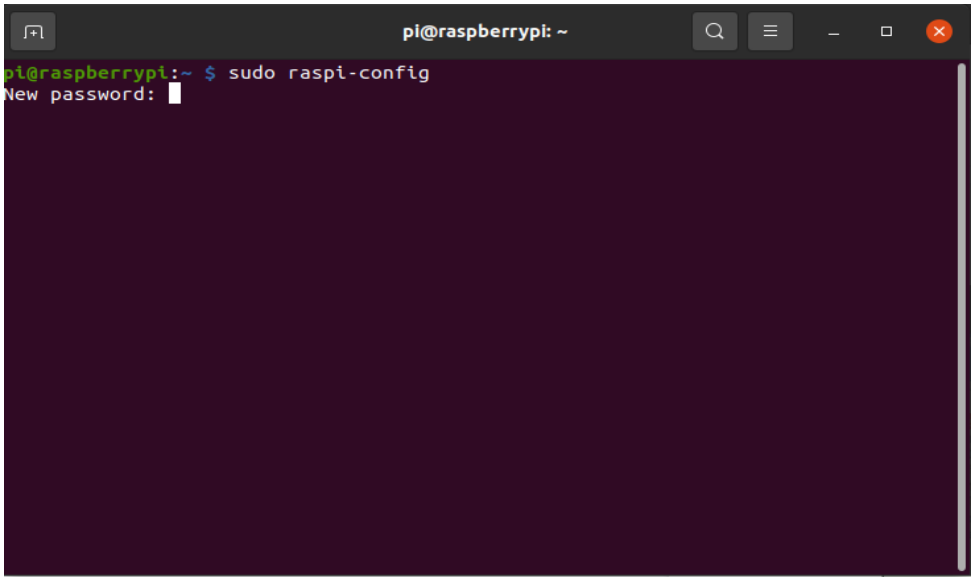

Рисунок 6.13 – Новий пароль.

6.3.8 Налаштування камери PiCam на Raspberry Pi

Модуль камери PiCam (рисунок 6.14), підключається до Raspberry Pi за допомогою гнучкого кабелю-шлейфа (рисунок 6.15). Перед підключенням потрібно вимкнути живлення Raspberry Pi.

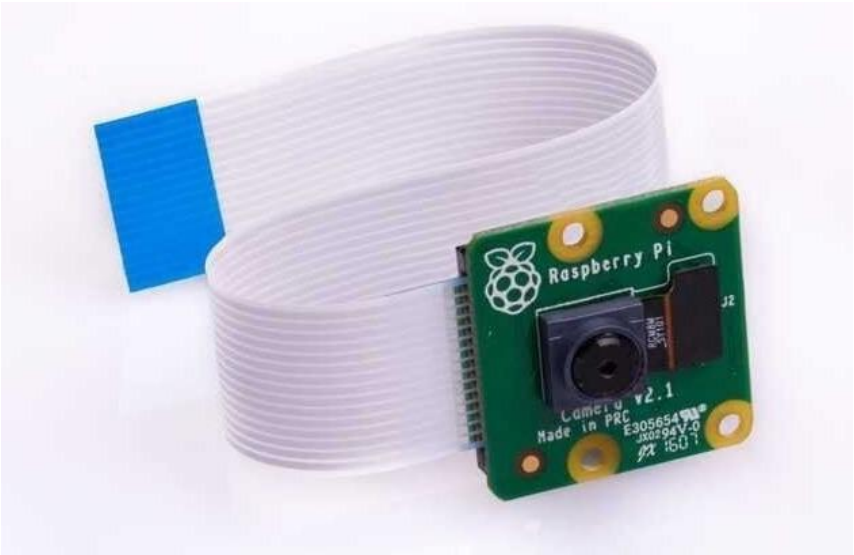

Рисунок 6.14 – Камера Pi Cam.

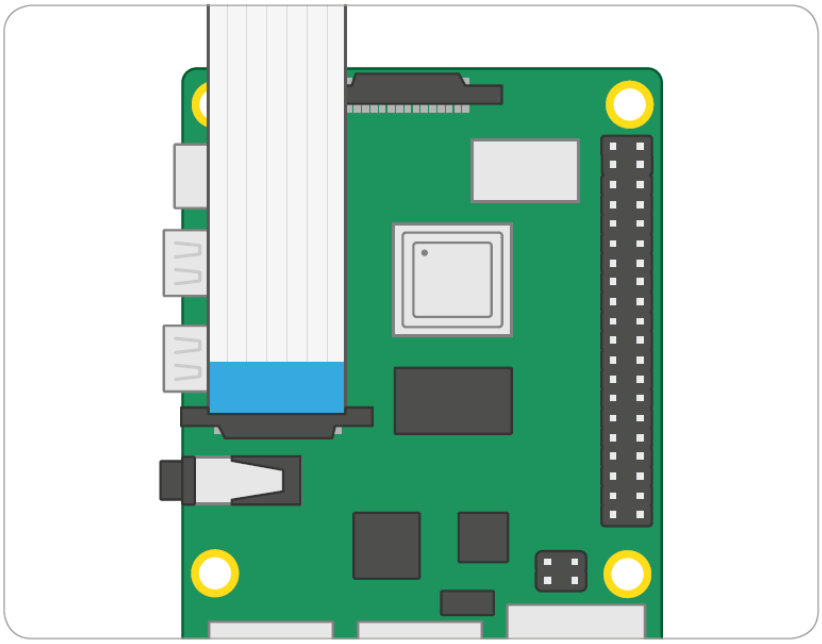

Рисунок 6.15 – Підключення камери Pi Cam до Raspberry Pi

Після підключення камери, потрібно її активувати. Для цього треба зайти на Raspberry Pi по протоколу SSH та ввести команду “sudo raspi-config”, вибрати пункт “Interfacing Options” (рисунок 6.16).

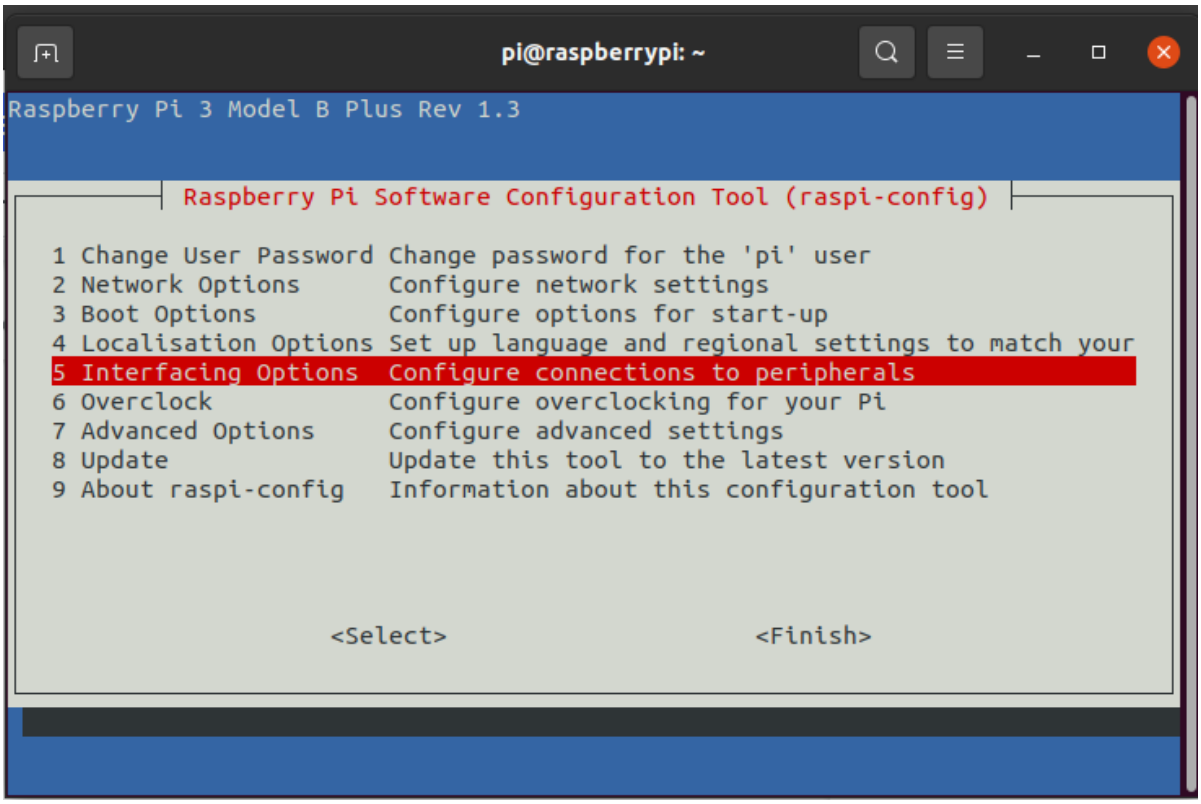

Рисунок 6.16 – “sudo raspi-config” пункт “Interfacing Options”.

Далі – потрібно обрати пункт “Camera” (рисунок 6.17) та підтвердити вмикання камери (рисунок 6.18) [20].

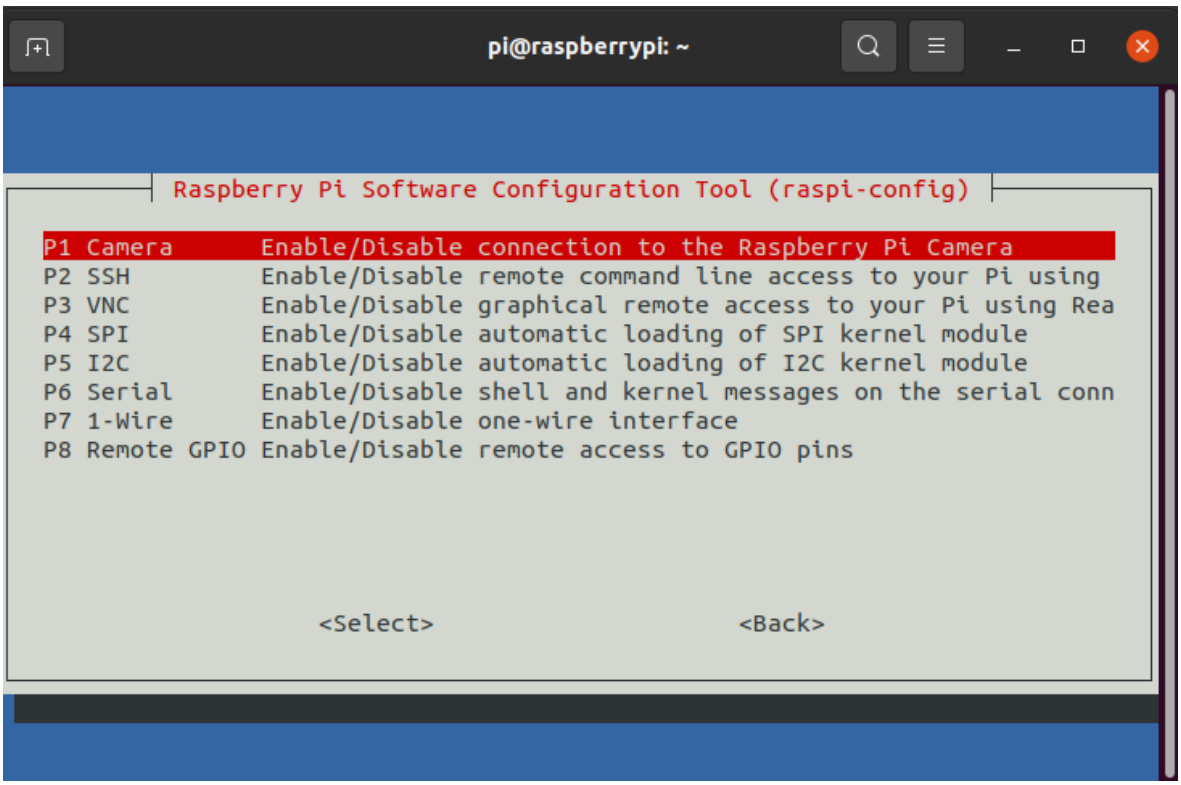

Рисунок 6.17 – “sudo raspi-config” пункт “Interfacing Options”

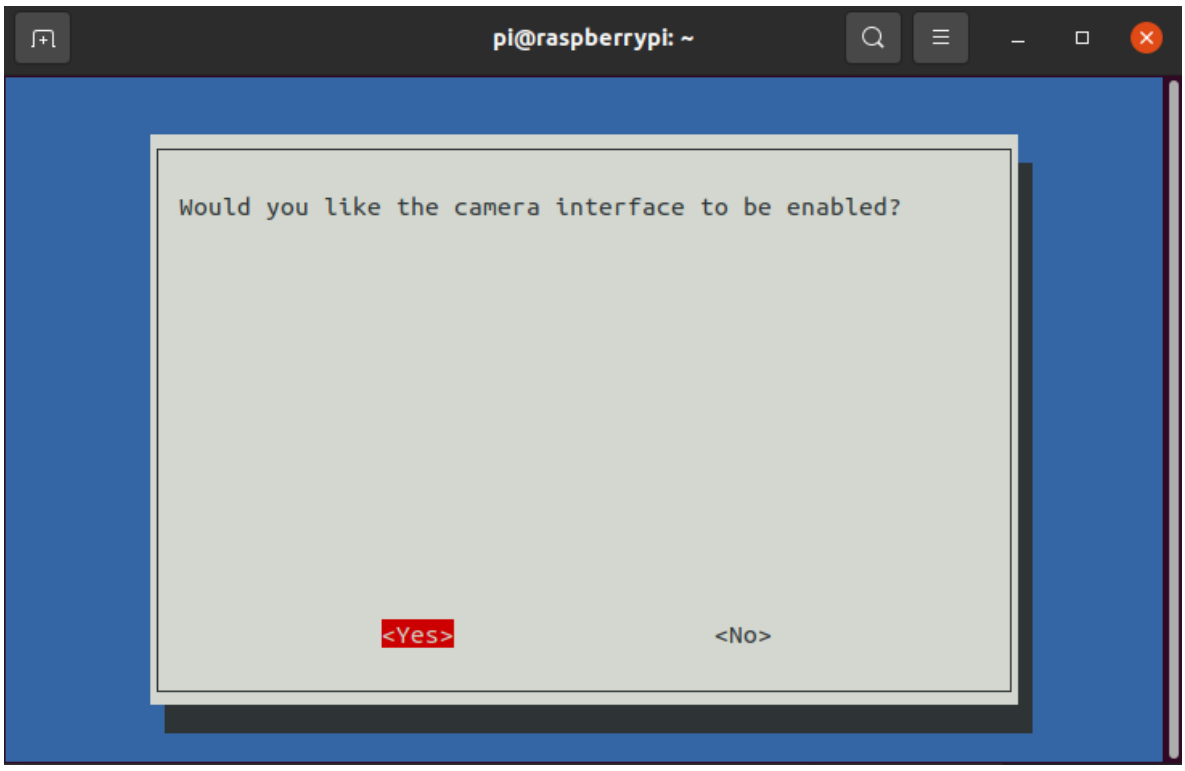

Рисунок 6.18 – “sudo raspi-config” пункт “Interfacing Options”

6.3.9 Встановлення програми cvlc

Для транслювання, по протоколу RTSP, відеопотока з камери, потрібно встановити програму “cvlc”, яка йде в комплекті з плеєром “VLC”. Для встановлення програми “cvlc” потрібно ввести команду “sudo apt update”, а потім команду “sudo apt install vlc”, як зображено на рисунку 6.19.

```
pi@raspberrypi:~ $ sudo apt update
Hit:1 http://raspbian.raspberrypi.org/raspbian buster InRelease
Hit:2 http://archive.raspberrypi.org/debian buster InRelease
Hit:3 https://deb.nodesource.com/node_8.x buster InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
124 packages can be upgraded. Run 'apt list --upgradable' to see them.
pi@raspberrypi:~ $ sudo apt install vlc
Reading package lists... Done
Building dependency tree
Reading state information... Done
vlc is already the newest version (3.0.12-0+deb10u1+rpt2).
0 upgraded, 0 newly installed, 0 to remove and 124 not upgraded.
pi@raspberrypi:~ $
```

Рисунок 6.19 – Команди “sudo apt update” та “sudo apt install vlc”

6.3.10 Перевірка роботи камери

Для запуску трансляції по протоколу RTSP на Raspberry Pi потрібно ввести команду (рисунок 6.20) – raspivid -o - -t 9999999 -w 1280 -h 720 --hflip | cvlc -v stream:///dev/stdin --sout '#rtp{sdp=rtsp://:8080/}' :demux=h264.

```
pi@raspberrypi:~ $ raspivid -o - -t 9999999 -w 1280 -h 720 --hflip  | cvlc -v stream:///dev/stdin --sout
'#rtp{sdp=rtsp://:8080/}' :demux=h264
VLC media player 3.0.12 Vetinari (revision 1.0.6-1618-g917488b78)
[00bc6690] vlcpulse audio output error: PulseAudio server connection failure: Connection refused
[00bac6d0] main interface error: no suitable interface module
[00b4b6d0] main libvlc error: interface "globalhotkeys,none" initialization failed
[00bac6d0] dummy interface: using the dummy interface module...
[729034a8] main stream error: unknown query 0x30e in demux_vaControlHelper
```

Рисунок 6.20 – запуск передачі відеопотоку з камери по протоколу RTSP.

Для перевірки роботи камери, на комп'ютері користувача потрібно встановити VLC плеєр. У VLC плеєрі потрібно зайти в (послідовність зображена на рисунок 6.21):

1) Media, Open Network Stream
2) Network
3) Вписати URL в форматі “rtsp://ip-raspberry-pi:8080/” та натиснути “Play”, після чого появиться зображення (рисунок 6.22).

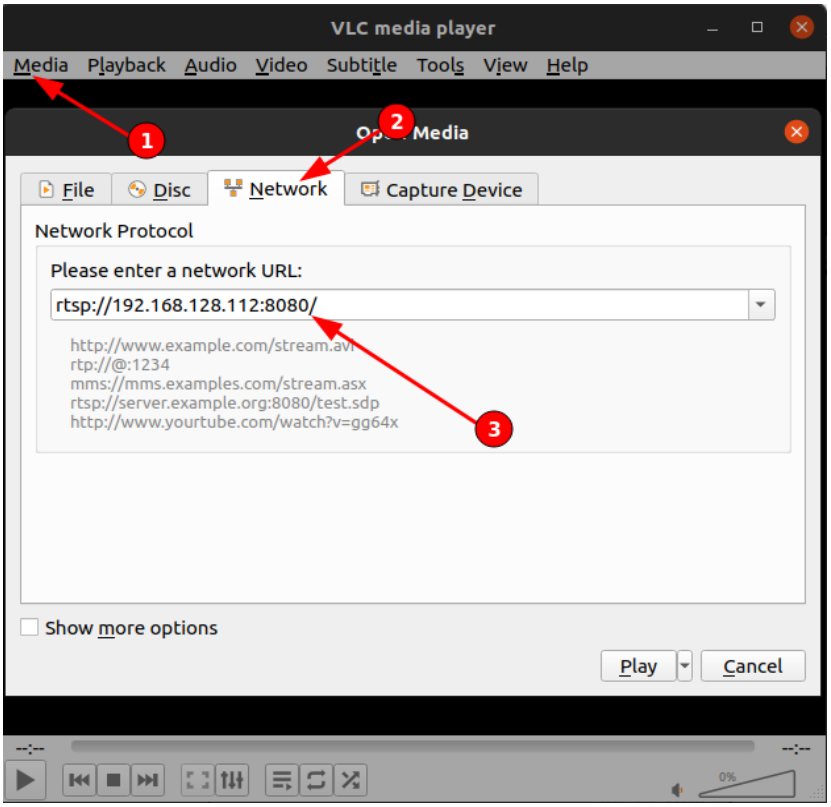

Рисунок 6.21 – Запуск передачі відеопотоку з камери по протоколу RTSP.

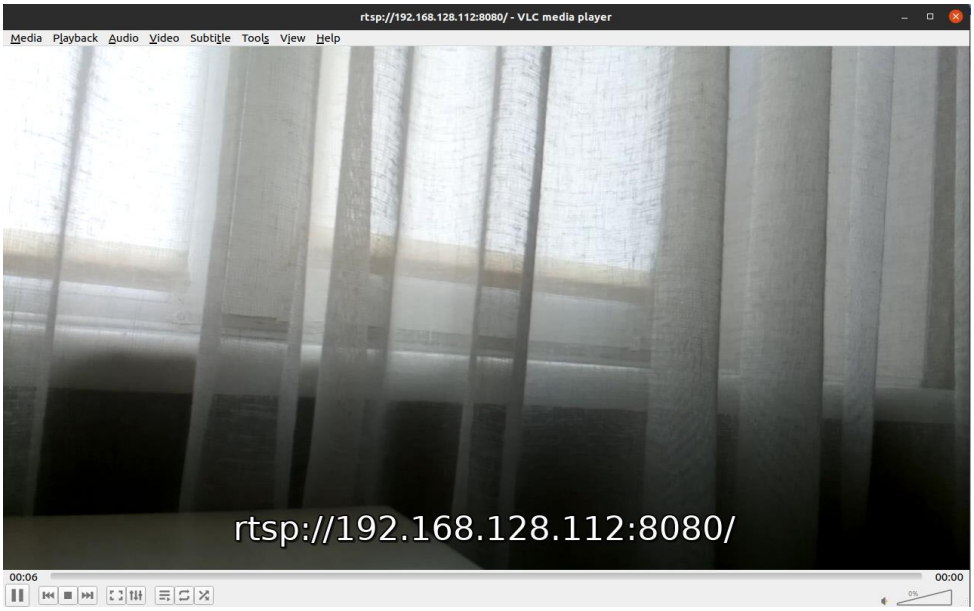

Рисунок 6.22 – Зображення з камери Raspberry Pi

6.3.11 Автозапуск камери, для роботи у live режимі

Для того, щоб камера могла передавати зображення незалежно від користувача, потрібно налаштувати автоматичний запуск передачі відеопотоку. Для цього потрібно:

1) В папці “/home/pi” створити файл “cam.sh” в який вставити команду:

raspivid -o - -t 9999999 -w 1280 -h 720 --hflip | cvlc -v stream:///dev/stdin --sout '#rtp{sdp=rtsp://:8080/}' :demux=h264 --sout-rtsp-user username --sout-rtsp-pwd password.

Замість username та password потрібно вставити логін та пароль, які будуть захищати відеопоток від неавторизованих користувачів.

2) Потрібно створити створити сервіс systemctl, який буде відповідати за автоматичний старт програми. Для цього потрібно створити файл “/etc/systemd/system/cam.service” з кодом (приклад на рисунку 6.23):

```
[Unit]
Description=CameraService
After=syslog.target

[Service]
WorkingDirectory=/home/pi
User=pi
ExecStart=/bin/bash /home/pi/start-cam.sh
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -L -s QUIT $MAINPID
PrivateTmp=true
Restart=on-failure
RestartSec=5s

[Install]
WantedBy=multi-user.target
```

```
GNU nano 3.2                                    /etc/systemd/system/cam.service

[Unit]
Description=CameraService
After=syslog.target

[Service]
WorkingDirectory=/home/pi
User=pi
ExecStart=/bin/bash /home/pi/start-cam.sh
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -L -s QUIT $MAINPID
PrivateTmp=true
Restart=on-failure
RestartSec=5s

[Install]
WantedBy=multi-user.target
```

Рисунок 6.23 – Код сервісу systemctl

3) Активувати за запустити сервіс завдяки команді “sudo systemctl enable cam && sudo systemctl start cam”.

6.4 Опис розробленої програми

6.4.1 Загальні відомості

Застосунок ділиться на клієнтську та серверну частину. Обидві частини було написано мовою JavaScript, але для цього було використано різні бібліотеки та фреймворки. Клієнтська частина написана завдяки бібліотеці React, а серверна частина, завдяки NodeJS. Ціль застосунку – показувати зображення з камер авторизованим користувачам.

6.4.2 Функціональне призначення

Функції, які виконує застосунок:

- додавання в систему користувачів;
- додавання в систему камер;
- надання доступу користувачам до камер;
- авторизація користувача
- перегляд користувачем камер у лайф режимі;
- перегляд записів камер на FTP сервері;

– запис камер при перегляді, та можливість завантажити записаний матеріал;

6.4.3 Опис логічної структури застосунку

6.4.3.1 Побудова та запуск застосунку

Для встановлення залежностей у проект було використано менеджер залежностей NPM. Для встановлення залежностей потрібно виконати команду “npm install”.

Для запуску застосунку потрібно запустити docker-compose завдяки команді “docker-compose up”. Ця команда завантажить необхідні docker образи та налаштує усі необхідні мікросервіси.

6.4.3.2 Реалізація серверної частини

При ініціалізації програми першим ділом завантажується сервіс адмін панелі разом з базою даних. Після цього, стартує сервіс обробки відеопотоку з камер, який звертається по API до панелі адміністратора за діючими камерами. Після отримання списку камер, сервіс обробки підключається до кожної камери, завдяки програмі FFMPEG. Сервіс робить fork програми FFMPEG та починає читати stdout.

При підключенні до камери, программа FFMPEG починає передавати дані в stdout, тим часом, сервіс обробки відеопотоку вичитує данні та починає записувати їх у файли, до яких можна получити доступ по протоколу SFTP, на сервері. Також сервіс ініціалізує канал передачі даних – WebSocket, який очікує підключення клієнтів.

При підключені до WebSocket, клієнт відсилає JWT токен, який він получив при авторизації. Сервіс його перевіряє, якщо токен валідний – починається передача відеопотоку.

При оновлені даних в адмін панелі, спрацьовує WebHook, який посилає нову інформацію до сервісу маршрутизації даних. Якщо були оновлені камери,

то сервіс маршрутизації даних сповіщає сервіс обробки відеопотоку, який звіряє та оновлює камери – включає нові відео потоки, виключає видалені.

6.4.3.3 Реалізація інтерфейсу користувача

Інтерфейс користувача складається з двох частин:

1) панель адміністратора;
2) сторінка перегляду камер.

Адмін панель – це місце, де адміністратор налаштовує систему. Для того, щоб зайти в панель адміністратора, спочатку потрібно ввести, на сторінці авторизації, адмінську електронну пошту та пароль (рисунок 6.24).

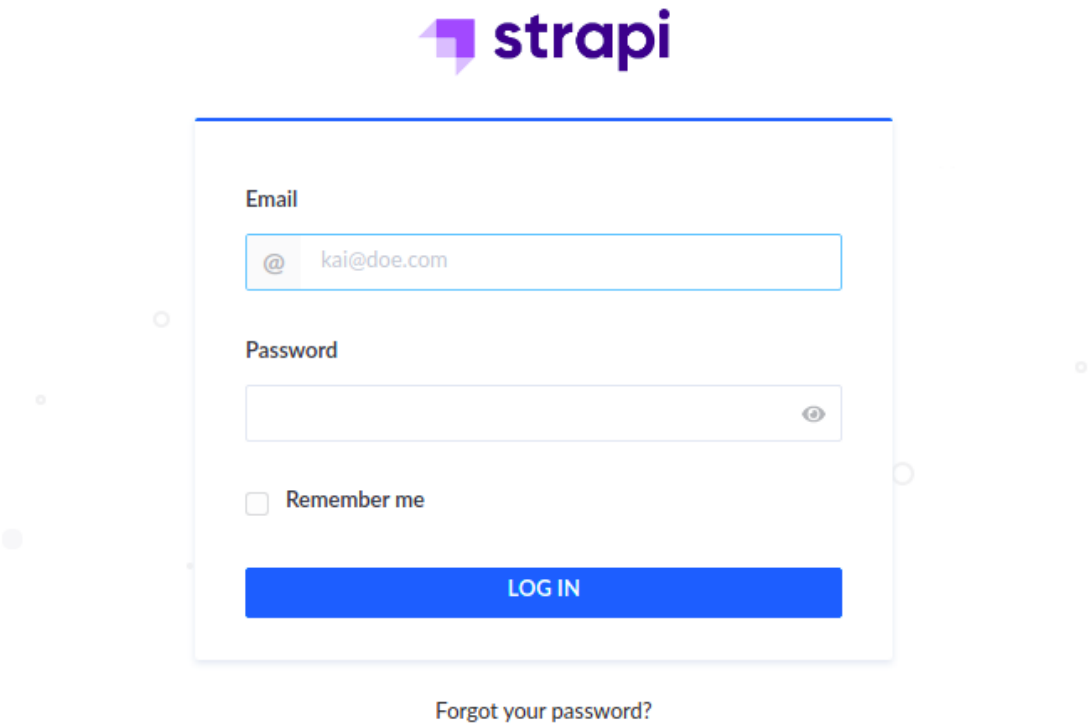

Рисунок 6.24 – Авторизація

Якщо авторизація пройшла успішно, користувач адмін панелі побачить меню (рисунок 6.25).

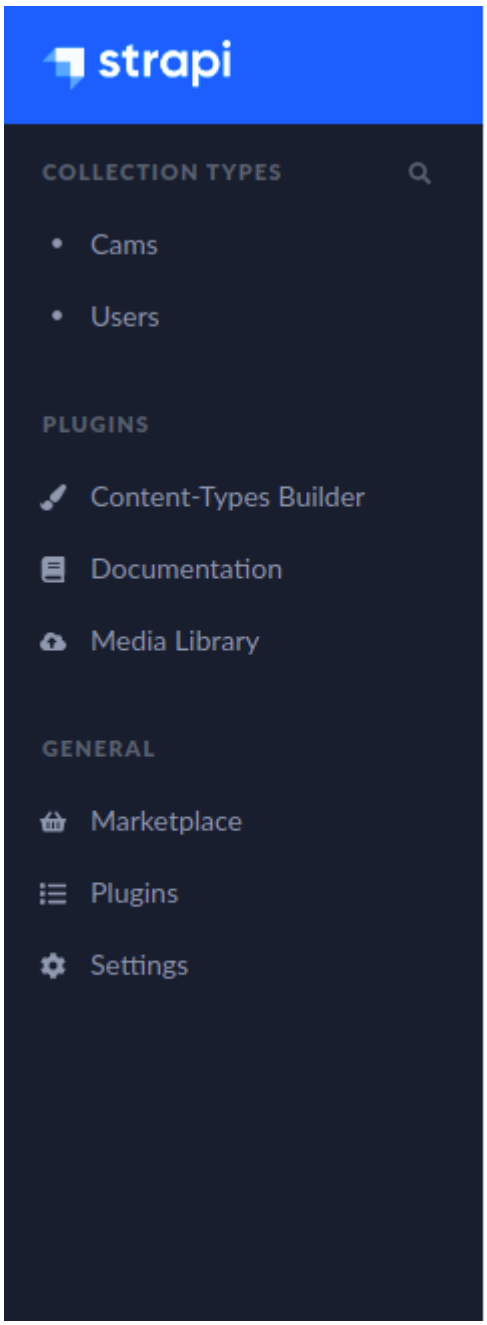

Рисунок 6.25 – Меню

В меню є два основних пункти, для роботи з системою:

1) Cams – це сторінка, на якій, користувач адмін панелі може переглядати (рисунок 6.26), створювати (рисунок 6.28), та змінювати (рисунок 6.27) відеокамери.

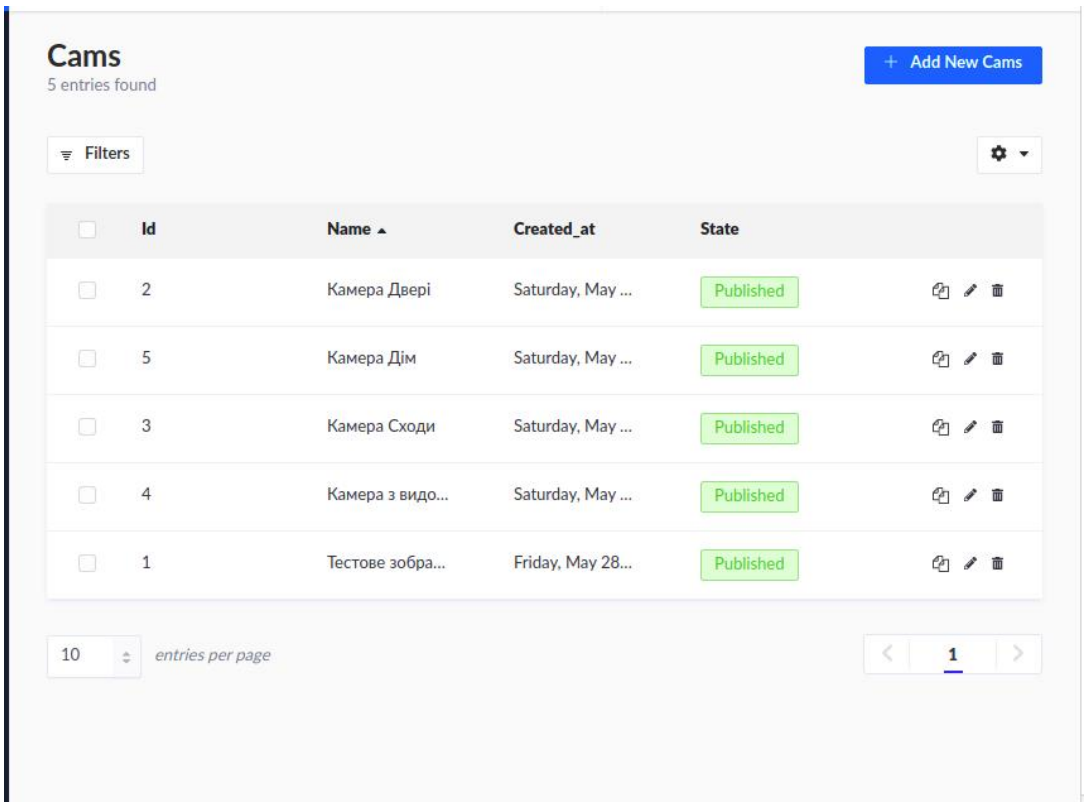

Рисунок 6.26 – Перегляд існуючих камер

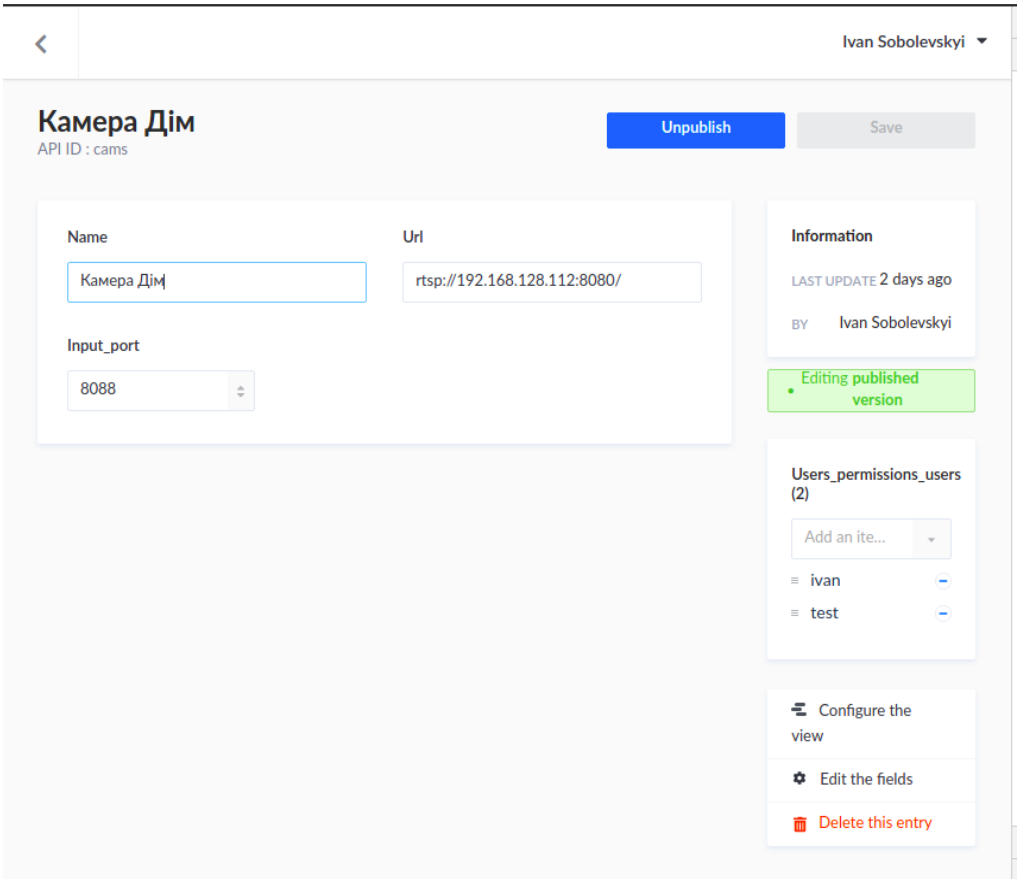

Рисунок 6.27 – Зміна існуючої камери

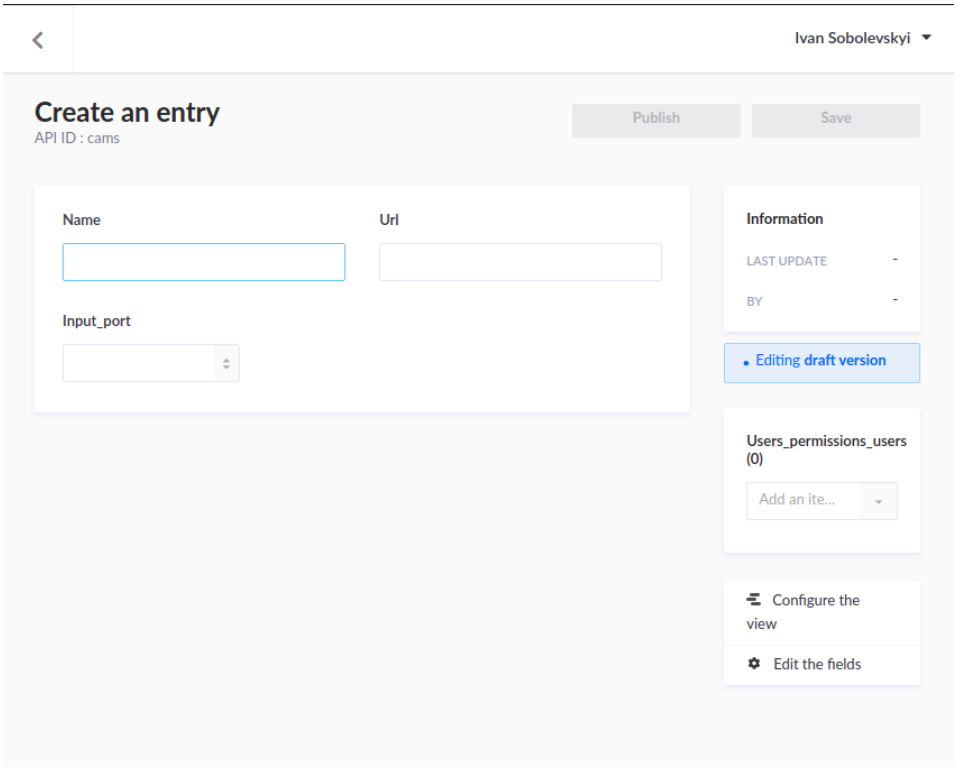

Рисунок 6.28 – Створення нової камери

Також користувач адмін панелі може добавляти чи змінювати користувачів, які мають доступ до конкретної камери (рисунок 6.29).

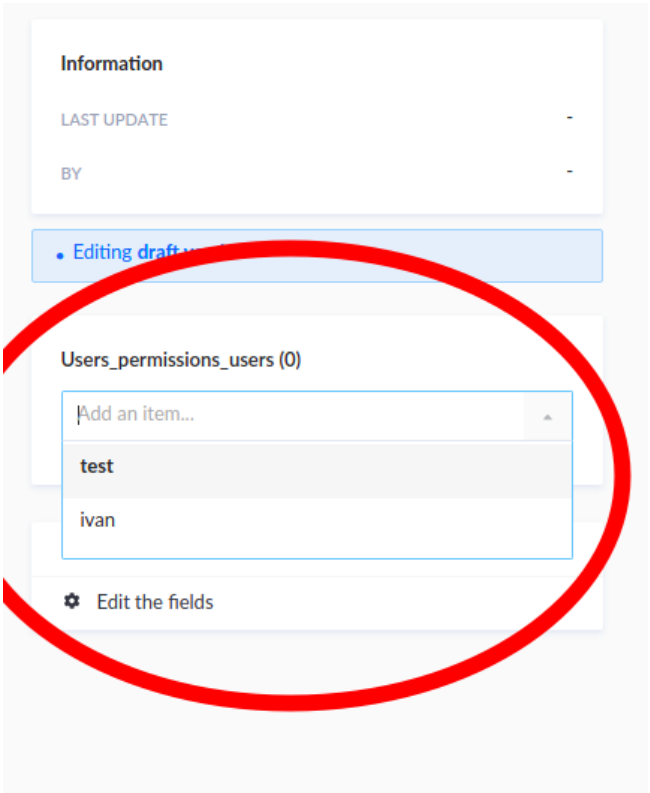

Рисунок 6.29 – Надання права перегляду камери користувачам

2) Users – це сторінка, на якій, користувач адмін панелі може переглядати (рисунок 6.30), створювати (рисунок 6.32), та змінювати (рисунок 6.31) користувачів системи.

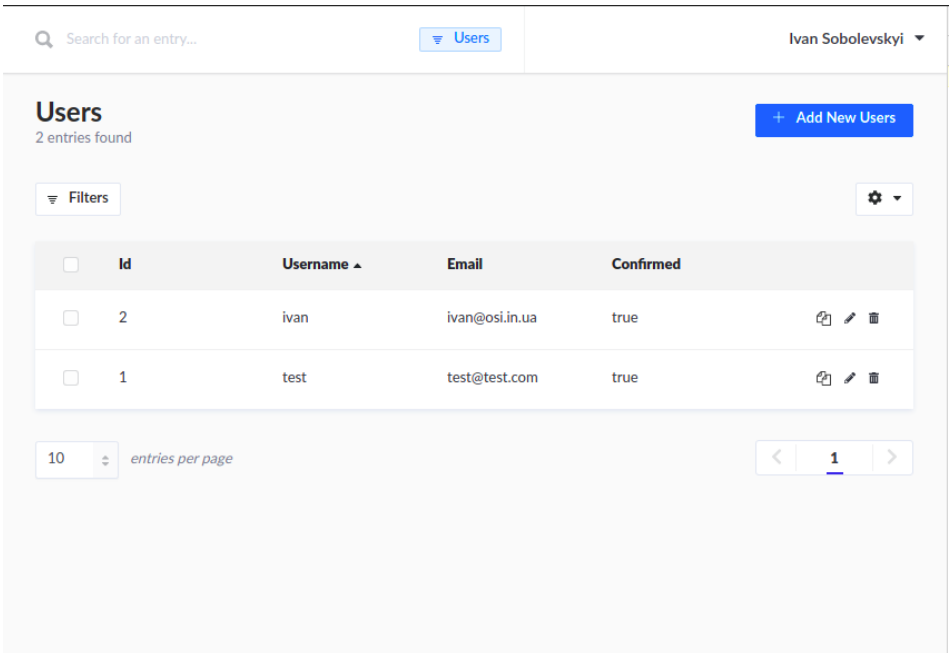

Рисунок 6.30 – Перегляд існуючих користувачів системи

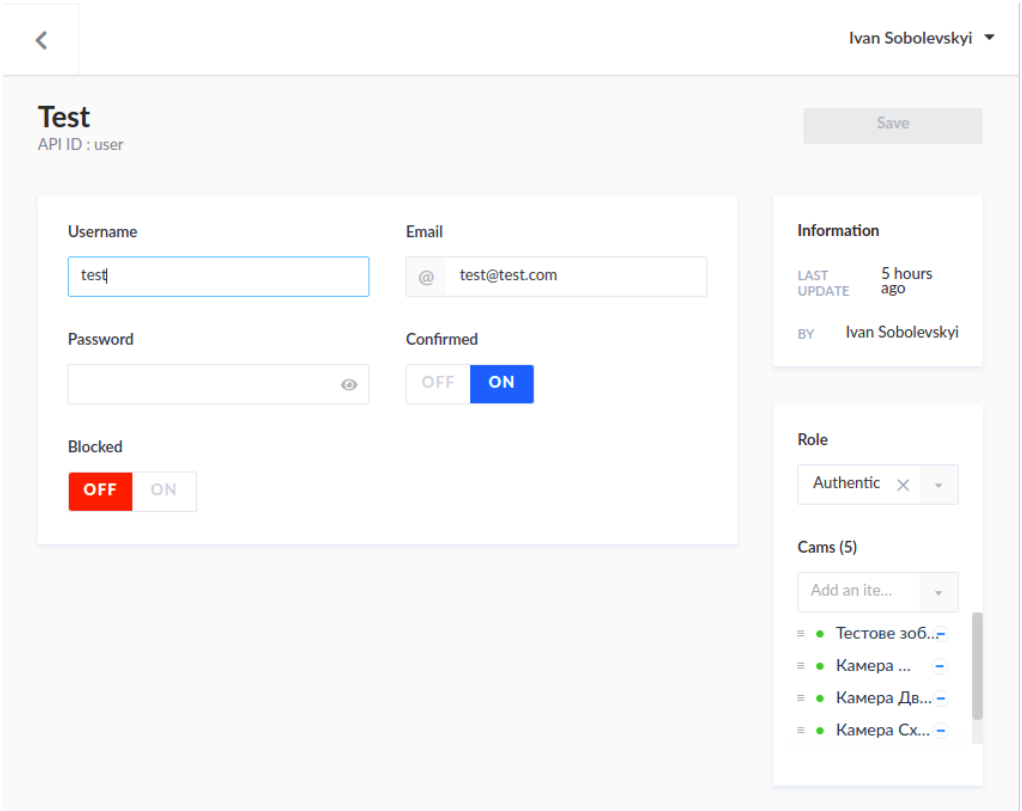

Рисунок 6.31 – Зміна існуючого користувача

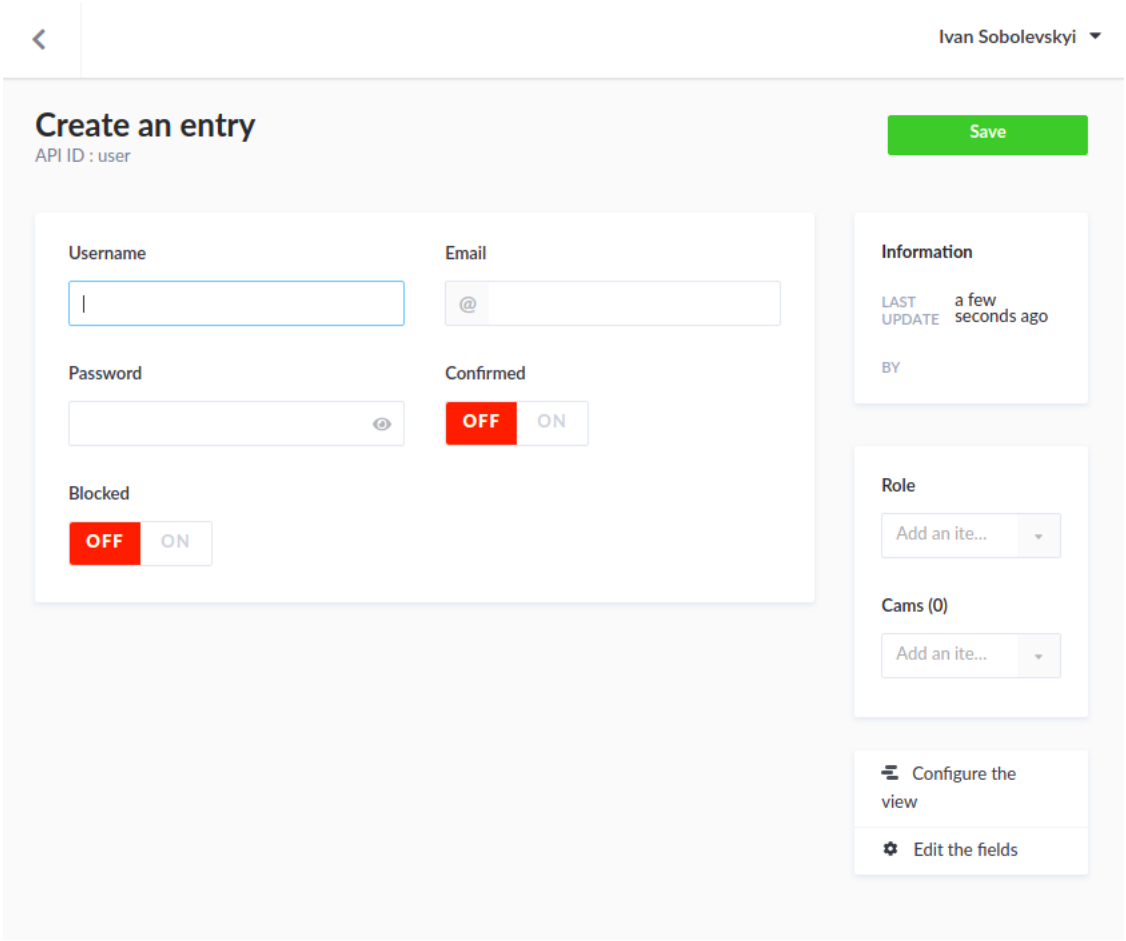

Рисунок 6.32 – Створення нового користувача

Також користувач адмін панелі може добавляти чи змінювати доступи до камер у конкретного користувача (рисунок 6.33).

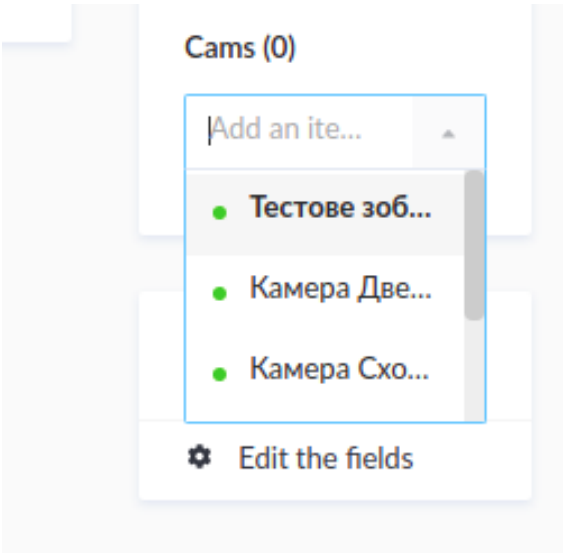

Рисунок 6.33 – Додавання камери користувачу

Сторінка перегляду камер. Спочатку, для того, щоб авторизуватись в системі, користувач повинен ввести, на сторінці авторизації, наданий йому, адміністратором, логін та пароль та натиснути на кнопку “AUTH” (рисунок 6.34).

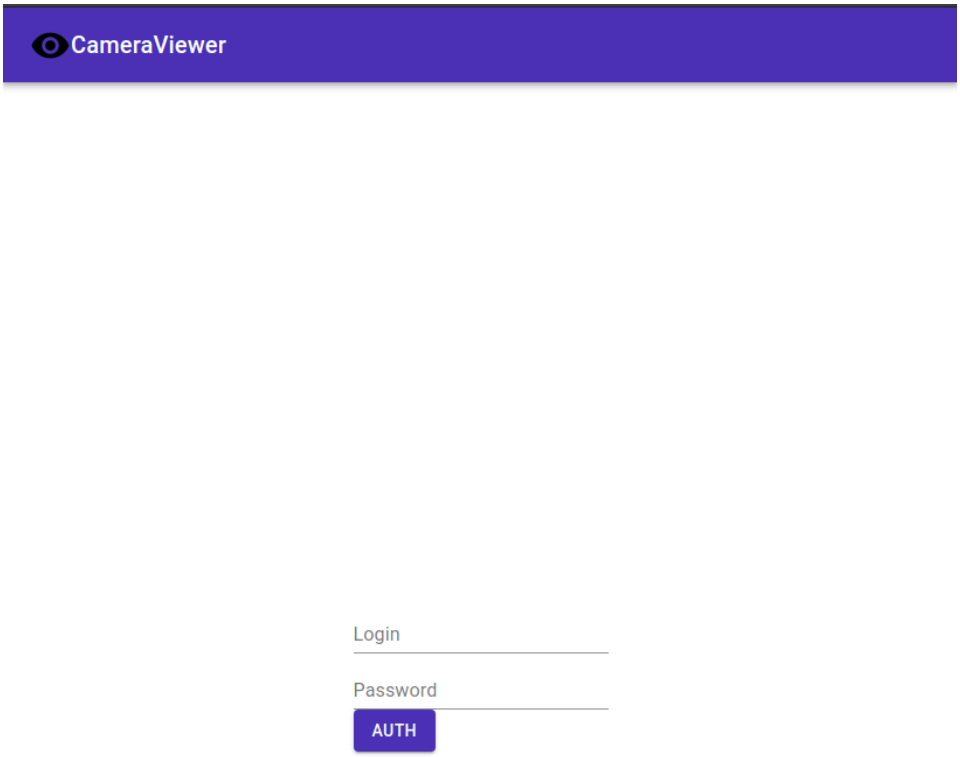

Рисунок 6.34 – Сторінка авторізації

Якщо користувач успішно авторизувався, він получить JWT токен та дані про камери. В цей момент сторінка зміниться. Користувач побачить інтерфейс для перегляду камер (Рисунок 6.35), який складається із елементів:

а) плеєр – це вікно, в якому користувач бачить потокове відео з камер;
б) список вибору камери – це спливаючий список призначений для вибору камери, що переглядається (Рисунок 6.36);
в) панель запису відео – завдяки цій панелі можна записувати відео, що переглядається. Для того, щоб почати запис, потрібно натиснути кнопку

“RECORD”. Після початку запису стане активною кнопка “STOP RECORD”, яку потрібно натиснути для завершення запису. Коли запис буде завершено, активується кнопка “DOWNLOAD”, яка видає записане відео в форматі mp4.

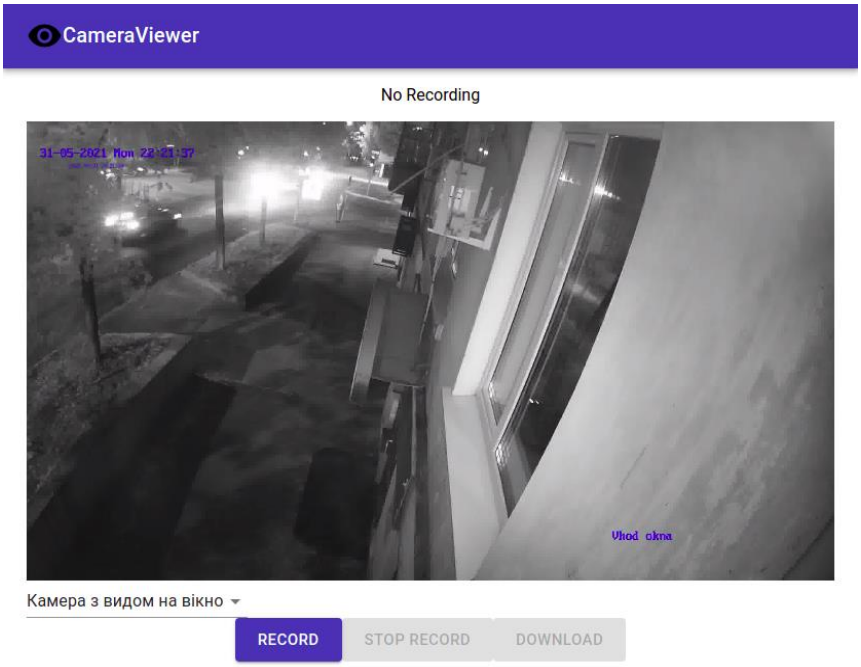

Рисунок 6.35 – Сторінка перегляду, наданих адміністратором, камер

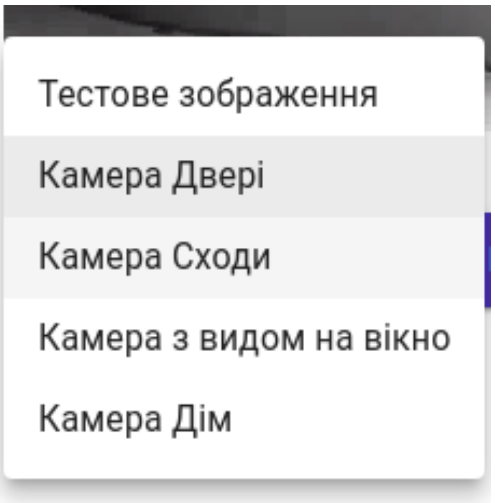

Рисунок 6.36 – Вибір поточної камери

6.4.3.4 Використовувані технічні засоби

Для забезпечення кросплатформеності та швидкого налаштування ПЗ було використано контейнеризацію завдяки Docker.

Docker – це платформа для ізолювання процесів у контейнерах. Завдяки такій контейнеризації налаштування сервісів запуску та необхідного ПЗ можна зберігатися в програмному коді.

Завдяки Docker було вирішено проблему налаштування мікросервісної архітектури, що значно прискорило розробку, та прискорює випуск нових релізів на головному сервері.

6.4.3.5 Виклик і завантаження застосунку

Для забезпечення версійності програмного забезпечення, код застосунку було залито у систему версій Git, а саме на сервера GitLab. До завантаження програмного коду, доступ мають лише авторизовані розробники, та адміністратор системи.

Для запуску застосунку потрібно виконати інструкцію з розділу 6.4.3.1. Застосунок запустить веб сервер бекенду та фронтенду на localhost.

6.4.3.5 Вхідні і вихідні дані

Вхід в админ панель:

а) точка API: http://localhost:1337;

б) метод авторизації: Basic Auth.

Вхід в інтерфейс користувача:

а) точка API: http://localhost:3000;

б) метод авторизації: Basic Auth.

Вхід для авторизації користувача:

а) точка API: http://localhost:1337/auth;

б) метод авторизації: Basic Auth.

Вхід для отримання інформації о камерах:

а) точка API: http://localhost:1337/cams;

б) метод авторизації: Bearer Token;

в) формат вихідних даних: Json;

г) вихідні дані:

- назва камери (string);
- адреса URL для доступу до камери (string);
- порт для підключення веб сокету (int).

Вхід для отримання відеопотоку з камер:

а) точка API: ws://localhost:80xx (для кожної камери відкривається окремий порт, заданий в адмін панелі)

б) метод авторизації: Bearer Token;

в) формат вихідних даних: Blob, MJPEG;

г) вихідні дані:

- бітова послідовність в формат MJPEG (bit)

ВИСНОВКИ

Під потреби підприємства “АН ЗОЛОТІ КЛЮЧІ” було розроблено мережу для корпоративного використовування. Мережа була розроблена для п’яти підрозділів підприємства. Було підібране обладнання, завдяки якому ця мережа може вправно функціонувати. Для забезпечення комфортної роботи користувачів було проведено математичні обчислення інтенсивності трафіка, та підібрано канал, який задовольняє потреби мережі.

Мережа підприємства “АН ЗОЛОТІ КЛЮЧІ” поєднано з мережею котеджного містечка “Золоті Ключі”.

Було розроблено систему відеоспостереження, яка базується на мікрокомп’ютері Raspberry Pi, камери було встановлено в чотирьох будівлях котеджного містечка, що підвищує рівень безпеки. Система розроблена з ціллю максимальної масштабованості, тому очікується нові бажаючі, для встановлення відеонагляду в котеджному містечку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Побудова схеми організаційної структури підприємства у MS Visio URL: http://modeling.at.ua/publ/10-1-0-54

2. DOM.RIA.com URL: https://dom.ria.com/uk/realty-prodaja-dom-dnepropetrovsk-zolotyie-klyuchi-olavkaya-lia-16481716.html

3. Чистяков В. И. Сравнение аналогового и IP-видеонаблюдения / В. И. Чистяков. // Международный студенческий научный вестник. – 2015. – №4. – С. 378–379.

4. Secur URL: https://secur.ua/ua/videonablyudenie/kamery/hd-sdi-camery/

5. Комп'ютерні мережі / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.

6. Zurawski R. RTP, RTCP, and RTSP - Internet Protocols for Real-Time Multimedia Communication / R. Zurawski, A. Durresi, R. Jain // The Industrial Information Technology Handbook / R. Zurawski, A. Durresi, R. Jain., 2005.

7. Phil Henken. RTSP – All You Need to Know About Real-Time Streaming Protocol. URL: https://corp.kaltura.com/blog/rtsp-streaming/ (дата звернення: 06.04.2021).

8. Osso R. Handbook of Emerging Communications Technologies: The Next Decade / Rafael Osso., 2000. – 416 с.

9. Обзор протокола HTTP. URL: https://developer.mozilla.org/ru/docs/Web/HTTP/Overview

10. Kaufmann M. The Internet and Its Protocols: a comparative approach / Morgan Kaufmann. – San Francisco, 2004. – 840 с.

11. Семенов Ю. А. Протоколы и алгоритмы маршрутизации в Интернет [Електронний ресурс] / Ю. А. Семенов // НОУ «ИНТУИТ». – 2007. – Режим доступу до ресурсу: http://book.itep.ru/1/intro1.htm .

12. Type of Network Topology: Bus, Ring, Star, Mesh, Tree, P2P, Hybrid. URL: https://www.guru99.com/type-of-network-topology.html

13. Cisco Packet Tracer Data Sheet. URL: https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

14. Cisco Packet Tracer URL: https://www.netacad.com/courses/packet-tracer

15. Що ви повинні знати про async & await в JavaScript URL:https://codeguida.com/post/658

16. Модуль PoE живлення POE_BOARD для Raspberry Pi 3+ та 4 URL: https://arduino.ua/prod2846-modyl-poe-pitaniya-poe_board-dlya-raspberry-pi

17. Комутатор мережевий Mikrotik CRS112-8P-4S-IN URL: https://www.itbox.ua/ua/product/Kommutator_setevoy_Mikrotik_CRS112-8P-4S-IN-p325594/?utm=shopping&utm_content=shopping&gclid=Cj0KCQjw--GFBhDeARIsACH_kda_cXzH_W0kVS81XplZFsCHPkS25HZ7BFJJ7G3rUfeK4_Od_-gfKRIaAi4DEALw_wcB#product-gallery-popup

18. Маршрутизатор Cisco C2901-WAASX-SEC/K9 URL: https://stack-systems.com.ua/marshrutizator-cisco-c2901-waasx-sec-k9

19. Коммутатор Cisco SB SF200-24FP (SF200-24FP-EU) URL: https://stack-systems.com.ua/kommutator-cisco-sb-sf200-24fp-sf200-24fp-eu

20. Monk S. Raspberry Pi Cookbook: Software and Hardware Problems and Solutions / Simon Monk., 2016. – 510 с.

21. Wieruch R. The Road to React: Your journey to master plain yet pragmatic React / Robin Wieruch., 2020. – 248 с.

22. Пауэрс Ш. Изучаем Node. Переходим на сторону сервера/Ш. Пауэрс. – Санкт-Петербург: Питер, 2017. – 304 с. – (2-е).

ДОДАТОК А

Текст програми веб відеонагляду

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
ВЕБ ВІДЕОНАГЛЯД

текст програми

804.02070743.20005-01 12 01

Листів 10

2021

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програми веб-відеонагляд. Програма призначена для обробки камер за протоколом RTSP, транслювання цих камер в режимі онлайн на веб сторінку, запис відеопотоку на FTP сервер.

ЗМІСТ

1 ТЕКСТ ПРОГРАМИ 5

1.1 Сервіс збору відеопотоку 5

1.2 Докер файл запуску сервісів серверного ПЗ 6

1.3 Сервіс інтерфейсу користувача 8

1 ТЕКСТ ПРОГРАМИ

1.1 Сервіс збору відеопотоку

```
const { getCams } = require('./api/cams/cams')
const Stream = require('./node-rtsp-stream-es6')
const Recorder = require('node-rtsp-recorder').Recorder

const onlineStreams = {}

function createRecord(cam) {
 console.log(cam.name.replace(/\s+/g, ''))
 var rec = new Recorder({
   url: cam.url,
   timeLimit: 5*60, // time in seconds for each segmented video file
   folder: '/code/videos',
   name: cam.name.replace(/\s+/g, ''),
   fileNameFormat: 'hh:mm:ss'
 })
 rec.fileNameFormat =
 rec.startRecording();
}

async function createStreams(cams) {
 for(const cam of cams) {
   stream = new Stream({
     name: cam.name,
     url: cam.url,
     port: cam.input_port
   })
   stream.start()
```

```
  createRecord(cam)
 }
}


async function main() {
 let data = undefined;
 while(data == undefined) {
  try {
   data = await getCams();
  } catch {
   data = undefined
  }
 }
 await createStreams(data);
 console.log(data)
}

main()
```

1.2 Докер файл запуску сервісів серверного ПЗ

```
version: '3'
services:
 strapi:
  build:
   context: ./admin/docker
  ports:
   - 1337:1337
  volumes:
   - ./admin:/code
```

```
    - /etc/localtime:/etc/localtime:ro
  command: yarn strapi develop

 rtsp-to-ws:
   build:
     context: ./rtsp-to-ws/docker
   restart: always
   ports:
     - 8081-8090:8081-8090
   depends_on:
      - "strapi"
   volumes:
     - ./rtsp-to-ws:/code
     - /etc/localtime:/etc/localtime:ro
   command: node index.js

 router:
   build:
     context: ./router/docker
   depends_on:
     - "strapi"
   volumes:
     - ./router:/code
     - /etc/localtime:/etc/localtime:ro
   command: npm start
```

1.3 Сервіс інтерфейсу користувача:

```
import React from 'react';
import store  from './store';
import TopBar from './components/TopBar';
```

```
import Stream from './components/Stream';
import { Auth } from './components/Auth';
import { Provider } from 'react-redux';

import Container from '@material-ui/core/Container';
import Select from '@material-ui/core/Select';
import MenuItem from '@material-ui/core/MenuItem';
import { useSelector } from 'react-redux'
import config from './config'

function MultipleStreamBar() {
 const cams = useSelector((state) => state.auth.cams)
 console.log(cams)
 const [port, setPort] = React.useState(cams[0].input_port);

 const jwt = useSelector((state) => state.auth.jwt)

 const handleChange = (event) => {
   console.log(event.target.value)
   setPort(event.target.value);
 };

 return (
   <>
     <Stream    url={`ws://${config.backend.url}:${port}/?key=${jwt}`}    key='tab-
8083' id="8083">
      <Select
         labelId="demo-simple-select-error-label"
         id="demo-simple-select-error"
         value={port}
```

```
        onChange={handleChange}
       >
        {cams.map((cam) => <MenuItem key={cam.name}
value={cam.input_port}>{cam.name}</MenuItem>)}
       </Select>
     </Stream>
  </>
)
}

function App() {
 const isAuth = useSelector((state) => state.auth.isAuth)
 console.log('token', isAuth)

 return (
   <div className="App">
    <header className="App-header">
     <TopBar
      name="CameraViewer"
     ></TopBar>
     <Container>
      {
       isAuth ?
         <MultipleStreamBar></MultipleStreamBar> :
         <Auth></Auth>
      }
     </Container>

    </header>
   </div>
```

```
 );
}

export function AppWrapper() {
 return (
   <Provider store={store}>
     <App />
   </Provider>
 )
}
```