

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ**

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «ІНФОРМАЦІЙНО-НАВЧАЛЬНЕ
СЕРЕДОВИЩЕ З СИСТЕМОЮ ІДЕНТИФІКАЦІЇ
ДЛЯ ЗАКЛАДІВ ОСВІТИ»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

*Кваліфікаційна робота містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

 (підпис)	 <i>Олександр СИЖКО</i> Ім'я, ПРІЗВИЩЕ здобувача
---	---

Виконав:	здобувач(ка) вищої освіти гр. <u>КСДМ-62</u> <u>Олександр СИЖКО</u> Ім'я, ПРІЗВИЩЕ
Керівник: <i>науковий ступінь, вчене звання</i>	<u>Віталій ВОЛОХІН</u> Ім'я, ПРІЗВИЩЕ
Рецензент: <i>науковий ступінь, вчене звання</i>	 Ім'я, ПРІЗВИЩЕ

Київ 2025

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти Магістр

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ

Завідувач кафедри Наталія ЛАЩЕВСЬКА

_____ Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Сижко Олександр Юрійович

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Інформаційно-навчальне середовище з системою ідентифікації для закладів освіти»

керівник кваліфікаційної роботи: Віталій ВОЛОХІН, канд.техн.наук, доцент

(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024р. №320

2. Строк подання кваліфікаційної роботи «29» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, технології передачі даних в системах відеоспостереження, методи ідентифікації особи, вимоги до навчальних середовищ.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Загальні відомості про системи відеоспостереження та штучний інтелект

2. Огляд технологій біометричного контролю доступу

3. Перелік сучасних інформаційно-навчальних середовищ

4. Підбір комплектуючих та налаштування системи

5. Перелік ілюстративного матеріалу: презентація

1. Мета, об'єкт, предмет дослідження

2. Актуальність роботи

3. Вибір обладнання для системи відеоспостереження та контролю доступу

4. Блок-схема структури локальної мережі навчального закладу

5. Фізична структура першого поверху навчального закладу

6. Фізична структура другого поверху навчального закладу

7. Демонстрація характеристик серверу та програм для функціонування системи

8. Кінцеве налаштування системи Moodle

9. Висновки

10. Публікації та апробація роботи

6. Дата видачі завдання «01» вересня 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	16.10-23.10.2024	виконано
2	Вивчення матеріалів для аналізу розвитку систем відеоспостереження та штучного інтелекту	23.10-6.11.2024	виконано
3	Аналіз розвитку систем біометричного контролю доступу та методів ідентифікації особи	6.11- 15.11.24	виконано
4	Аналіз переваг та особливостей актуальних інформаційно-навчальних середовищ	15.11-22.11.24	виконано
5	Підбір обладнання для систем відеоспостереження, біометричного контролю доступу та інформаційно-навчального середовища	22.11-1.12.24	виконано
6	Встановлення необхідних програм та налаштування пристроїв	1.12-6.12.24	виконано
7	Оформлення роботи: вступ, висновки, реферат	6.12-7.12.24	виконано
8	Розробка демонстраційних матеріалів	7.12- 11.12.24	виконано
9	Попередній захист роботи	12.12.24	виконано

Здобувач вищої освіти

(підпис)

Олександр СИЖКО
(Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи

(підпис)

Віталій ВОЛОХІН
(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступня магістр: 105 стор., 75 рис., 12 табл., 32 джерел.

Мета роботи – проектування та налаштування інформаційно-навчального середовища з системою ідентифікації особи за допомогою відеоспостереження та системи контролю доступу в навчальному закладі.

Об'єкт дослідження – інформаційно-навчальне середовище навчального закладу та системи ідентифікації особи.

Предмет дослідження – інтеграція технології ідентифікації особи, системи відеоспостереження та контролю доступу та інформаційно-навчальне середовище і їх впровадження в навчальний заклад.

Короткий зміст роботи: У роботі оглянуто сучасні типи відеоспостереження, систем біометричного контролю доступу та актуальних інформаційно-навчальних середовищ.

У практичній частині реалізовано підбір та налаштування обладнання для реалізації систем відеоспостереження та контролю доступу та інформаційно-навчального середовища. Розроблено проєкт розташування систем відеоспостереження та контролю доступу в навчальному закладі.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНО-НАВЧАЛЬНЕ СЕРЕДОВИЩЕ, СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ, ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ, СИСТЕМА БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ, МЕТОДИ ІДЕНТИФІКАЦІЇ ОСОБИ, ШТУЧНИЙ ІНТЕЛЕКТ, СЕРВЕР.

ABSTRACT

Text part of the master's qualification work: 105 pages, 75 figures, 12 tables, 32 sources.

The purpose of the work – design and configuration of an informational and educational environment with a facial identification system using video surveillance and access control in an educational institution.

Object of research – informational and educational environment of an educational institution and personal identification systems.

Subject of research – Integration of facial identification technology, video surveillance and access control systems, and the informational and educational environment into an educational institution.

Summary of the work: The study explores modern types of video surveillance, biometric access control systems, and current informational and educational environments.

In the practical part, equipment selection and configuration were implemented for the realization of video surveillance and access control systems, as well as the informational and educational environment. A project for the placement of video surveillance and access control systems within an educational institution was developed.

KEYWORDS: INFORMATIONAL AND EDUCATIONAL ENVIRONMENT, VIDEO SURVEILLANCE SYSTEM, DATA TRANSMISSION TECHNOLOGIES, BIOMETRIC ACCESS CONTROL SYSTEM, PERSONAL IDENTIFICATION METHODS, ARTIFICIAL INTELLIGENCE, SERVER.

ЗМІСТ

ВСТУП.....	9
1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО СИСТЕМИ ВІДЕОПОСТЕРЕЖЕННЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ	10
1.1 Відеоспостереження в навчальному закладі.....	10
1.2 Завдання які вирішують камери відеоспостереження в навчальному закладі та законність їх впровадження	11
1.3 Способи передачі даних в системах відеоспостереження	13
1.4 Штучний інтелект та сфери його застосування	22
2 ОГЛЯД ТЕХНОЛОГІЙ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ	27
2.1 Сучасні уявлення про технології біометричної ідентифікації для контролю та управління доступом	27
2.2 Технології біометричної ідентифікації	28
2.2.1 Ідентифікація за допомогою відбитків пальців	30
2.2.2 Ідентифікація за допомогою райдужної оболонки ока	31
2.2.3 Ідентифікація за геометрією обличчя.....	32
2.2.4 Ідентифікація за малюнком вен	35
2.3 Допоміжне обладнання для системи біометричного контролю доступу ..	37
3 ПЕРЕЛІК СУЧАСНИХ ІНФОРМАЦІЙНО-НАВЧАЛЬНИХ СЕРЕДОВИЩ	43
3.1 Поняття інформаційно-навчальне середовище та огляд існуючих платформ.....	43
3.2 Обладнання для організації інформаційно навчального середовища	48
4 ПІДБІР КОМПЛЕКТУЮЧИХ ТА НАЛАШТУВАННЯ СИСТЕМИ	50
4.1 Підбір компонентів комплексної системи контролю доступу та відеоспостереження	50
4.2 Проєктування та налаштування системи контролю доступу та відеоспостереження.	65
4.3 Встановлення та налаштування навчального середовища Moodle на локальний сервер навчального закладу.	77
ВИСНОВКИ	90
ПЕРЕЛІК ПОСИЛАНЬ	91
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ(Презентація)	94

ВСТУП

Сучасний розвиток інформаційних технологій ставить нові виклики перед закладами освіти, які прагнуть підвищити рівень ефективності навчального процесу, забезпечити безпеку всіх учасників освітнього середовища та оптимізувати управлінські процеси. Одним із ключових завдань є побудова комплексної системи, що об'єднує функції навчання, ідентифікації осіб та контролю доступу до території навчального закладу.

Актуальність дослідження зумовлена необхідністю створення інформаційно-навчального середовища з інтегрованими системами відеоспостереження та контролю доступу на основі ідентифікації облич. Такі рішення забезпечують не лише безпеку навчального закладу, а й покращують організацію освітнього процесу завдяки ефективному управлінню даними.

Мета даної дипломної роботи полягає у проєктуванні інформаційно-навчального середовища з інтегрованою системою ідентифікації осіб та контролю доступу для навчального закладу. Досягнення цієї мети передбачає вирішення низки завдань, зокрема проєктування архітектури системи, вибір обладнання, налаштування програмного забезпечення та забезпечення взаємодії усіх компонентів системи.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ

1.1 Відеоспостереження в навчальному закладі

Головним завданням є забезпечення безпеки дітей, які проводять значну частину часу в навчальних закладах як під час занять, так і в позаурочний час. Школи є місцями, де учні перебувають найбільше часу, тому забезпечення їхньої безпеки є пріоритетом для батьків, адміністрації та суспільства в цілому. Сучасні системи відеоспостереження здатні ефективно вирішити це завдання, створюючи умови для контролю за подіями в навчальному закладі та підвищуючи рівень дисципліни серед учнів.

Встановлення систем відеоспостереження у школі має кілька важливих переваг. По-перше, воно сприяє формуванню дисциплінарного ефекту, що позитивно впливає на поведінку учнів. По-друге, наявність відеокамер дає можливість оперативно та об'єктивно з'ясувати обставини інцидентів, таких як травми, хуліганство, крадіжки або інші небажані ситуації, які можуть виникнути у навчальному закладі. Це забезпечує прозорість і дозволяє уникнути непорозумінь між учасниками конфліктів.

Водночас встановлення систем відеоспостереження потребує раціонального та делікатного підходу. Камери мають бути розміщені у важливих і стратегічних зонах, де це справді необхідно, а не повсюди. Планування та впровадження системи відеоспостереження повинно розпочинатися з обговорення між адміністрацією навчального закладу, педагогами, учнями та їхніми батьками. Це дозволить врахувати інтереси всіх сторін, забезпечити відповідність законодавчим нормам і створити оптимальну систему, яка не лише захищає дітей, а й зберігає їхню приватність.

Таким чином, впровадження сучасних систем відеоспостереження в навчальних закладах є важливим кроком до створення безпечного середовища, де діти можуть навчатися та перебувати під надійним захистом.[2]



Рисунок 1.1 – Відеоспостереження в навчальному закладі.

1.2 Завдання які вирішують камери відеоспостереження в навчальному закладі та законність їх впровадження

Правильно спроектувавши систему відеоспостереження для школи, можна уникнути багатьох правопорушень, а також вирішити такі завдання:

- контролювати на віддаленій відстані всі входи і виходи;
- знайти винних у разі вчинення правопорушення або хуліганських дій;
- вчасно виявити виникнення надзвичайної ситуації;
- запобігти незаконному проникненню на територію сторонніх осіб;
- виявити регулярно спізнюються учнів;
- повністю контролювати навчальний процес (виконання педагогами своїх посадових обов'язків, попередження та вирішення конфліктів, що виникають та інше.).

Можна сказати, що установка відеоспостереження в школі дозволяє не тільки забезпечити безпеку співробітників і учнів, а й підвищити рівень їх дисципліни, а також якість навченості.

На перший погляд, організувати відеоспостереження в шкільних закладах може здатися нескладним завданням: потрібно лише знайти фінансування та встановити камери відеоспостереження. Це, безумовно, дозволить покращити безпеку учнів та персоналу, допомогти у боротьбі з підлітковою злочинністю, а також зберегти шкільне майно від пошкоджень. Окрім того, враховуючи, що в школі, як правило, працює лише один охоронець, а приміщення навчального закладу можуть бути досить великими, відеоспостереження стане важливим інструментом для моніторингу порушень дисципліни серед учнів і своєчасного попередження конфліктів.

Проте процес організації відеоспостереження не є таким простим, адже збір інформації має здійснюватися законно. Важливо пам'ятати, що відеоспостереження торкається особистих прав і свобод громадян, що часто викликає дискусії серед учнів, батьків та викладачів. Крім того, на сьогоднішній день законодавство України щодо використання відеоспостереження в навчальних закладах недостатньо регулюється.

Перед установкою системи відеоспостереження в школі необхідно заручитися згодою вчителів, батьків, учнів та технічного персоналу. Без такої згоди подібні дії можуть призвести до адміністративної та кримінальної відповідальності. Директор навчального закладу має прийняти акт, що визначає порядок організації системи відеоспостереження, а також перелік осіб, які матимуть доступ до відеоданих і терміни зберігання інформації.

Водночас необхідно дотримуватися певних етичних та правових норм. Відеоспостереження неприпустимо в тих місцях, де порушуються права на захист особистого життя, таких як туалети, роздягальні, медпункт, кабінети психолога та інші приватні приміщення. Також обов'язково потрібно повісити табличку про те, що ведеться відеоспостереження, і забезпечити конфіденційність отриманих даних, яка зображена на рис. 1.2.



Рисунок 1.2 – Попередження про ведення відеоспостереження.

1.3 Способи передачі даних в системах відеоспостереження

Основною перевагою бездротових систем відеоспостереження є простота монтажу. При встановленні такої системи головне завдання полягає в забезпеченні джерела живлення, яке має бути розташоване неподалік від відеокамери. Після цього залишається лише встановити камери на обраних місцях і налаштувати пристрій для запису даних.

Бездротове відеоспостереження є оптимальним рішенням у випадках, коли прокладання кабелю є неможливим або надто витратним, що робить традиційні системи нераціональними. Такі системи також ефективно використовуються у мобільних рішеннях охорони або для віддаленого моніторингу об'єктів, де відсутні постійні охоронці чи інший персонал. У подібних ситуаціях до систем висуваються вимоги автономної роботи та мінімального обслуговування.

Бездротові системи відеоспостереження також користуються популярністю у приватному секторі, де виникає потреба передавати інформацію власнику будинку або ділянки. Для передачі даних використовуються різні технології, такі як GSM-модулі, Bluetooth, Wi-Fi тощо. Вибір конкретного модуля залежить від відстані, на яку необхідно передати інформацію, та особливостей об'єкта спостереження.

Бездротові відеокамери мають ряд недоліків, які можуть обмежувати їх ефективність у системах відеоспостереження. Одним із найбільших недоліків

є низька якість зображення. Більшість бездротових відеокамер, що доступні на ринку сьогодні, мають роздільну здатність менше 720×480 пікселів, що не завжди відповідає сучасним вимогам безпеки.

Ще одним значним недоліком є те, що бездротові камери працюють у діапазоні 2,4 ГГц, який є надзвичайно завантаженим. Цю частоту активно використовують мікрохвильові печі, мобільні телефони, автосигналізації, а також Bluetooth-адаптери. Перевантаження діапазону може спричинити перекриття каналів, що, своєю чергою, призводить до втрати сигналу та відеоданих. Якщо додати ще кілька пристроїв, які працюють у цьому ж діапазоні, це може стати критичною проблемою для системи безпеки.

Wi-Fi є універсальною технологією бездротового підключення, що використовує радіочастоти для передачі даних. Ця технологія дозволяє забезпечити високошвидкісне з'єднання без використання кабелів, що робить її популярним рішенням для побудови бездротових мереж.

Wi-Fi є стандартним методом підключення комп'ютерів та інших пристроїв до бездротових мереж. Більшість сучасних комп'ютерів, мобільних пристроїв та ігрових систем підтримують Wi-Fi, що дозволяє їм легко підключатися до маршрутизаторів і взаємодіяти з іншими пристроями в мережі. Для забезпечення доступу до Інтернету сам маршрутизатор повинен бути підключений до мережі через кабельне з'єднання.

Кожен комп'ютер або пристрій, який підключений до мережі, зменшує пропускну здатність, доступну для інших пристроїв, які використовують те саме підключення до Інтернету. Це відбувається через те, що всі ці пристрої ділять одну й ту ж бездротову мережу та підключення до Інтернету від провайдера широкосмугового зв'язку. У цьому випадку вузьким місцем не обов'язково є саме бездротове з'єднання, а скоріше обмеження трафіку або пропускну здатності, яку може передавати маршрутизатор до провайдера послуг широкосмугового зв'язку.

Wi-Fi є стандартом бездротових мереж, тому будь-який пристрій із сертифікованою бездротовою картою Wi-Fi має бути сумісним з будь-якою точкою доступу, що також має сертифікацію Wi-Fi. Однак бездротові маршрутизатори можуть бути налаштовані на роботу лише з певним стандартом 802.11, що може ускладнити спілкування старшого обладнання з маршрутизатором. Наприклад, маршрутизатор 802.11n може бути налаштований на роботу лише з пристроями, які підтримують стандарт 802.11n. У такому випадку пристрої з чіпами 802.11g Wi-Fi не зможуть підключитися до цього маршрутизатора, навіть якщо вони мають сертифікацію Wi-Fi.

Мережі Wi-Fi працюють у неліцензованих радіодіапазонах 2,4 ГГц, із швидкостями передачі даних 11 Мбіт/с для стандарту 802.11b або 54 Мбіт/с для стандарту 802.11a. Порівняльні характеристики стандартів Wi-Fi наведено в табл. 1.1.

Таблиця 1.1 - Порівняльні характеристики стандартів Wi-Fi.

IEEE Standart	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Час створення	1999	1999	2003	2009	2014	2019
Частота	5Ghz	2.4Ghz	2.4Ghz	2.4Ghz & 5Ghz	2.4Ghz & 5Ghz	2.4Ghz & 5Ghz
Максимальна швидкість передачі даних	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Wi-Fi безпроводне відеоспостереження використовує 2,4 ГГц діапазон.

Щоб організувати систему знадобляться:

- роутер;
- ір телекамери з вбудованим Wi-Fi приймально / передавачем, або провідні телекамери, які підключаються до точки доступу для подальшої бездротової передачі даних;
- ноутбук, стаціонарний комп'ютер, або мобільний телефон.

Wi-Fi системи більш надійні, ніж аналогові і можуть застосовуватися в сучасних охоронних системах відеоспостереження. Переваги такої системи є відсутність сигнальних проводів, можливість передачі відео на дуже великі відстані. Недоліками являється дороге обладнання, можливість зникнення, завмирання відеосигналу, обмежена швидкість передачі (обумовлена обмеженою шириною каналу), і найголовніше - необхідність прямої видимості між передавальною і приймальною стороною.

Перевага Bluetooth тільки в тому, що він має найменше енергоспоживання, але підходить тільки в тому випадку, якщо сигнал потрібно передавати в межах об'єкту. Тому використовувати Bluetooth в системах безпеки не завжди оправдано.

Порівняльні характеристики Wi-Fi та Bluetooth наведено в табл. 1.2.

Таблиця 1.2 - Порівняльні характеристики Wi-Fi та Bluetooth

Параметр модуля	Wi-Fi	Bluetooth
Призначення	Місцеві мережі	Bluetooth-з'єднання
Відстань дії	100м	10м
Швидкість передачі даних	до 200 Мбіт/с	723,2 Кбіт / с

Висока швидкість передачі даних, стабільність і захищеність каналу зв'язку для організації бездротового відеоспостереження забезпечує Wi-Fi.

Bluetooth не набув широко застосування в системах безпеки через неспроможність дії на велику відстань та малу швидкість. Враховуючи все вище наведене, для бездротового відеоспостереження краще технологія Wi-Fi.

HD відеоспостереження – це система відеоспостереження з високою роздільною здатністю, що використовує формат Full HD. Такі системи зазвичай використовують стандарт передачі відеосигналів HD-SDI (High-Definition Serial Digital Interface), що дозволяє передавати відео через коаксіальний кабель, який є добре знайомим і широко використовуваним у традиційних системах відеоспостереження.

Стандарт HD-SDI виник у сфері телебачення високої чіткості (HDTV). Він був розроблений і стандартизований Товариством інженерів кіно і

телебачення (SMPTE) для передачі відеопотоку через коаксіальні кабелі. Завдяки своїй здатності забезпечувати високу якість зображення і стабільний сигнал на великих відстанях, HD-SDI швидко знайшов своє застосування не лише в телебаченні, а й у системах охоронного відеоспостереження. Це дозволило отримати якісне зображення без втрат на довгих відстанях передачі, що стало важливою перевагою для систем спостереження за об'єктами. Схему побудови HD системи відеспостереження, зображено на рис 1.3.

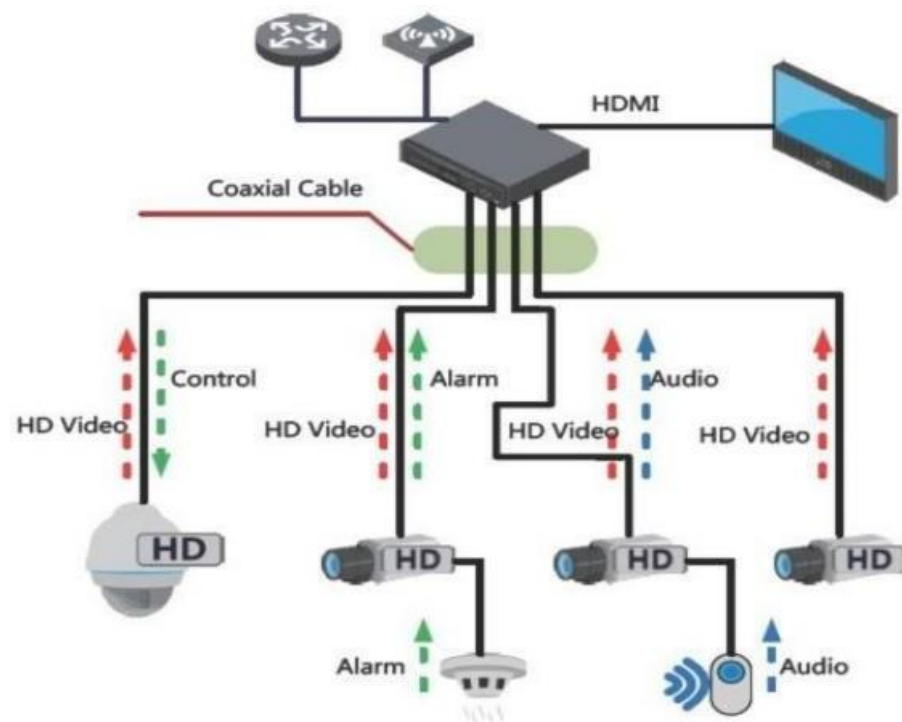


Рисунок 1.3 – Схема побудови HD системи відеспостереження.

У HD відеоспостереженні обробка відеозображення здійснюється за допомогою сучасного кодека H.264, який є одним з варіантів кодека MPEG4. І якщо подивитися на це більш глобально, то як користувачі системи ви можете отримати безперечну перевагу в тому, що з використанням сучасних камер можна охопити на багато більше спостережуваного простору, ніж при використанні аналогових камер відеоспостереження.

Це найбільш очевидно в створенні охоронного відеоспостереження на невеликих об'єктах. Так якщо вам потрібно організувати спостереження в офісі, будинку, невеликому магазині або кафе, то достатньо буде 2-3 камер відеоспостереження, щоб охопити весь об'єкт. Що вже говорити про об'єкти з великою територією, де HD відеоспостереження може в рази зменшити кількість встановлених камер і забезпечити користувачів охоронної системи деталізованим чітким зображенням.

Одним з плюсів дротових відеокамер рис. 1.4 це спостереження є можливість розраховувати на те, що картинка неодмінно надійде в рекордер. Живлення та відео можна отримувати по одному і тому ж кабелю. Немає перешкод від телефонів, Bluetooth, бездротових мереж, мікрохвильових печей, відеонянь або автосигналізацій. Більш широкий вибір стилів відеокамер доступний для використання. Можливість використовувати відеокамеру з зумом, що дозволить мати всього одну камеру, щоб розглянути все навколо. Також є можливість додати звук на вашій системі відеоспостереження без будь-яких серйозних неприємностей. Немає необхідності встановлювати відеокамеру близько до джерела живлення, кабель передасть його куди вам потрібно, звичайно в межах розумного. Є кілька різних типів кабелю, які можна використовувати для підключення до камер. Провідні відеокамери відрізняються тим, що перервати їх роботу набагато важче.

Деякі ускладнення може викликати прокладання кабелів. Наприклад, можливість зіткнутися з бетонними блоками або іншими перешкодами, які спершу не були помічені через приховування їх гіпсокартоном. Якщо прокладати кабель біля високовольтної лінії передач, можливо отримати перешкоди в зображенні відеокамери.

На сьогоднішній день існують аналогові та цифрові дротові камери відеоспостереження. У аналогових систем є кілька переваг. Аналогові системи відмінно вивчені, надійні, відносно дешеві - а тому відмінно підходять для невеликих об'єктів. Сучасні IP-системи, в свою чергу, перевершують аналог за

рахунок високої якості сигналу, більшої гнучкості в питаннях, пов'язаних з переглядом, обробкою і зберіганням відео.



Рисунок 1.4 – Камера ір відеоспостереження.

З практичної точки зору у IP-систем велику кількість переваг:

- якість зображення;
- використання спеціалізованого програмного забезпечення, що дозволяє використовувати такі опції, як облік кількості відвідувачів, відправлення тривожних повідомлень на e-mail, розпізнавання номерів, інтеграція з POS та багато іншого;
- можливість фільтрувати відеопотоки через інтернет;
- масштабованість - легкість додавання нових камер у вже існуючу систему;
- менша вартість інсталяції.

IP-камера це основний пристрій в системі відеоспостереження, а в залежності від системи це може бути єдиний пристрій, і в майбутньому кількість таких систем буде тільки рости. Особливо відрадно, що для того щоб перетворити IP-камеру минулого в IP-камеру майбутнього в деяких випадках буде досить оновити прошивку IP-камери.

IP-камера це цілком собі маленький комп'ютер, в якому, крім ISP-процесора, є центральний процесор керуючий відеокамерою, мережевий інтерфейс, процесор керуючий алгоритмами стиснення відеопотоку, і інші модулі, наприклад, мікрофон або блок для управління тривожними входами

або додаткові відеовиходи. Найважливішою частиною IP- камери є вбудоване програмне забезпечення , зазвичай використовується дуже сильно урізана Linux , на базі якої розгорнуто веб-сервер , він відповідає при зверненні до відеокамери по IP-адресою .

Мережеве IP-відеоспостереження надає неймовірну зручність своїм користувачам. Так різні люди користуються самими різними електронними відео пристроями: телевізорами, комп'ютерами, ноутбуками, планшетами, смартфонами, телефонами, тощо. IP-відеоспостереження через інтернет дозволяє використовувати будь-який з цих пристроїв для перегляду відеозаписів з камери для відеоспостереження. А також користувачі мережі Інтернет використовують для свого комфорту різні WEB браузер. Мережеве відеоспостереження через Інтернет ніяк не обмежує можливість перегляду відеозаписів через будь-який веб-браузер.

Установка ір-відеоспостереження істотно заощаджує витрати користувача на прокладання кабелю, підготовку конструкцій, тощо, так як в більшості сучасних приміщеннях, офісах, будинках і квартирах вже є мережа LAN або ж безпроводна мережа wi-fi. Наявність інтернет мережі дозволяє встановити систему ір відеоспостереження в дуже короткі терміни і без додаткових витрат.

На відміну від кабельних аналогових систем відеоспостереження, де можна отримувати різні перешкоди по проводах, в системах ір відеоспостереження виключена можливість отримувати перешкоди при передачі даних. Так при передачі даних може знижуватися швидкість передачі, але не якість зображення.

Для організації системи відеоспостереження за допомогою IP-камер використовується персональний комп'ютер, який виконує роль відеосервера для налаштування та управління камерами. Живлення і передача даних здійснюються через PoE-комутатор, що дозволяє використовувати лише один кабель Ethernet для підключення кожної камери, значно спрощуючи встановлення системи. IP-камери забезпечують запис і передачу відеоданих у

реальному часі, а роутер надає доступ до інтернету для віддаленого моніторингу та оновлення програмного забезпечення. Блок-схема зображена на рис 1.5.

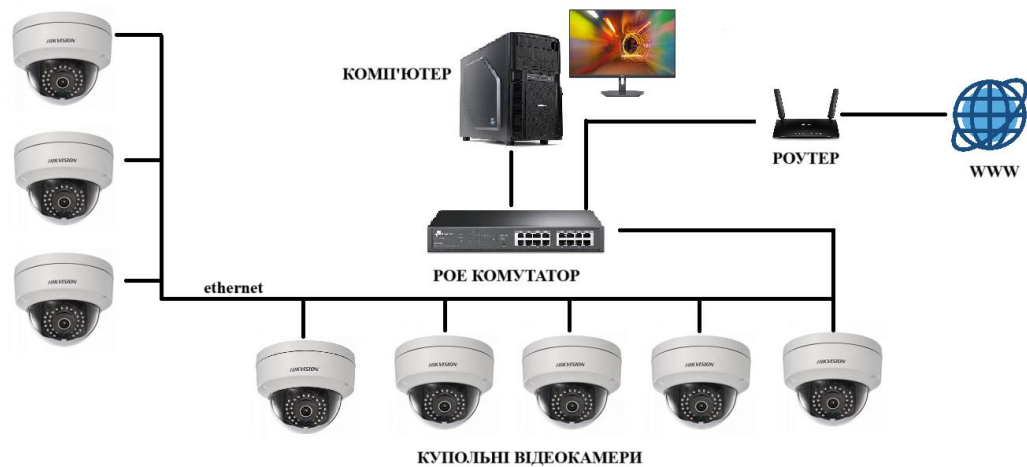


Рисунок 1.5 – Схема побудови відеоспостереження за допомогою ір камер

На рис. 1.6 зображена загальна логічна структура всієї мережі відеоспостереження. Вона розрахована на 8 камер з підтримкою PoE. Для побудови мережі використають 1 комутатор з підтримкою PoE на 16 портів для можливості майбутнього масштабування та інших девайсів та 8 Ір камер.

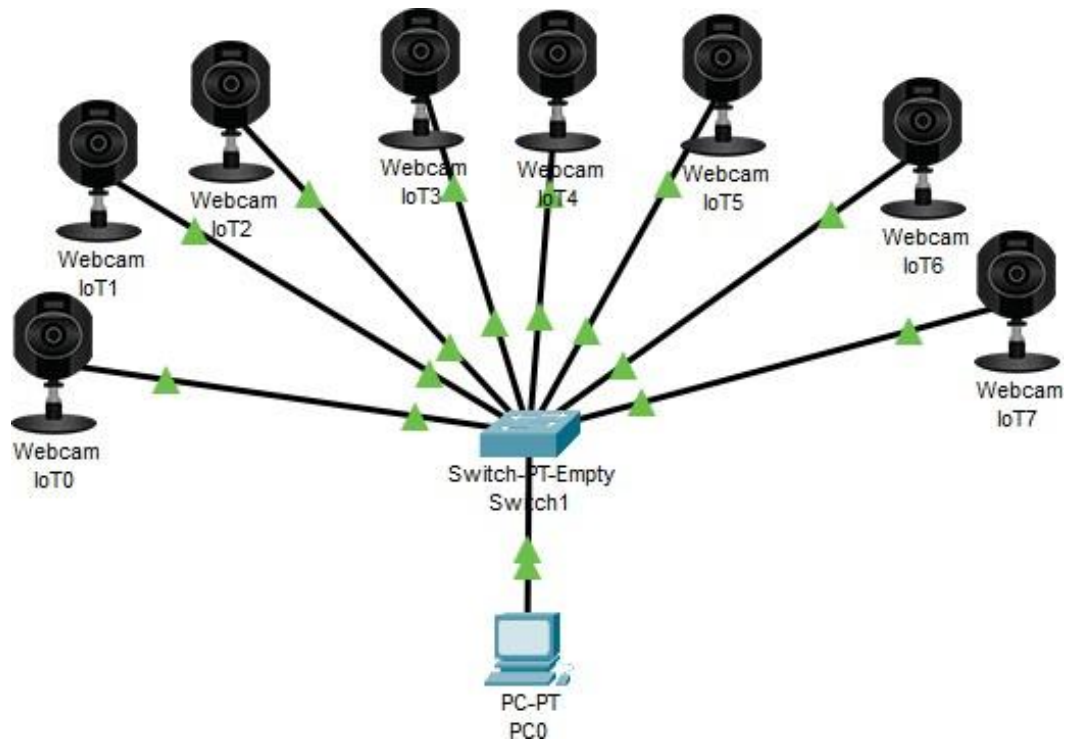


Рисунок 1.6 – Логічна структура мережі відеоспостереження.

1.4 Штучний інтелект та сфери його застосування

Штучний інтелект – це міждисциплінарна наука, яка поєднує в собі знання з кібернетики, програмування, математики, біології та інших галузей. Її метою є створення інтелектуальних систем, здатних виконувати завдання, які традиційно вважалися прерогативою людини, такі як навчання, міркування, прийняття рішень та розв'язання проблем.

Основним принципом штучного інтелекту є використання алгоритмів для аналізу великих обсягів даних. Завдяки цьому алгоритми можуть виявляти приховані закономірності та робити прогнози, що дозволяє приймати обґрунтовані рішення.

Сьогодні штучний інтелект широко використовується у різних сферах, таких як наука, медицина, бізнес, фінанси, транспорт і послуги. Його застосування стало невід'ємною частиною сучасного життя, а розвиток ШІ продовжує стрімко просувати науку і технології вперед.

Штучний інтелект у відеоспостереженні відіграє дедалі важливішу роль. Можна очікувати, що вже за кілька десятиліть усі системи відеоконтролю

будуть тією чи іншою мірою використовувати нові технології машинного навчання. Вони передбачають збір, обробку та аналіз отриманої інформації за заданими алгоритмами. Штучний інтелект (ШІ) — це комп'ютерна програма, яка працює на основі серії алгоритмів і послідовностей. Вона аналізує отриману інформацію, порівнює її з еталоном і робить висновки.[8]

Розглянемо детальніше, які технології штучного інтелекту у відеоспостереженні вже стали реальністю та почали активно використовуватися в системах контролю.

Використання штучного інтелекту перестало здаватися далеким майбутнім: алгоритми машинного навчання починають використовуватися все частіше, що робить камери більш «розумними», точними та корисними для виявлення небезпечних ситуацій. Можна перерахувати кілька технологій ШІ, які стали найбільш затребуваними в системах відеоспостереження.

- Машинне навчання. Штучний інтелект обробляє отримані дані й звіряє їх із заданими зразками. Машинне навчання передбачає запам'ятовування нових даних та їх використання в подальшому аналізі.
- Комп'ютерний зір. ШІ за допомогою камери «бачить» об'єкт, тобто отримує дані про нього та проводить обробку. Він порівнює його з наявними в пам'яті зразками, аналізує схожість і відмінності та на основі цього робить висновок про безпеку явища. Це дозволяє системам безпеки не реагувати на безпечні об'єкти: рух гілок дерев, птахів, вуличних котів тощо. Це зменшує кількість хибних тривог.
- Нейронні мережі та глибоке навчання. Нейромережі з розподіленими потоками даних здатні обробляти величезні масиви інформації. Це дає можливість аналізувати отримані дані з сотень камер одночасно і миттєво розпізнавати події, що відбуваються. Поки машини можуть помилятися, але помилки

трапляються дедалі рідше, а можливості ШІ з кожним роком зростають.

Переваги використання штучного інтелекту у відеоспостереженні. Впровадження технологій обробки даних за допомогою штучного інтелекту відкриває нові перспективи в розвитку систем відеоконтролю. Уже зараз «розумні» камери дедалі менше потребують допомоги живих операторів. Більше не потрібно годинами переглядати зображення на моніторі — система сама «помітить» зміни, відреагує на них і подасть сигнал оператору при виявленні тривожних ознак.

Сфера безпеки. Системи спостереження зі штучним інтелектом контролюють промислові підприємства, міські вулиці, банки, магазини та інші об'єкти. Вони не лише розпізнають стороннє вторгнення, але й можуть заздалегідь проаналізувати поведінку осіб, які вважаються підозрілими через невідповідність заданим алгоритмам;

Транспортна сфера. Камери виявляють порушників правил дорожнього руху, автоматично зчитують номери, а ШІ розпізнає передані дані. Штучний інтелект у відеоспостереженні використовується й іншими способами. Наприклад, у мегаполісах він оцінює завантаженість вулиць і інтенсивність транспортного потоку. Зібрані дані дозволяють керувати світлофорами, щоб розвантажити вулицю або, навпаки, сповільнити рух автомобілів;

Роздрібна торгівля. ШІ в найближчому майбутньому спростить систему оплати. Покупцям більше не доведеться користуватися банківськими картками чи прикладати телефон до терміналу — система буде списувати гроші з банківського рахунку просто на основі сканування обличчя. Система FacePay вже існує і починає впроваджуватися, хоча поки що вона не отримала повсюдного поширення.

Надалі штучний інтелект у відеоспостереженні буде застосовуватися дедалі ширше. Розвиток технологій не зупинити: дуже скоро кожна вулиця буде контролюватися системами збору даних, які оброблятимуть величезні масиви інформації за лічені секунди. Це дозволить контролювати

переміщення, вчасно виявляти порушників і забезпечувати безпеку. Проте питання конфіденційності невдовзі постануть гостріше: буде дуже складно навіть на короткий час вийти з-під контролю.

Однак нові технології незабаром стануть звичною реальністю, нове покоління сприйматиме їх як постійну норму життя. ШІ стане постійним помічником у забезпеченні безпеки й допоможе значно знизити кількість правопорушень.

Сучасний штучний інтелект (ШІ), незважаючи на його великі досягнення та широке використання в різних сферах, має низку вразливостей, які можуть становити загрозу для безпеки, приватності та етичності його використання.

ШІ моделі значною мірою залежать від даних, на яких вони навчаються. Якщо зловмисники мають доступ до навчальних даних, вони можуть їх змінити або пошкодити. Це може призвести до неправильних результатів або небезпечних рішень ШІ. Атака на дані може внести хибні приклади, через які система розпізнавання облич може почати ідентифікувати людей неправильно.

ШІ моделі можуть бути вразливими до спеціально підготовлених даних, які зовні здаються нормальними, але насправді спрямовані на введення в оману системи. Зловмисники можуть змінити дані так, щоб ШІ приймав неправильні рішення. Невелика модифікація зображення може обманути систему розпізнавання об'єктів, змусивши її класифікувати його неправильно.

ШІ часто приймає рішення на основі даних, що можуть містити упередження. Це може призвести до дискримінаційних рішень щодо певних груп населення. Системи розпізнавання облич можуть мати нижчу точність для людей із певними етнічними або гендерними характеристиками, якщо навчальні дані недостатньо репрезентативні.

Якщо модель ШІ "занадто добре" навчається на конкретних даних, вона може втратити здатність до узагальнення нових даних. Це означає, що модель буде ефективною лише на обмеженій кількості завдань, з якими вона вже

стикалась. Система, що навчена розпізнавати певні типи загроз на основі специфічних шаблонів, може не впоратися з новими або трохи зміненими сценаріями.

ІІІ системи можуть збирати й аналізувати великі обсяги особистої інформації, що викликає ризики порушення конфіденційності та зловживання даними. Системи розпізнавання облич можуть використовуватися без згоди людини, що створює загрозу її приватності в громадських місцях або на роботі.

ІІІ системи можуть бути чутливими до змін у навколишньому середовищі або у вхідних даних, через що їх продуктивність може різко погіршитися. Зміна умов освітлення або ракурсу в камерах може вплинути на точність системи розпізнавання облич, що вимагає постійного адаптивного навчання.

Завдяки ІІІ можна створювати реалістичні зображення, відео або аудіо, які використовуються для обману та маніпуляцій громадською думкою. Відео зі зміненою особою публічної особи може бути використане для поширення дезінформації або шантажу.

Для розробки, навчання та функціонування багатьох сучасних ІІІ систем потрібні величезні обчислювальні ресурси. Це робить їх дорогими та залежними від інфраструктури. Високопродуктивні графічні процесори потрібні для навчання глибоких нейронних мереж, що може стати вузьким місцем у розвитку та впровадженні таких систем.[19]

Усі ці вразливості вимагають додаткових досліджень, впровадження нових підходів до безпеки та етики у сфері ІІІ, а також розробки механізмів для зменшення ризиків, пов'язаних із їх використанням.

2 ОГЛЯД ТЕХНОЛОГІЙ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ

2.1 Сучасні уявлення про технології біометричної ідентифікації для контролю та управління доступом

Система контролю та управління доступом (СКУД) – це сукупність спеціалізованого обладнання та програмного забезпечення, призначеного для організації на певній території системи обмеження, реєстрації та контролю доступу людей і транспорту через двері, ворота, контрольно-пропускні пункти тощо.[3]

Біометрична система контролю та управління доступом дозволяє розпізнавати людей за їх фізичними індивідуальними ознаками такими ,як відбитки пальців, як показано на рис. 2.7, або долоні, сітківка райдужної оболонки ока, голос, риси обличчя, ДНК, тощо. Таким чином, якість контролю та безпеки системи значно підвищується, знижується ризик несанкціонованого проникнення та обману системи.

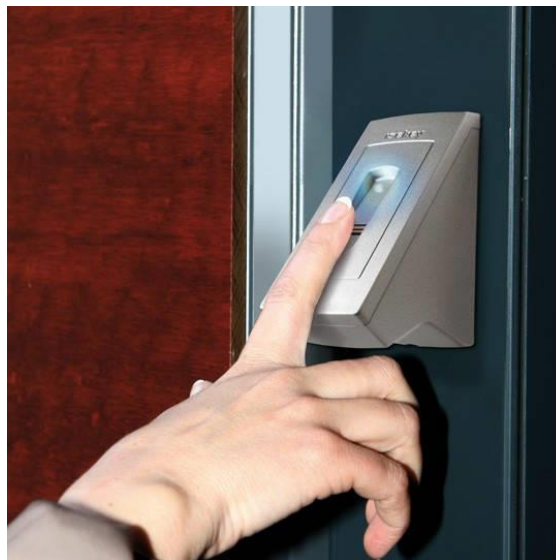


Рисунок 2.1 – Система біометричного контролю доступу, яка використовує відбитки пальців.

На сьогоднішній день біометричні системи контролю доступу є дуже затребуваними серед покупців, що вплинуло на готовність виробників розвивати галузь і технології, розширювати номенклатуру та характеристики обладнання. Сучасні технології дозволяють інтегрувати їх практично в будь-яку діючу систему СКУД. Саме обладнання стало більш функціональним, легшим, компактнішим, зручнішим в експлуатації та доступнішим за вартістю. Кілька років тому встановлення такої системи могли дозволити собі лише великі підприємства, а зараз спектр замовлень розширився від локальних систем до великих мережових структур територіально розподілених об'єктів. Обладнання стало широко використовуватися не лише в банках і особливо контрольованих установах, але й в звичайних офісах, школах, лікарнях, житлових будинках, тощо.

Біометричні системи контролю доступу зручні для користувачів, оскільки носії даних завжди з ними, їх неможливо втратити або вкрати. Біометричний контроль доступу вважається більш надійним, оскільки ідентифікатори не можуть бути передані третім особам чи скопійовані.[17]

2.2 Технології біометричної ідентифікації

Методи біометричної ідентифікації.

Статичні, засновані на фізіологічних ознаках людини, які присутні з нею протягом усього життя:

- ідентифікація за відбитком пальця;
- ідентифікація за обличчям;
- ідентифікація за райдужною оболонкою ока;
- ідентифікація за геометрією руки;
- ідентифікація за термограмою обличчя;
- ідентифікація за ДНК;
- ідентифікація на основі акустичних характеристик вуха;
- ідентифікація за малюнком вен.

Динамічні, засновані на поведінкових характеристиках людей, а саме на підсвідомих рухах під час повторення якоїсь звичної дії такі як почерк, голос, тощо:

- ідентифікація за голосом;
- ідентифікація за рукописним почерком;
- ідентифікація за клавіатурним почерком;
- та інші.

FAR (False Acceptance Rate) – коефіцієнт помилкового допуску, цей показник характеризує ймовірність помилкового прийняття неавторизованої особи як авторизованої. FAR показує, як часто система помилково ідентифікує некоректну особу як правильну. Такий тип помилки є критичним для систем безпеки, оскільки призводить до того, що стороння людина отримує доступ до системи чи об'єкта, на який вона не має права.

FRR (False Rejection Rate) – коефіцієнт помилкового відхилення, цей показник характеризує ймовірність помилкового відхилення авторизованої особи. Іншими словами, FRR показує, як часто система не розпізнає коректну особу та блокує її доступ, навіть якщо вона є правомірним користувачем. Такий тип помилки є неприємним для кінцевого користувача, оскільки створює перешкоди для отримання доступу.[9]

Таблиця 2.1 – Порівняння результативності використання методів біометричної автентифікації.

Методи біометричної автентифікації	FAR	FRR	Фальсифікація	Комфорт користувача	Вартість
Відбиток пальця	0,001%	0,6%	Можлива	Середній	Низька
Розпізнавання обличчя 2D	0,1%	2,5%	Можлива	Середній	Середня
Розпізнавання обличчя 3D	0,0005%	0,1%	Проблематична	Середній	Висока

Радужка ока	0,00001%	0,016%	Неможлива	Високий	Висока
Візерунок вен долоні	0,0008%	0,01%	Неможлива	Середній	Середня

Існують також системи ідентифікації, які поєднують різні біометричні характеристики і можуть задовольнити найсуворіші вимоги до надійності та безпеки систем контролю доступу.

2.2.1 Ідентифікація за допомогою відбитків пальців

Розпізнавання відбитків пальців або дактилоскопія є одним з найбільш популярних на сьогодні методом біометричної ідентифікації особистості. Стимулом для розвитку цієї технології стало її розповсюджене використання в криміналістиці минулого століття. Кожній людині притаманний папілярний візерунок відбитків пальців, який є унікальним, що і дозволяє проводити ідентифікацію. Найчастіше алгоритмами використовуються характерні точки на відбитках пальців, а саме лінії візерунка, окремі точки, розгалуження ліній.

Крім того, збирається інформація щодо морфологічної структури відбитка пальця: відносне розташування замкнених ліній папілярного візерунка, спіральних і аркових ліній. Здійснюється перетворення особливостей папілярного візерунка в певний код, який є унікальним і зберігає інформативність відбитка та зображення. У базі даних, яка використовується для пошуку та порівняння, здійснюється зберігання саме таких кодів відбитків пальців. Величина часу, необхідного для перетворення зображення відбитка пальця в код і проведення його ідентифікації, зазвичай не перевищує однієї секунди та визначається розміром бази. Час, необхідний на піднесення руки, до уваги не береться.

До переваг цього методу можна віднести його високу достовірність, статистичні показники методу вищі, ніж у методів ідентифікації за голосом, розписом, обличчям. Також важливою є досить низька вартість пристроїв, які здійснюють сканування зображення відбитка пальця. Також варто відзначити

простоту процедури сканування відбитка. Однак метод має і свої недоліки, такі як чутливість папілярного візерунка пальця до пошкоджень через дрібні порізи й подряпини. Також практика показує наявність високого ступеня відмов при скануванні на підприємствах, що налічують кілька сотень співробітників. Деякі сканери втрачають адекватність при наявності сухої шкіри, погано ідентифікують людей похилого віку. Крім того, можна сказати про недостатній захист від підробок зображення відбитка, що є наслідком широкого поширення методу.

2.2.2 Ідентифікація за допомогою райдужної оболонки ока

До унікальних характеристик людини можна віднести райдужну оболонку ока, показано на рис 2.2.



Рисунок 2.2 – ідентифікація за допомогою райдужної оболонки ока

Формування візерунка райдужки відбувається на восьмому місяці внутрішньоутробного розвитку, остаточна стабілізація відбувається у віці близько двох років, після чого практично не спостерігається змін протягом життя, окрім тих, які спричинені сильними травмами або різкими патологіями. Цей метод також належить до одного з найбільш точних у біометрії. Систему ідентифікації особистості за райдужною оболонкою можна логічно розділити на дві частини: пристрій захоплення зображення, що здійснює його первинну обробку та передачу контролеру, задача якого полягає у порівнянні

зображення з тими, що зберігаються у базі даних, та передачі команди про доступ виконавчому пристрою. Часовий інтервал, необхідний для первинної обробки зображення, в сучасних системах становить близько 300–500 мс. Швидкість порівняння отриманого зображення з базою даних досягає 50 000–150 000 порівнянь на секунду на типовому персональному комп'ютері. Очевидно, що при такій швидкості порівняння не виникає обмежень щодо використання методу на підприємствах з великою кількістю працівників. Завдяки використанню алгоритмів оптимізації пошуку та спеціалізованих контролерів, з'являється можливість ідентифікувати людину серед жителів цілої країни.

Перевагою цього методу є висока статистична надійність алгоритму. Існує можливість захоплення зображення райдужної оболонки на відстані від кількох сантиметрів до кількох метрів, при цьому немає необхідності у фізичному контакті людини з пристроєм. Також варто зазначити високу захищеність райдужної оболонки від пошкоджень, завдяки чому вона практично не змінюється з часом. До переваг також відноситься можливість використання великої кількості методів, які захищають від підробки.

До недоліків методу можна віднести високу ціну системи, яка перевищує вартість систем, що здійснюють розпізнавання за відбитком пальця або обличчям. Також характерною є досить низька доступність готових рішень.

2.2.3 Ідентифікація за геометрією обличчя.

Наразі розроблено велику кількість методів розпізнавання за геометрією обличчя. Основою всіх цих методів є факт, що форма черепа та риси обличчя у кожної людини унікальні. Для багатьох ця область біометрії є дуже привабливою, оскільки людям властиво впізнавати один одного в першу чергу за обличчям. Цю область можна умовно поділити на два напрями: 2-D розпізнавання та 3-D розпізнавання. Кожен напрям має свої переваги та

недоліки, проте на ступінь застосування того чи іншого методу значно впливають вимоги й область застосування, які пред'являються до конкретного алгоритму.



Рисунок 2.3 – ідентифікація за геометрією обличчя.

Метод 2-D розпізнавання обличчя є одним із найменш ефективних біометричних методів з точки зору статистики. Він був розроблений досить давно і орієнтований переважно на використання в криміналістиці, що і стало основою для його розвитку. Останнім часом були розроблені комп'ютерні інтерпретації методу, що підвищило його надійність, але не можна не відзначити його постійне відставання від інших біометричних методів ідентифікації особистості. Наразі через слабкі статистичні показники сфера його застосування обмежена мультимодальною біометрією та соціальними мережами.

Перевагою методу можна вважати відсутність необхідності у дорогому обладнанні, а також можливість розпізнавання на досить великих відстанях від камери. До недоліків належать низький рівень статистичної надійності, наявність певних вимог до освітлення. Багато алгоритмів не працюють за наявності перешкод, таких як окуляри, борода або деякі елементи зачіски. Також не можна вважати перевагою обов'язкову фронтальну позицію обличчя, яка допускає лише незначні відхилення. Більшість алгоритмів не здатні

враховувати можливі зміни міміки обличчя, іншими словами, передбачається, що вираз обличчя повинен бути нейтральним.

Реалізація методу 3D-розпізнавання обличчя є досить складним завданням. Однак, на сьогоднішній день розроблено велику кількість методів, які виконують 3D-розпізнавання обличчя. Ці методи практично не піддаються порівнянню один з одним, тому що в них застосовуються різні бази даних і сканери, далеко не всі з них видають показники FAR і FRR, і вони засновані на принципово різних підходах. Перехідним від 2D до 3D можна вважати метод, у якому реалізується накопичення інформації про обличчя. Цей метод має кращі характеристики, ніж 2D, проте, подібно до нього, заснований на використанні лише однієї камери. У процесі занесення суб'єкта до бази даних, суб'єкт повертає голову, після чого алгоритм виконує з'єднання зображення в єдине ціле і створення 3D-шаблону. Для розпізнавання використовується кілька кадрів відеопотоку. Цей метод можна віднести до експериментальних, оскільки його готова реалізація поки не зафіксована.

Найбільш класичним можна вважати метод проектування шаблону. Він полягає в тому, що на обличчя проектується сітка. Після цього камерою робляться знімки з частотою в кілька десятків кадрів на секунду, а обробка отриманих зображень здійснюється за допомогою спеціальної програми. Відбувається викривлення променя, що падає на вигнуту поверхню: зі збільшенням кривизни поверхні зростає й викривлення променя. У перших розробках використовувалося джерело видимого світла, яке подавалося через спеціальну сітку. Згодом видиме світло замінили на інфрачервоне, яке має певні переваги. Найчастіше на першому етапі обробки відбувається відсів зображень, на яких або взагалі не видно обличчя, або присутні сторонні предмети, що ускладнюють ідентифікацію. За отриманими знімками здійснюється відновлення 3D-моделі обличчя з виділенням і видаленням непотрібних перешкод наприклад, борода, зачіска, вуса, окуляри. Далі модель аналізується, тобто відбувається виділення антропометричних особливостей, які поміщаються в унікальний код, що заноситься до бази даних. Часовий

інтервал, необхідний для захоплення та обробки зображення, становить 1–2 секунди для найкращих моделей. Останнім часом інтенсивно розвивається метод 3D-розпізнавання за зображенням, отриманим з кількох камер.

До переваг методу 3D-розпізнавання обличчя можна віднести відсутність необхідності в контакті зі сканувальним пристроєм, низьку чутливість до зовнішніх факторів як на самому об'єкті такі як поява бороди, окулярів, зміна зачіски, так і в його оточенні поворот голови, освітленість. Також перевагою є високий рівень надійності, порівнянний з методом ідентифікації за відбитками пальців.

Графічна блок-схема алгоритму розпізнавання обличчя показана на рис 2.4.

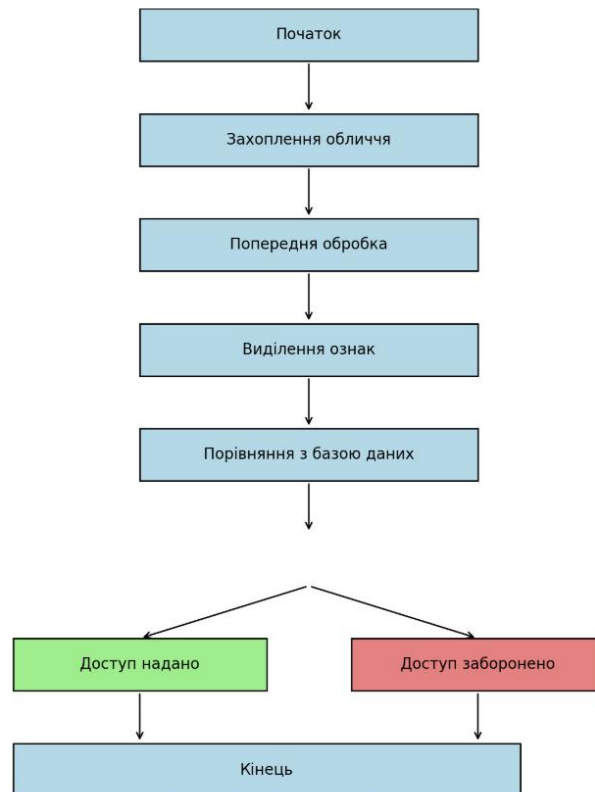


Рисунок 2.4 – блок-схема алгоритму розпізнавання обличчя.

2.2.4 Ідентифікація за малюнком вен

Розпізнавання за малюнком вен в руці є новою технологією в біометричній сфері, її широке застосування почалося менше десяти років

тому. За допомогою інфрачервоної камери робляться знімки зовнішньої або внутрішньої сторони руки. Формування малюнка вен відбувається завдяки поглинанню ІЧ-випромінювання гемоглобіном крові. Внаслідок цього спостерігається зменшення відбиття, що дозволяє побачити вени на камері у вигляді чорних ліній, як показано на рис 2.5. Спеціальна програма, на основі отриманих даних, здійснює формування цифрового відбитка. Немає необхідності в контакті людини зі сканером. Цю технологію можна порівняти за надійністю з розпізнаванням за райдужною оболонкою ока: в чомусь вона перевершує цей метод, а в чомусь поступається.



Рисунок 2.5 – Розпізнавання за малюнком вен в руці.

Цей метод має низку переваг: відсутність необхідності в контакті зі сканером, висока ступінь достовірності. Існують також свої недоліки: неприпустимість засвітлення сканера сонячними променями або променями, що випромінюються галогеновими лампами. Окрім цього, через наявність деяких вікових захворювань, наприклад, артриту, значно погіршуються показники FAR і FRR. Цей метод ще недостатньо вивчений порівняно з іншими статистичними біометричними методами.

2.3 Допоміжне обладнання для системи біометричного контролю доступу

Окрім основних компонентів, таких як біометричні сканери (розпізнавання обличчя, відбитків пальців, райдужної оболонки ока або вен руки), для ефективної роботи системи біометричного контролю доступу важливим є допоміжне обладнання, яке забезпечує інтеграцію, функціональність і підвищує рівень надійності системи.

Контролери доступу є центральними елементами будь-якої системи біометричного контролю доступу. Їх основна функція полягає в обробці та прийнятті рішень на основі отриманих сигналів від біометричних зчитувачів, які сканують обличчя, відбитки пальців, райдужну оболонку ока, або інші біометричні дані користувачів. Контролери визначають, чи надати доступ користувачу на основі зіставлення його даних із заздалегідь збереженими шаблонами у базі даних. Крім цього, контролери можуть виконувати додаткові функції, такі як зберігання журналу подій, інтеграція з іншими системами безпеки та управління часом роботи персоналу.

Контролери доступу можуть бути інтегровані з іншими системами безпеки або управління, що дозволяє створити комплексну систему контролю і моніторингу на об'єкті. Інтеграція з камерами дозволяє записувати події доступу та забезпечувати візуальне підтвердження.

Контролери можуть відслідковувати робочий час співробітників, що дозволяє інтегрувати систему доступу з програмами для управління персоналом.

В екстрених ситуаціях, як приклад пожежа, контролери можуть автоматично розблоковувати всі двері для забезпечення безпечної евакуації.

Сервери та мережеве обладнання, як показано на рис 2.6. є ключовими компонентами у системах біометричного контролю доступу, особливо для великих об'єктів з високими вимогами до безпеки. Вони забезпечують централізоване управління всіма процесами в системі, зберігання даних та

надійний зв'язок між усіма компонентами системи, від біометричних зчитувачів до контролерів доступу.



Рисунок 2.6 – Сервери та мережеве обладнання

Сервери виконують важливі функції, пов'язані зі зберіганням, обробкою та управлінням біометричними даними, а також забезпечують централізоване керування всією системою БКД. Сервери у таких системах можуть бути як локальними, так і розміщеними у хмарі, залежно від потреб конкретного об'єкта.

Сервери зберігають шаблони біометричних даних користувачів, такі як зображення обличчя, відбитки пальців або інші біометричні параметри. Також вони отримують інформацію від зчитувачів і контролерів, перевіряють її відповідність даним у базі і приймає рішення про надання доступу. Сервери фіксують усі події в системі, хто і коли отримав доступ, які були спроби несанкціонованого доступу тощо. Ці дані можуть бути використані для аналізу і створення звітів. Для забезпечення безперебійної роботи та безпеки даних сервери можуть підтримувати функції резервного копіювання (бекапів), що гарантує збереження даних навіть у випадку збою системи.

Для забезпечення стабільної роботи системи БКД потрібне надійне мережеве обладнання, яке з'єднує всі елементи системи такі як зчитувачі, контролери, сервери, робочі станції адміністратора, відеокамери тощо. Воно

забезпечує обмін даними між всіма компонентами в режимі реального часу, підтримуючи високу продуктивність та безперебійну роботу системи.

Сервери та мережеве обладнання є основою для побудови масштабованих, надійних і безпечних систем біометричного контролю доступу. Від правильного налаштування серверної інфраструктури, захищеної мережевої архітектури та використання сучасного мережевого обладнання залежить ефективність системи в цілому. Обираючи компоненти для системи БКД, важливо забезпечити не лише продуктивність, але й високий рівень безпеки, надійності та можливості масштабування для майбутніх потреб.

Датчики руху, турнікети та шлагбауми є важливими компонентами системи фізичного контролю доступу, що працюють у поєднанні з біометричними зчитувачами, контролерами доступу та іншими елементами безпеки. Ці пристрої допомагають ефективно контролювати вхід і вихід, а також реагувати на несанкціоновані дії.

Датчики руху, які показано на рис 2.7, використовуються для виявлення присутності або руху людей у зоні контролю доступу. Вони можуть бути інтегровані в системи безпеки для автоматичного відкриття дверей, включення світла або виклику охорони в разі несанкціонованих дій.



Рисунок 2.7 – Різні за типом датчики руху

Є декілька типів датчиків руху. Інфрачервоні це найпоширеніший тип датчиків, який реагує на теплове випромінювання від людського тіла. Вони фіксують зміни в теплових сигналах у зоні дії, що дозволяє виявити присутність людини.

Ультразвукові датчики використовують високочастотні звукові хвилі для виявлення руху. Вони випромінюють хвилі та фіксують їх відбиття від об'єктів. Якщо об'єкт переміщується, зміна частоти сигналу (ефект Доплера) свідчить про рух.

Мікрохвильові датчики працюють на основі радіохвиль і можуть фіксувати навіть найменші рухи на великій відстані. Вони мають більший діапазон дії, ніж ІЧ-датчики, але можуть бути чутливішими до сторонніх перешкод.

Комбіновані датчики поєднують кілька технологій, наприклад, інфрачервоні та ультразвукові. Це підвищує їх точність та зменшує кількість помилкових спрацьовувань.

Турнікети є механічними пристроями для контролю доступу, які обмежують рух людей в певні зони і дозволяють проходити тільки після відповідної аутентифікації за допомогою біометрії або карт доступу. Турнікети встановлюються у місцях з високим трафіком людей, таких як офісні будівлі, стадіони, вокзали та інші об'єкти.

Є декілька видів турнікетів такі як: триподи, роторні, флєп турнікети, оптичні турнікети. Деякі з них показано на рис 2.8.



Рисунок 2.8 – Триподи та флєп турнікети.

Триподи це класичні турнікети з трьома рухомими планками. Вони дозволяють проходити по одній особі після успішної ідентифікації. Такі турнікети використовуються в місцях з середнім або високим потоком людей і забезпечують надійний фізичний контроль доступу.

Роторні турнікети складаються з кількох обертових ступок, які обмежують доступ до приміщень. Вони можуть бути високого або низького рівня, залежно від потреб об'єкта.

Флеп-турнікети використовують автоматичні стулки, що відкриваються горизонтально при наданні доступу. Вони пропускають людей швидше, ніж традиційні триподи, і більше підходять для об'єктів з великим потоком людей.

Оптичні турнікети забезпечують безконтактний контроль доступу, використовуючи світлові або інфрачервоні бар'єри для виявлення несанкціонованих проходів. Вони не мають фізичних бар'єрів, але можуть спрацьовувати на сигнал тривоги при виявленні порушень.

Турнікети можуть бути легко інтегровані з системами біометричного контролю доступу. Після успішної аутентифікації за допомогою зчитувача відбитків пальців, обличчя або райдужної оболонки, турнікет відкривається і дозволяє доступ. Турнікети також можуть бути пов'язані з камерами відеоспостереження та датчиками руху для підвищення рівня безпеки.

Шлагбауми використовуються для контролю в'їзду та виїзду транспортних засобів на територію. Вони широко застосовуються на паркувальних майданчиках, промислових підприємствах, у житлових комплексах та інших об'єктах, де потрібен контроль над переміщенням автомобілів.

Шлагбауми відкриваються після ідентифікації автомобіля або водія за допомогою картки доступу, систем розпізнавання номерів або біометричних систем. Вони допомагають контролювати інтенсивність руху транспортних засобів, що особливо важливо на територіях з обмеженим доступом або в умовах високого трафіку. шлагбауми обмежують доступ несанкціонованим транспортним засобам, запобігаючи несанкціонованим в'їздам на територію.

Датчики руху, турнікети та шлагбауми є важливими компонентами систем контролю доступу, що забезпечують ефективне управління доступом до об'єктів і територій, підвищують рівень безпеки та допомагають контролювати потік людей і транспортних засобів

Допоміжне обладнання є критично важливим елементом для успішної роботи систем біометричного контролю доступу. Від правильного підбору і налаштування всіх компонентів залежить загальна ефективність, надійність і безпека системи. Інтеграція різноманітного обладнання, починаючи від контролерів і електронних замків до серверів та відеоспостереження, створює комплексний захист для об'єктів і дозволяє забезпечити високий рівень безпеки в різних умовах експлуатації.

Для організації системи контролю доступу за допомогою терміналу розпізнавання облич використовується персональний комп'ютер, який виконує роль сервера для налаштування та управління терміналом і турнікетом. Комутатор забезпечує з'єднання між сервером, терміналом розпізнавання облич і турнікетом, виступаючи ключовим елементом мережевої інфраструктури. Роутер підключає систему до інтернету, що дозволяє оновлювати програмне забезпечення та синхронізувати дані. Термінал розпізнавання облич ідентифікує користувачів, надаючи або забороняючи доступ, а турнікет забезпечує фізичний контроль доступу відповідно до результатів ідентифікації. Блок-схема зображена на рис 2.9.

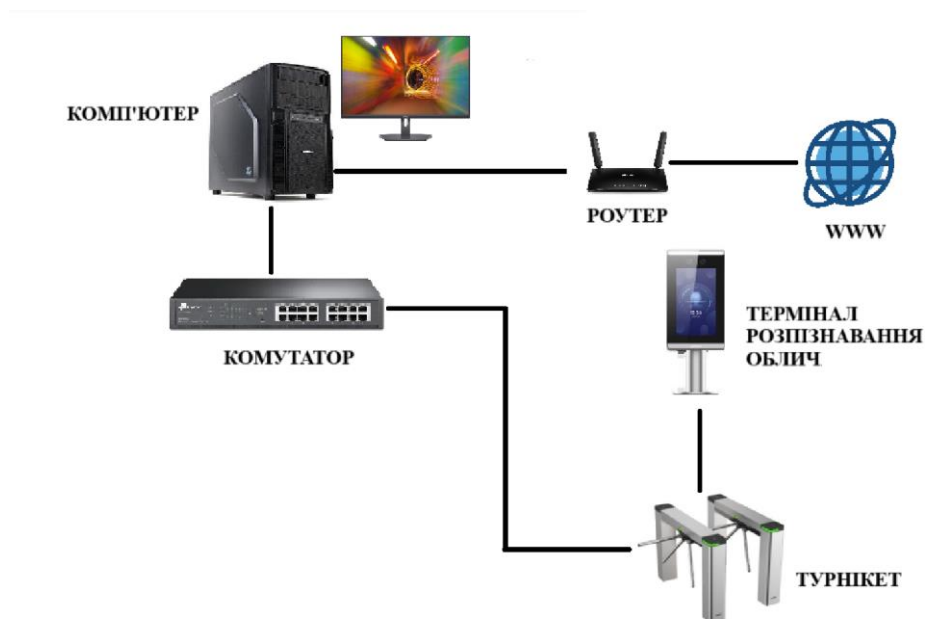


Рисунок 2.9 – Схема побудови системи контролю доступу з використанням терміналу розпізнавання обличчя

3 ПЕРЕЛІК СУЧАСНИХ ІНФОРМАЦІЙНО-НАВЧАЛЬНИХ СЕРЕДОВИЩ

3.1 Поняття інформаційно-навчальне середовище та огляд існуючих платформ

Інформаційно-навчальне середовище можна визначити як програмно-телекомунікаційне середовище, засноване на використанні комп'ютерної техніки, яке реалізує якісне інформаційне забезпечення школярів, педагогів, батьків, адміністрації навчального закладу та громадськості єдиними технологічними засобами та взаємопов'язаним змістовним наповненням. Таке середовище має включати організаційно-методичні засоби, сукупність технічних і програмних засобів для зберігання, обробки, передачі інформації, що забезпечують оперативний доступ до педагогічно значущої інформації і створюють можливість для спілкування педагогів і тих, хто навчається.[5]

Огляд сучасних інформаційно навчальних платформ які об'єднують технології, що забезпечують навчання, обмін знаннями і комунікацію для всіх учасників освітнього процесу.

Google Classroom — це безкоштовна платформа, орієнтована на викладачів і учнів для організації навчального процесу та виконання завдань онлайн. Цей сервіс для дистанційного навчання був створений ще у 2014 році, на сьогодні його функціонал став дуже актуальним та затребуваним. Classroom є поєднанням кількох сервісів Google, адаптованих для освітніх потреб. Інтерфес показано на рис 3.1.

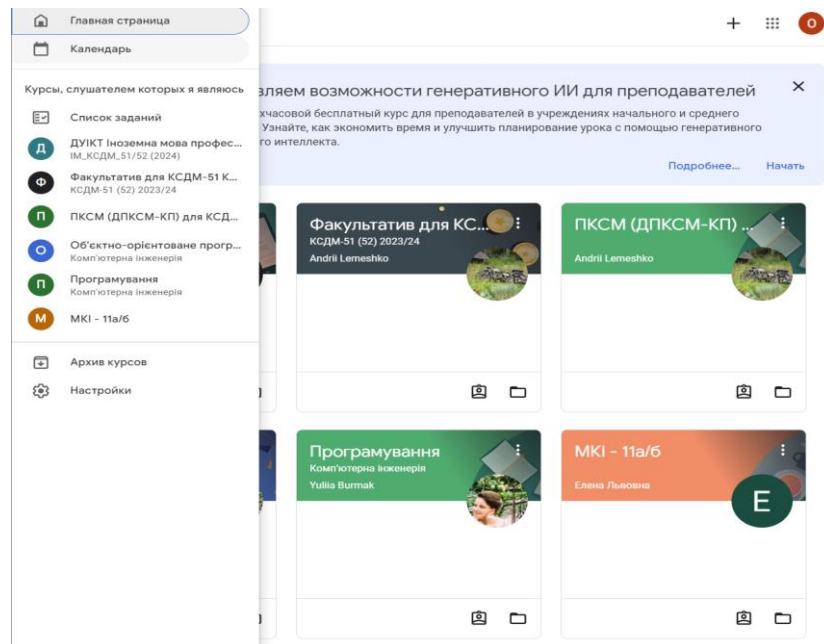


Рисунок 3.1 – Інтерфейс Google Classroom

У Classroom учитель може створити власний віртуальний клас і окремі курси, яким присвоюються унікальні посилання, за якими можуть приєднуватися учні. На сторінці кожного курсу вчитель може публікувати навчальні матеріали, проводити опитування, тести та створювати тематичні завдання.

До кожного завдання можна встановити термін виконання, а вчитель у режимі реального часу може спостерігати за тим, як учні виконують завдання, бачити список зданих і незданих робіт та виставляти учням оцінки.

Вчитель може публікувати оголошення в стрічці класу, додавати текстові нотатки, фото, відео з YouTube, спілкуватися з учнями в чаті. Учні можуть бачити список завдань курсу, які вже виконані і які ще потрібно

виконати. При цьому кожному учню вчитель може дати індивідуальне завдання, яке не побачать інші.

Microsoft Teams — це цифровий центр, що об'єднує чати, зустрічі, файли та додатки в одному місці. Оскільки він базується на Microsoft 365, навчальні заклади отримують переваги від інтеграції з відомими додатками та службами Office.

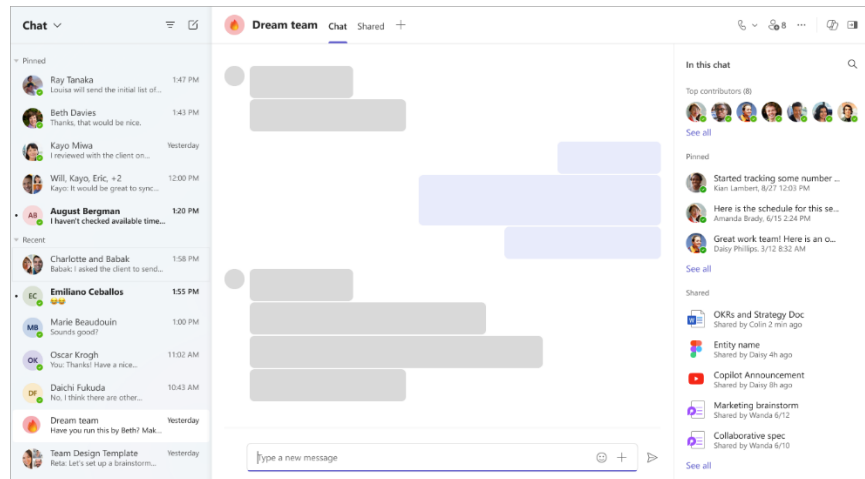


Рисунок 3.2 – Microsoft Teams

Він забезпечує безпеку та відповідність корпоративного рівня, з можливістю розширення та налаштування відповідно до потреб кожного навчального закладу.

За допомогою Microsoft Teams можливо:

- Створювати аудиторії для співпраці.
- Спілкуватися у професійних навчальних спільнотах.
- Спілкуватися з працівниками навчального закладу.
- Координувати дослідження в різних установах.
- Легко підтримувати студентське життя, як-от клуби або позакласні заходи.

Це середовище дозволяє викладачам, студентам та адміністрації закладу взаємодіяти як під час очного навчання, так і в умовах дистанційного або змішаного навчання.

Edmodo це платформа для навчання, яка поєднує елементи соціальної мережі та інструментів для освіти. Вона створена для допомоги викладачам в організації навчального процесу, комунікації з учнями та надання доступу до навчальних матеріалів у безпечному онлайн-середовищі.

Викладачі можуть створювати окремі класи для кожного курсу, запрошувати учнів за допомогою спеціальних кодів і налаштовувати доступ до матеріалів.

Платформа дозволяє легко завантажувати та ділитися різними файлами, презентаціями, документами, зображеннями, відео тощо. Усі матеріали зберігаються в хмарі, що дає можливість учням доступатися до них у будь-який час.

Інтерфейс Edmodo, який показано на рис 3.3, нагадує соцмережу, тому тут передбачені функції для повідомлень, коментарів та обговорень. Це полегшує комунікацію між учасниками навчального процесу та сприяє обміну знаннями та ідеями.

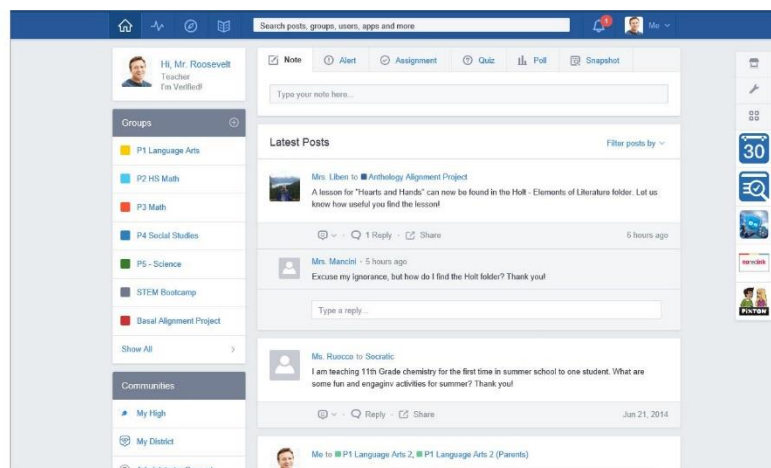


Рисунок 3.3 – Інтерфейс Edmodo

Edmodo підходить для шкіл, де важлива ефективна комунікація, організація навчального процесу та інтерактивність, і дозволяє створити активне навчальне середовище для викладачів, учнів та батьків.

Moodle (Modular Object-Oriented Dynamic Learning Environment) це популярна система управління навчанням (Learning Management System, LMS), яка широко використовується в освітніх установах для організації навчального процесу. Moodle є платформою з відкритим кодом, що дозволяє її легко адаптувати до різних навчальних потреб, інтегрувати з іншими системами і налаштовувати функціонал відповідно до вимог конкретного закладу або курсу.

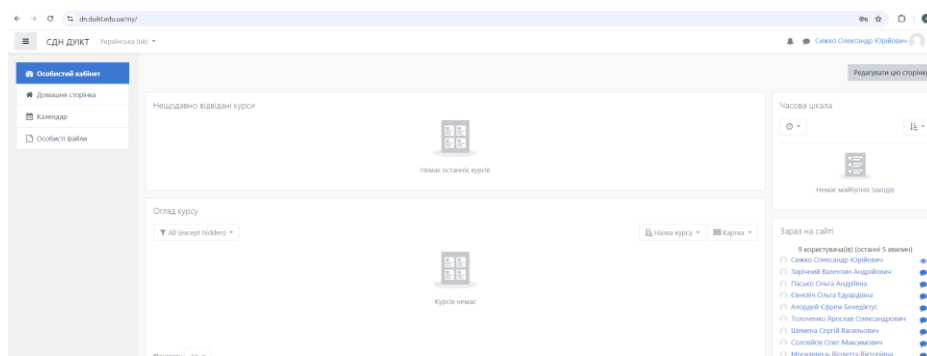


Рисунок 3.4 – Інтерфейс Moodle

Moodle це безкоштовна система електронного навчання. Важливу роль у системі відіграють плагіни, які допомагають змінювати дизайн і розширювати функціональні можливості системи. Плагіни розробляють учасники спільноти Moodle. Зараз їх налічується близько 1500, і більшість з них безкоштовні.[6]

Викладачі можуть створювати курси, завантажувати навчальні матеріали, такі як лекції, презентації, відео, документи, а також налаштовувати доступ до них. Курси можуть бути організовані за темами, тижнями, модулями або іншим способом, що відповідає навчальній програмі.

Moodle включає інструменти для проведення тестів, вікторин, опитувань та іншого формального і неформального оцінювання. Система автоматичного оцінювання дозволяє швидко отримувати результати тестів і надає індивідуальний зворотний зв'язок. Підтримує різноманітні види питань:

з вибором однієї чи кількох відповідей, правильні та неправильні твердження, відповідності, короткі відповіді та інші.

Кожен студент може відстежувати власний прогрес, бачити виконані завдання, оцінки та коментарі від викладача. Викладачі також мають доступ до звітів і можуть бачити активність студентів на платформі, що допомагає в моніторингу успішності.

Викладачі можуть налаштовувати зовнішній вигляд курсів, додавати опитування, таймери, віджет зворотного зв'язку, інтерактивні завдання тощо. Moodle можна налаштувати під потреби кожного навчального закладу або курсу, додаючи або відключаючи різні функції.

Moodle доступний як на комп'ютерах, так і на мобільних пристроях та, що робить навчання доступним у будь-якому місці і в будь-який час.

Moodle часто використовується у вищих навчальних закладах, школах та компаніях для створення індивідуальних і колективних курсів, а також у професійному навчанні.

3.2 Обладнання для організації інформаційно навчального середовища

Для організації інформаційно-навчального сервера у навчальному закладі, який забезпечуватиме ефективне управління курсами, доступ до навчальних матеріалів та взаємодію між студентами та викладачами, потрібне відповідне серверне обладнання. Це включає як апаратне, так і програмне забезпечення.

Основне це серверний комп'ютер або серверна платформа з достатньою продуктивністю. Бажано використовувати багатоядерний процесор (мінімум 4 ядра, краще 8-16) для обробки великої кількості запитів одночасно. Також Рекомендується мінімум 16 ГБ для невеликих закладів (до 100 користувачів) та від 32 ГБ для середніх і великих закладів (до 500 і більше користувачів). Накопичувач SSD об'ємом від 500 ГБ до 2 ТБ залежно від обсягу навчальних матеріалів. Високошвидкісна мережева карта для стабільного підключення.

Важливо мати зовнішній жорсткий диск або окремий сервер для зберігання резервних копій даних та джерело безперебійного живлення необхідне для захисту сервера від раптових відключень електроенергії та втрати даних, що дуже актуально зважаючи на ситуацію в країні.

Для розгортання інформаційно-навчального сервера у навчальному закладі важливо вибрати відповідне програмне забезпечення (ПЗ), яке забезпечить ефективне управління навчальними процесами, безпеку даних та зручний інтерфейс для користувачів. Операційна система на сервері повинна бути стабільною, безпечною та добре підтримуваною для освітніх цілей. Найчастіше використовують Linux або Windows.[22]

LMS це ядро інформаційно-навчального середовища, яке дозволяє організувати курси, тестування, контроль успішності тощо.

Moodle безкоштовна та відкрита LMS, яка надає великий набір функцій для управління курсами, тестуванням, завданнями, комунікацією та аналізом навчального процесу.

Для створення інформаційно-навчального середовища необхідна база даних. База даних зберігає інформацію про користувачів, курси, оцінки, файли тощо. MySQL це популярна система управління реляційними базами даних (СУБД) з відкритим кодом, що використовується для зберігання та управління великими обсягами структурованих даних. Вона підтримує мову SQL (Structured Query Language), яка дозволяє створювати, змінювати, маніпулювати та отримувати доступ до даних у базах.

MySQL є популярним вибором для вебдодатків та інформаційних систем, таких як Moodle, WordPress та інші платформи, де потрібна стабільна й ефективна робота з базами даних.

Необхідний вебсервер який дозволяє користувачам отримувати доступ до веб-інтерфейсу LMS через інтернет чи локальну мережу.

Apache найбільш популярний вебсервер для платформ Moodle та Canvas. Він сумісний із більшістю операційних систем і добре працює з PHP. Проєкт Apache HTTP Server це зусилля з розробки та підтримки HTTP-сервера з

відкритим кодом для сучасних операційних систем, включаючи UNIX та Windows. Метою цього проекту є надання безпечного, ефективного та розширюваного сервера, який надає HTTP-послуги відповідно до сучасних стандартів HTTP.[15]

Комплекс цих програмних і технічних рішень дозволяє створити стабільне і багатофункціональне середовище для дистанційного та гібридного навчання, яке може бути легко налаштоване під специфічні потреби і інтегроване у локальну мережу навчального закладу.

4 ПІДБІР КОМПЛЕКТУЮЧИХ ТА НАЛАШТУВАННЯ СИСТЕМИ

4.1 Підбір компонентів комплексної системи контролю доступу та відеоспостереження

Мій вибір камери Hikvision DS-2CD2143G0-IS, яка зображена на рис 4.1, обумовлений її надійністю та високою якістю, підтвердженою роками досвіду компанії Hikvision на світовому ринку. Камера є частиною продукції одного з найвідоміших і впізнаваних брендів у сфері відеоспостереження, що забезпечує додаткову впевненість у якості обладнання. Важливою перевагою є підтримка виробника у вигляді офіційного програмного забезпечення, яке дозволяє легко налаштовувати й керувати пристроєм, а також забезпечує регулярні оновлення для покращення функціоналу та безпеки системи.



Рисунок 4.1 – IP камера Hikvision DS-2CD2143G0-IS.

Камера демонструє відмінну сумісність з іншою продукцією бренду Hikvision, що дозволяє інтегрувати її у вже наявні системи без необхідності використання додаткових перехідників чи сторонніх рішень. Це робить систему відеоспостереження максимально зручною та ефективною для масштабування.

Hikvision DS-2CD2143G0-IS - купольна чотирьох мегапіксельна IP-камера. Підходить для використання як в приміщенні, так і на вулиці. Зображення чітко вибудовується за допомогою регулювання об'єктива і поліпшується за допомогою функцій цифрового покращення зображення і апаратного WDR. Карта пам'яті на 128 гігабайт і підтримка кодека H.265 + дозволяє зберігати записи прямо на камері, що робить її привабливішою для домашнього використання.[4] Камера антивандальна, захищена від води за стандартом IP67, а від вандалів - за стандартом IK10. Детальні характеристики IP-камери наведено в табл. 4.1.

Таблиця 4.1 - Детальні характеристики Hikvision DS-2CD2143G0-IS.

Тип підключення	дротове
Розширення відео	2560 x 1440
Тип сенсора	1/3 "Progressive Scan CMOS
Розширення	4 Мп
Дальність ІК підсвічування	30 м
Джерело живлення	DC 12В ± 25%
Напруга	12 ВС, 25%, PoE (802.3af)
Формат запису відео	H.264 / H.265 / MJPEG
Підсвічування	інфрачервоне
Клас захищеності	IP67
Підтримка мережевих протоколів	TCP / IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS та інш.
Формат запису аудіо	PCM
Зовнішні порти і роз'єми	1 RJ45
Підтримка карт пам'яті	Micro SD (SD / SDHC / SDXC) до 128Гб

Для виконання ролі відеореєстратора та управління системою контролю доступу достатньо потужності середнього ПК, його головна задача працювати 24 години на добу, і мати жорсткий диск великого об'єму рекомендований для систем відеоспостереження, моя збірка дозволить працювати на комп'ютері, як для виконання простих офісних задач в той час як він використовується для керування системою відеоспостереження та системою контролю доступу.

В ролі процесора підійде AMD Ryzen 5 5600G, це процесор 5000 лінійки для персональних комп'ютерів, який зображено на рис. 4.2, Процесори цього типу чудово підходять для створення продуктивних і універсальних робочих комп'ютерів, де немає потреби у використанні дискретної відеокарти. AMD Ryzen 5 5600G виготовлений за сучасним 7-нм техпроцесом, що забезпечує не лише підвищену продуктивність, а й знижене тепловиділення. Процесор має 6 ядер і 12 потоків, базова тактова частота становить 3,9 ГГц, а в режимі

автоматичного прискорення досягає 4,4 ГГц. Інтегрована графічна система Radeon Vega 7, що оснащена 7 ядрами, працює на частоті до 1900 МГц. У комплекті постачання передбачено фірмову систему охолодження Wraith Stealth, що забезпечує ефективне відведення тепла.



Рисунок 4.2 – Процесор AMD Ryzen 5 5600G
(<https://hotline.ua/ua/computer-processor/amd-ryzen-5-5600g-100-100000252box/#gallery>)

Детальні характеристики процесора наведено в табл. 4.2.

Таблиця 4.3 – характеристики AMD Ryzen 5 5600G

Модель	AMD Ryzen 5 5600G
Архітектура	Zen 3
Техпроцес	7 нм
Кількість ядер/потоків	6 ядер / 12 потоків
Базова частота	3.9 ГГц
Турбо-частота	До 4.4 ГГц
Кеш L2	3 МБ
Кеш L3	16 МБ
Інтегроване графічне ядро	AMD Radeon Vega 7

Графічна частота	1900 МГц
Роз'єм (Socket)	AM4
Підтримка пам'яті	DDR4-3200
Рівень TDP	65 Вт
Максимальна температура	95°C

В ролі материнської плати підійде бюджетне рішення ASUS PRIME A520M-R це материнська плата форм-фактора Micro-ATX, яка зображена на рис. 4.3, створена для побудови продуктивних, надійних і доступних систем на базі процесорів AMD Ryzen. Вона ідеально підходить для офісного використання, домашніх комп'ютерів і невеликих геймерських ПК. Завдяки чіпсету A520, плата підтримує ключові функції сучасних процесорів, забезпечуючи стабільність і довговічність.



Рисунок 4.3 – материнська плата ASUS PRIME A520M-R

Материнка пропонує базові можливості для підключення периферії, має підтримку високошвидкісної оперативної пам'яті та надає все необхідне для стабільної роботи системи. Використання інженерних рішень ASUS, таких як

захист від перенапруги, якісна схема живлення, гарантує довговічність і надійність.

Детальні характеристики процесора наведено в табл. 4.3.

Таблиця 4.3 – характеристики ASUS PRIME A520M-R

Модель	ASUS PRIME A520M-R
Форм-фактор	Micro-ATX
Чіпсет	AMD A520
Процесорний роз'єм	AM4
Підтримка процесорів	AMD Ryzen 3000/5000 серій
Слоти оперативної пам'яті	2 x DDR4
Максимальний обсяг RAM	64 ГБ
Роз'єми для накопичувачів	4 x SATA III, 1 x M.2 (PCIe 3.0 x4, NVMe)
Слоти розширення	1 x PCIe 3.0 x16, 1 x PCIe 3.0 x1
Аудіосистема	7.1-канальний HD Audio (Realtek ALC887)
Мережа	Realtek RTL8111H (Gigabit Ethernet)
Роз'єми на задній панелі	4 x USB 3.2 Gen 1, 2 x USB 2.0, HDMI, D-Sub

Для стабільної роботи комп'ютера потрібно 16 гб оперативної пам'яті DDR4 двома планками по 8 гб для активації двухканального режиму роботи. Я вибрав рішення від компанії Crucial модель DDR4 2666 MHz Ballistix Black, яку зображено на рис. 4.4.



Рисунок 4.4 – Оперативна пам'ять Crucial DDR4 2666 MHz Ballistix Black.

Детальні характеристики оперативної пам'яті наведено в табл. 4.4.

Таблиця 4.4 – характеристики Crucial DDR4 2666 MHz Ballistix Black

Виробник	Crucial
Обсяг, ГБ	16
Кількість планок в комплекті	2
Тип	DDR4
Стандарт	PC4-21300
Ефективна частота, МГц	2666
Штатні таймінги	CL16
Робоча напруга, В	1.2
Радіатори	є
Підтримка XMP	+ (XMP 2.0)
Перевірка і корекція помилок (ECC)	non-ECC
Формфактор пам'яті	288-pin DIMM
Серія	Ballistix

Один з найважливіших компонентів системи відеоспостереження є сховище даних, для цього я вибрав спеціальну серію жорстких дисків високої ємності WD Purple на 8 тб, який зображено на рис. 3.5. WD Purple 8 TB - жорсткий диск високого обсягу, який спеціально спроектований для використання в системах відеоспостереження. Він призначений для безперервної цілодобової роботи з камерами і відеореєстраторами при підвищених температурах, тому забезпечує високу надійність і довговічність. При робочому навантаженні до 180 ТБ / рік і підтримки до 64 камер накопичувачі WD Purple є оптимальним вибором для систем спостереження.

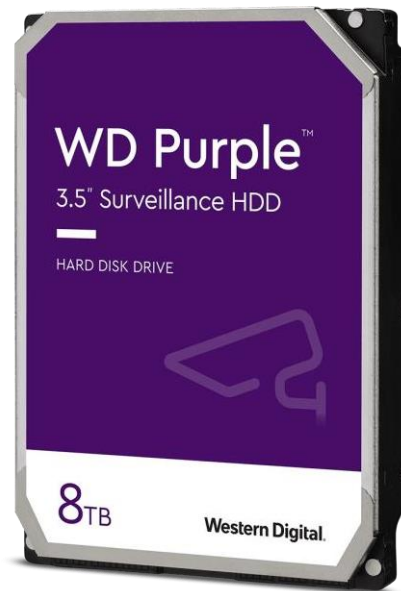


Рисунок 4.5 – Жорсткий диск WD Purple на 8 тб.

Диски WD Purple ємністю 8 ТБ, 10 ТБ, 12 ТБ, 14ТБ і 18ТБ підтримують аналітичні системи з технологією глибокого навчання, що дозволяє працювати з мережевими відеореєстраторами, що володіють можливостями штучного інтелекту. Вони мають збільшений об'єм робочого навантаження до 360 ТБ в рік і до 16 каналів, виділених для аналітичних даних системи штучного інтелекту.

Можливі, пропущені кадри і втрата записів можуть мати серйозні наслідки, якщо через них ви пропустите потрібний момент. У всіх дисках WD Purple реалізована технологія AllFrame, яка покращує потокову передачу АТА. Застосування цієї технології дозволяє зменшити втрату кадрів, поліпшити відтворення відео і збільшити кількість дискових відсіків, підтримуваних мережових відеореєстратором.

Накопичувачі WD Purple витримують в 3 рази більше навантаження, ніж накопичувачі для настільних ПК, і тому більше відповідають високим вимогам систем відеоспостереження. Детальні характеристики жорсткого диска наведено в табл. 4.5.

Таблиця 4.5 – характеристики WD Purple 8 TB

Виробник	WD
Лінійка	Purple
Тип	Жорсткий диск
Тип HDD	внутрішній
Обсяг, ГБ	8000
Інтерфейс підключення	SATA rev. 3.0
Форм-фактор, дюйм	3,5
Призначення	для систем відеоспостереження
Швидкість обертання шпинделя, об/хв	7200
Буфер, МБ	256

На думку багатьох на блоці живлення не потрібно економити, це один з найважливіших елементів комп'ютера який захищає від перепадів напруги та коротких замикань. Тому я вибрав рішення від компанії Thermaltake модель TR2 S 500W, яке зображено на рис. 4.6.

Блоки живлення серії TR2 S оснащується високоякісними компонентами та має ефективність до 86%. Ідеально підійде для комп'ютерів класу мейнстрім для виконання щоденних завдань. TR2 S має єдину +12 лінію з функцією стабілізації. Вбудований вентилятор ефективно охолоджує всі компоненти працюючи при цьому виключно тихо. Доступні моделі від 500W до 700W.



Рисунок 4.6 – Блок живлення Thermaltake TR2 S 500W.

Наявність високоякісних конденсаторів гарантує захист від витікання електроліту і вибуху, що забезпечує надійну і безперебійну роботу протягом довгого часу. Детальні характеристики оперативної пам’яті наведено в табл. 4.6.

Таблиця 4.6 – характеристики Thermaltake TR2 S 500W

Виробник	Thermaltake
Форм-фактор БЖ	ATX
Потужність сумарна, Вт	500
Потужність по каналах +3,3 V і +5 V, Вт	100
Потужність по каналам, сумарно по +12V1, 12V2, ..., Вт	420
Тип роз'єму підключення до материнської плати	ATX 20 +4 pin
Тип роз'єму підключення живлення процесора	1x4+4pin

HDD (IDE)	4
SATA	5
FDD	1
Роз'єми дод. живлення для відеокарт	2x6 + 2pin
Вхідна напруга, В	230
Функція PFC	активна
Стандарт 80 PLUS	80 PLUS
ККД (%)	86
Розміри, мм	140x150x86
Вентилятор, мм	120
Вихідний струм (+ 3.3V), А	20
Вихідний струм (+ 5V), А	15
Вихідний струм (+ 12V), А	35

В якості корпус підійде рішення від Zalman модель Z1 з двома 120мм вентиляторами. Корпус зображений на рис. 4.7.



Рисунок 4.7 – Корпус Zalman Z1.

В якості монітора підійде 27 дюймовий IPS монітор Dell S2721NX, який зображено на рис. 4.8.



Рисунок 4.8 – Монітор Dell S2721NX.

Dell S2721NX це 27 дюймовий IPS-монітор із сучасним дизайном та високою якістю зображення. Він створений для повсякденного використання, мультимедіа та роботи. Завдяки технології IPS, монітор забезпечує широкі кути огляду та точну передачу кольорів. Тонкі рамки та стильний вигляд роблять його відмінним вибором для домашнього або офісного використання.

Таблиця 4.7 – характеристики Dell S2721NX.

Виробник	Dell
Тип матриці	IPS
Діагональ екрану	27 дюймів
Роздільна здатність	Full HD (1920 x 1080)
Частота оновлення	75 Гц
Яскравість	300 ніт
Інтерфейси	HDMI 1.4 x 2, VGA
Енергоспоживання	20 Вт

В якості миші для комп’ютера підійде бюджетне рішення від компанії Logitech модель B-100, яку зображено на рис. 4.9.



Рисунок 4.9 – Миша Logitech модель B-100.

В якості клавіатури для комп'ютера підійде бюджетне рішення від компанії Trust модель ClassicLine, яку зображено на рис. 4.10.



Рисунок 4.10 – Клавіатура Trust ClassicLine.

Для проекту системи відеоспостереження навчального закладу підійде 16-портовий PoE комутатор від компанії TP-LINK модель TL-SG1016PE, який зображено на рис. 4.11. PoE комутатор забезпечує на видаленні електроживлення IP пристроїв, які приєднуються до нього за допомогою стандартного кабелю - кручена пара п'ятої категорії. Електропостачання і інформація транслюються одночасно з мережевого кабелю. Детальні характеристики TP-LINK TL-SG1016PE наведено у табл. 4.8.



Рисунок 4.11 - Комутатор PoE ONV-H1108PL.

Таблиця 4.8 – характеристики ONV-H1108PL

Тип пристрою	PoE комутатор, Некерований комутатор
Кількість портів	16
Стандарт PoE	IEEE 802.3af/at
Uplink порти	2 x 100 Мбіт / с
Загальна потужність PoE	110 вт
Стандарт живлення PoE	IEEE802.3af / at
Швидкість передачі даних	10/100/1000 Мбіт/с
Пропускна спроможність	32 Гбіт / с
Призначення	для забезпечення з'єднання IP пристроїв і подача живлення з підтримкою PoE
Живлення	AC 100-240V
Діапазон температур	0 ° C ~ + 40 ° C

В якості терміналу контролю доступу обрано модель Hikvision DS-K5671-ZU з можливістю ідентифікації особи, яка заходить в начальний заклад, за допомогою технології розпізнавання обличчя та алгоритмом глибокого

навчання, термінал зображено на рис. 4.12. Детальні характеристики Hikvision DS-KD9613-E6 наведено у табл. 4.9.



Рисунок 4.12 – Термінал ідентифікації особи Hikvision DS-K5671-ZU.

Таблиця 4.9 – характеристики Hikvision DS-K5671-ZU

Пам'ять	50 000 осіб
Час розпізнавання обличчя	0.2 с
Дисплей	7"
Відстань зчитування	0.3 - 3 м
Інтерфейс зв'язку	1 RJ-45 10/100/1000 мбіт/с
Камера	2 МП
Ступінь захисту	IP65
Робоча температура	-30°C - 60 °C

Цей модуль розпізнавання осіб є сучасним проектним обладнанням, яке використовує алгоритми глибокого навчання для забезпечення високої точності та швидкості розпізнавання. Пристрій оснащений 7-дюймовим сенсорним LCD-дисплеєм, двома камерами з роздільною здатністю 2 Мп кожна, а також вбудованим модулем Wi-Fi. Він сумісний із турнікетами

Hikvision і може підключатися до обладнання інших виробників через інтерфейси виводу або Wiegand.[26]

Модуль підтримує голосові підказки та різнорежимне підсвічування для зручності використання. Час розпізнавання обличчя становить менше 0,2 секунди, а точність перевищує 99%. У базі пристрою може зберігатися до 50 000 записів. Корпус модуля виконаний у мінімалістичному дизайні, відрізняється зручністю, високою герметичністю та міцністю.

На прохідній буде встановлено турнікет Hikvision DS-K3G501LX, який зображено на рис 4.13, для зручного проходу в обох напрямках та разом з терміналом розпізнавання особи буде виконувати роль системи контролю доступу навчального закладу.



Рисунок 4.13 – Турнікет Hikvision DS-K3G501LX

4.2 Проєктування та налаштування системи контролю доступу та відеоспостереження.

Ця блок-схема демонструє структуру локальної мережі навчального закладу, в якій головний ПК виконує роль сервера для навчального середовища Moodle, відеореєстратора для IP-камер відеоспостереження, а також налаштовує та керує турнікетом і терміналом розпізнавання облич. Використання головного ПК як централізованого відеореєстратора та контролера для системи контролю доступу усуває необхідність у додаткових

апаратних відеореєстраторів для камер і контролерах СКУД для турнікета та терміналу, що робить систему більш економічно вигідною та спрощує її налаштування.

РoЕ-комутатор об'єднує мережу й одночасно забезпечує живлення IP-камер через кабелі Ethernet, що дозволяє мінімізувати використання додаткових проводів і обладнання. Додаткові комутатори розташовані в навчальних класах і виконують функцію об'єднання навчальних комп'ютерів у єдину мережу, забезпечуючи підключення до головного сервера. Підключення мережі до інтернету здійснюється через маршрутизатор провайдера, що забезпечує доступ до глобальної мережі для синхронізації даних, віддаленого управління та оновлення програмного забезпечення. Кожен елемент мережі взаємодіє з головним сервером, створюючи централізовану, ефективну та надійну систему для контролю доступу, відеоспостереження й організації навчального процесу в освітньому закладі.

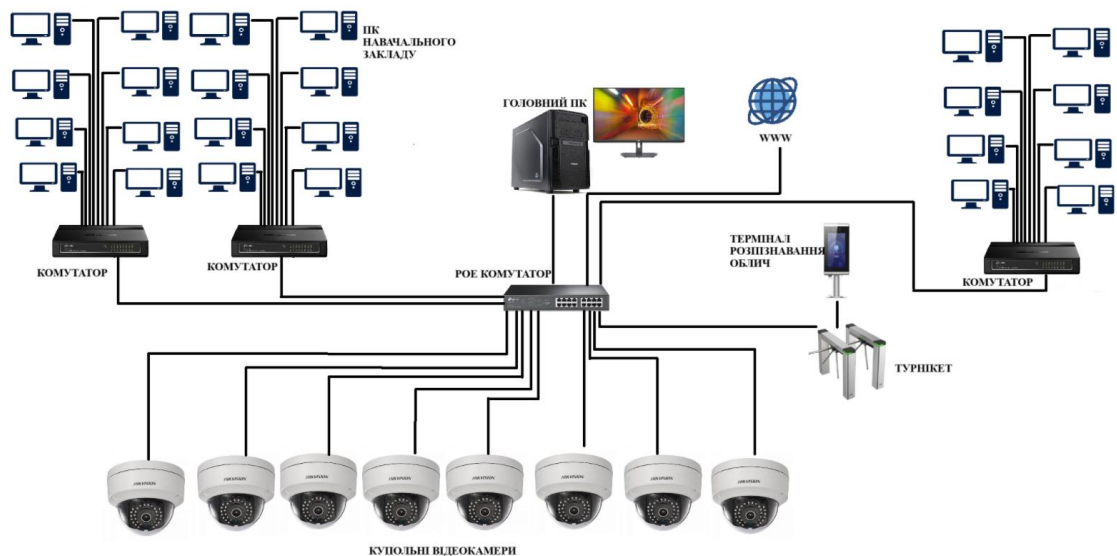


Рисунок 4.14 – структура локальної мережі навчального закладу

На рис. 4.14 зображено фізичну структуру першого поверху навчального закладу. Школа містить 2 поверхи, 14 класів, бібліотеку, учительську, кабінет охорони, кладову, котельню та 2 санвузли.

На першому поверсі до мережі підключено 5 камер за допомогою комутатора, який сховано в кабінеті охорони. Кабелі сховано в підвісній стелі. Живлення камер відбувається по кабелях Ethernet.

У вестибюлі розміщено турнікет з терміналом ідентифікації особи та камера, щоб уникнути проникнення в школу посторонніх осіб. В коридорі на першому поверсі розміщено дві камери які стежать за порядком, їх поле зору покриває весь коридор. Також ще одна знаходиться в класі інформатики, вона стежить за порядком під час навчального процесу та береже дороге обладнання в класі. На задньому дворі за порядком стежить камера, її поле зору охоплює входи в кладову та котельню.

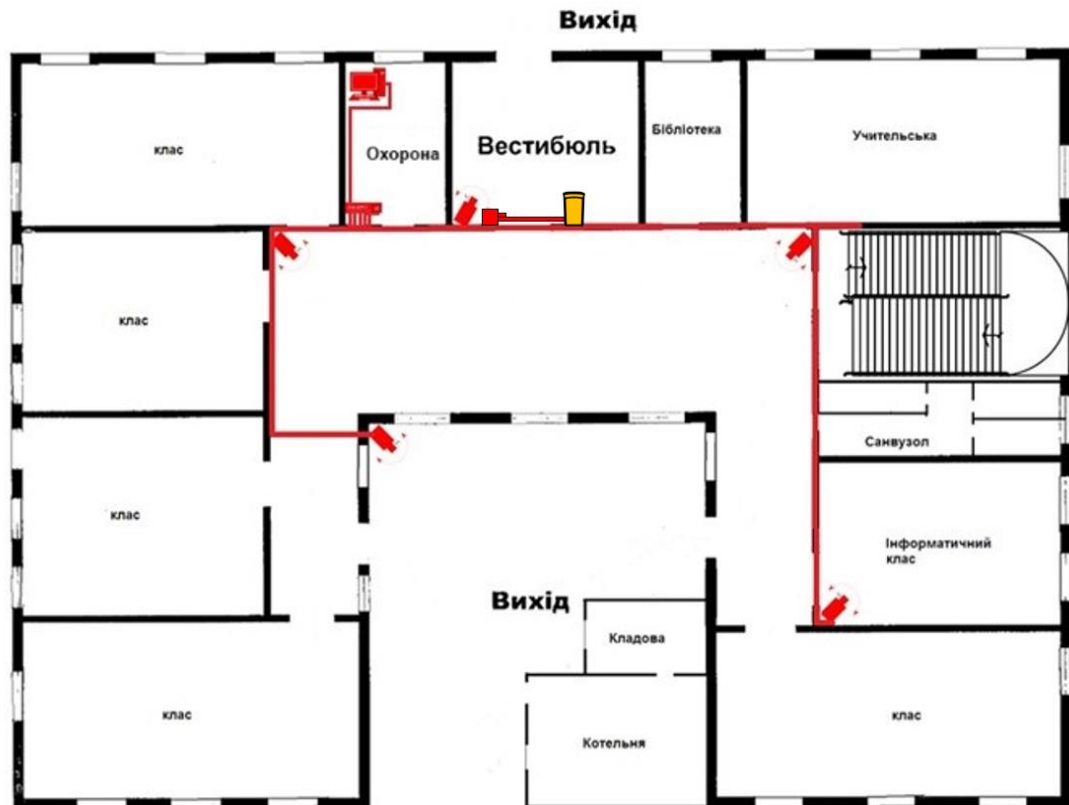


Рисунок 4.14 – Фізична структура мережі відеоспостереження першого поверху.

На рис. 4.15 зображено фізичну структуру другого поверху навчального закладу.

На другому поверсі до мережі підключено 3 камери за допомогою комутатора ,який сховано в кабінеті директора. Кабелі сховано в підвісній стелі. Живлення камер відбувається по кабелях Ethernet.

В коридорі на другому поверсі розміщено дві камери які стежать за порядком, їх поле зору покриває весь коридор. Одна камера розміщена на сходовому майданчику.

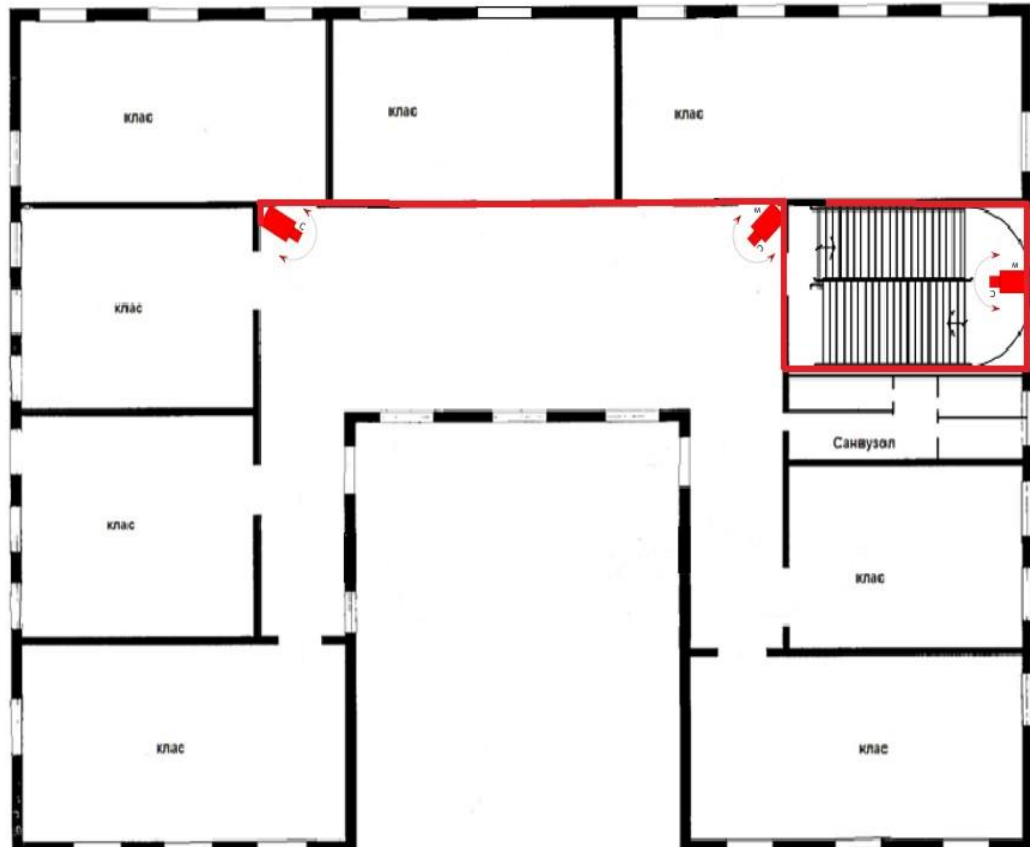


Рисунок 4.15 – Фізична структура мережі відеоспостереження другого поверху.

Щоб керувати системою контролю доступу я буду працювати з програмою iVMS-4200. Hikvision iVMS-4200 є безкоштовним і універсальним програмним забезпеченням для управління відеоспостереженням. Програмне забезпечення надає безліч функціональних можливостей, в тому числі відображення відео в режимі реального часу, запис відео, віддалений пошук і

відтворення запису, резервне копіювання файлів, а також підключення пристроїв для різних завдань відеоспостереження.

Гнучка розподілена структура і простота у використанні функцій широко застосовується в проектах відеоспостереження середнього або малого масштабів.

Щоб комп'ютер виконував функції відеореєстратора потрібно при встановленні вказати на встановлення утиліти Storage Server, як показано на рис. 4.16.

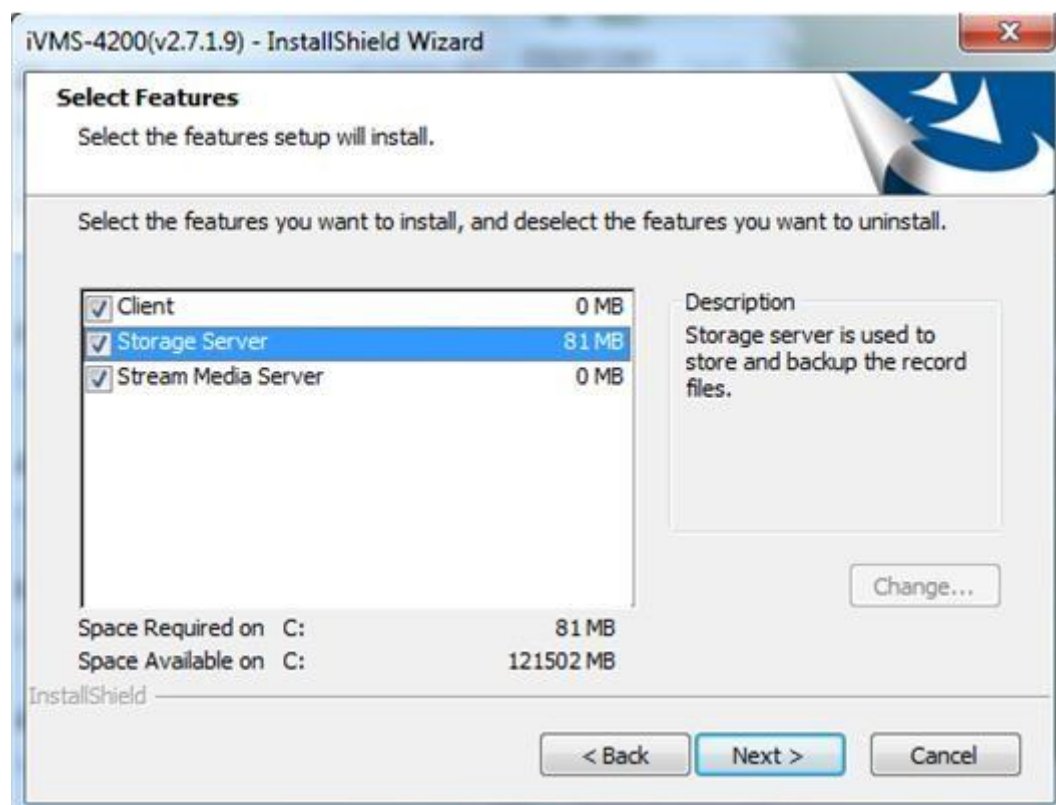


Рисунок 4.16 – Процес встановлення iVMS-4200.

Після встановлення програми iVMS-4200, в головному меню вибираємо пункт Maintenance and Management, як показано на рис. 4.17.

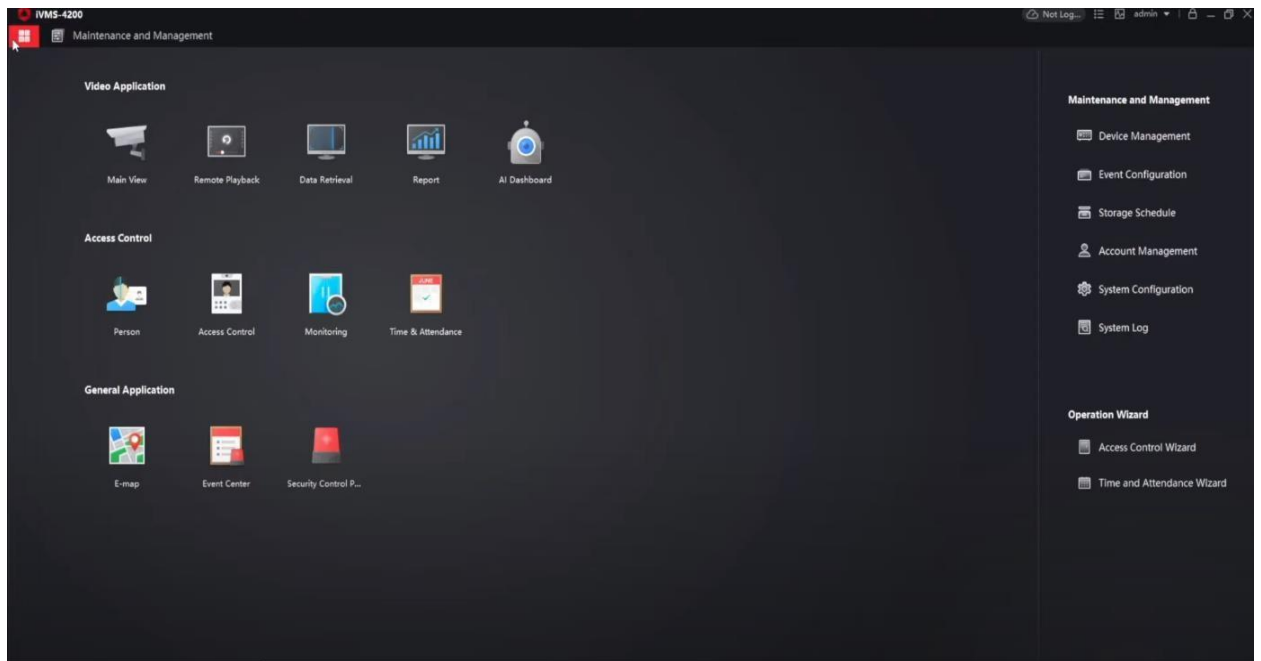


Рисунок 4.17 - Головне меню iVMS-4200.

У вкладці online device шукаємо пристрій storage server та натискаємо add, після цього на з'явиться вікно, як показано на рис. 4.18 де потрібно придумати пароль та вказати іншу ip адресу для роботи в нашій мережі.

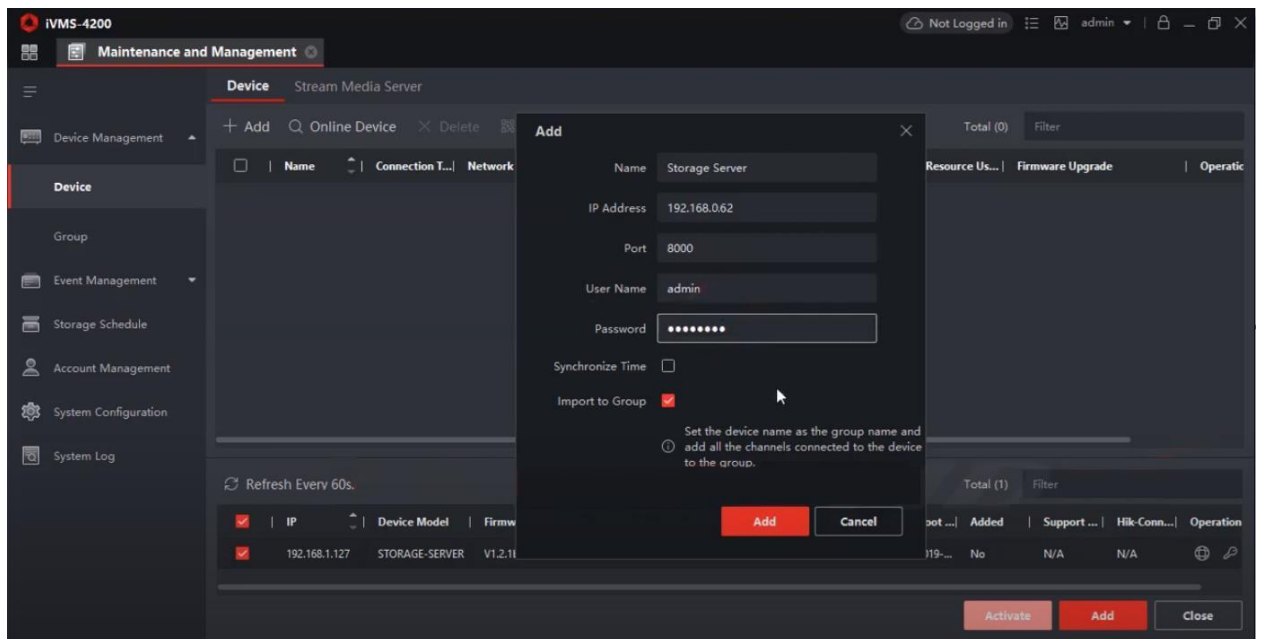


Рисунок 4.18 – Вікно налаштування пристрою.

Наступний крок, потрібно перейти в налаштування нашого серверу та відкрити вкладку storage а в ній вкладку general, як показано на рис. 4.19, та вибрати диск для запису даних та натиснути кнопку format. Після цього диск відформатується і буде працювати в ролі сховища для відео з камер. В той час, як інший диск можливо буде використовувати для інших потреб.

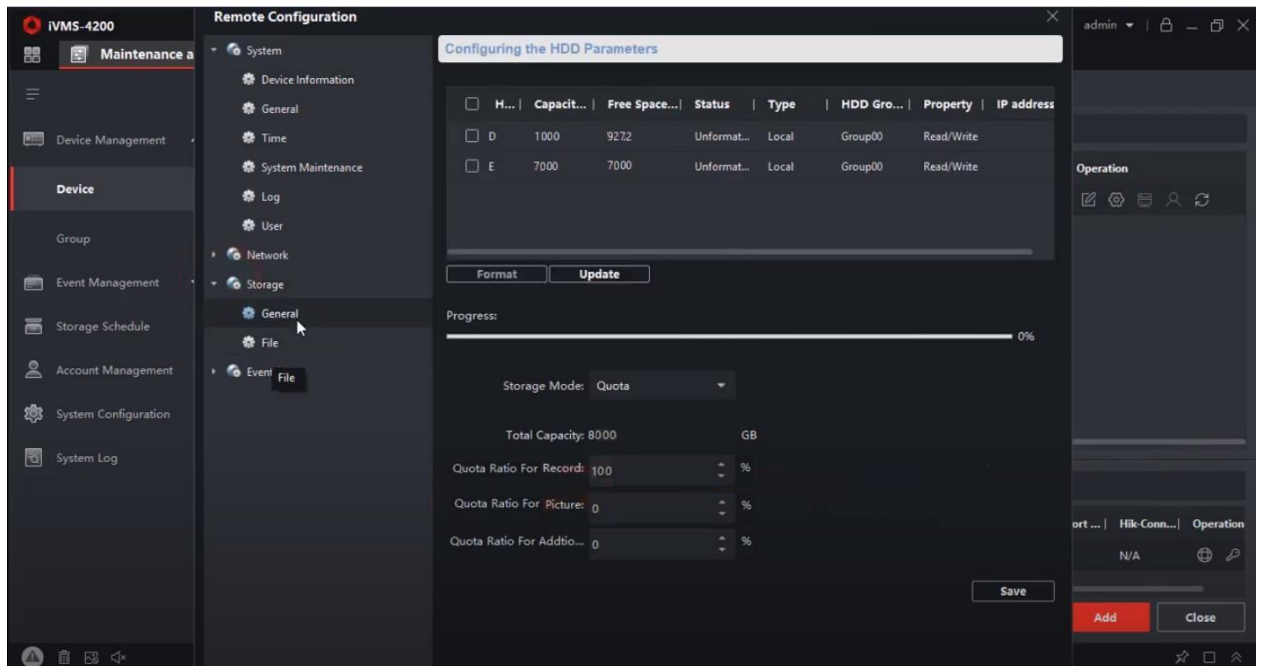


Рисунок 4.19 – Налаштування серверу.

Після налаштування сховища, потрібно у вкладці online device вибрати нашу першу камеру та перейти в її налаштування. В налаштуваннях змінюємо її ip адресу за замовчуванням (192.168.1.64) на ip адресу яка може використовуватися в нашій мережі (192.168.0.62), та натискаємо ок, як показано на рис. 4.20.

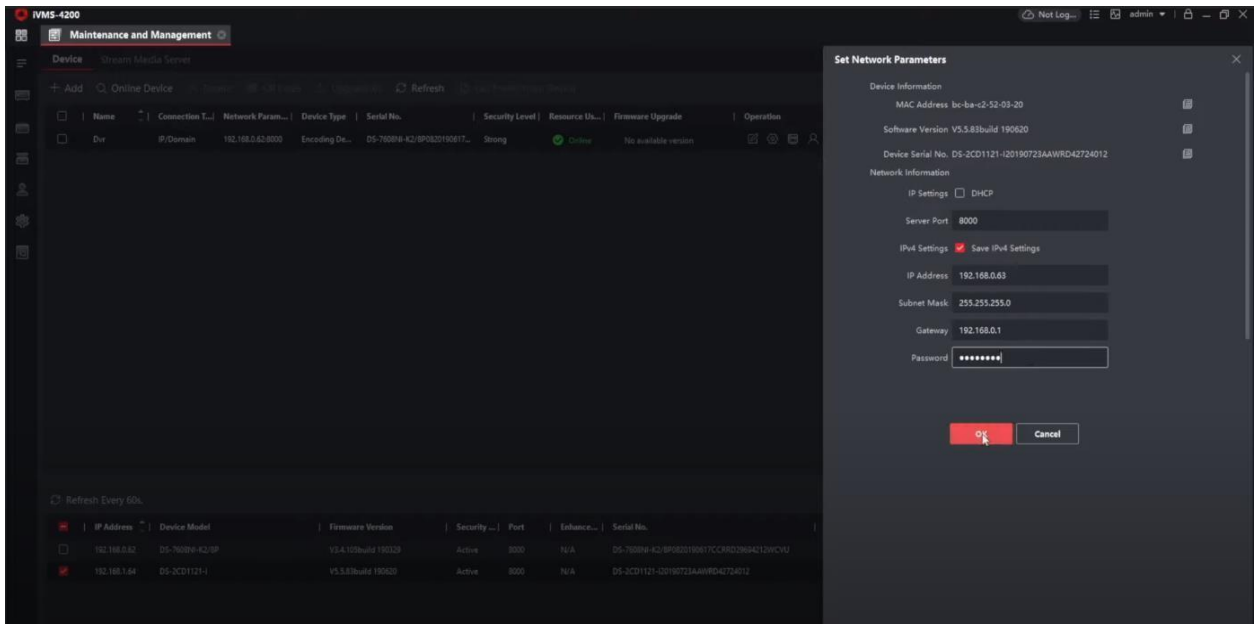


Рисунок 4.20 – Налаштування ір камери.

Як показано на рис. 4.21 напроти нашої камери і нашого серверу вказаний зелений статус online.

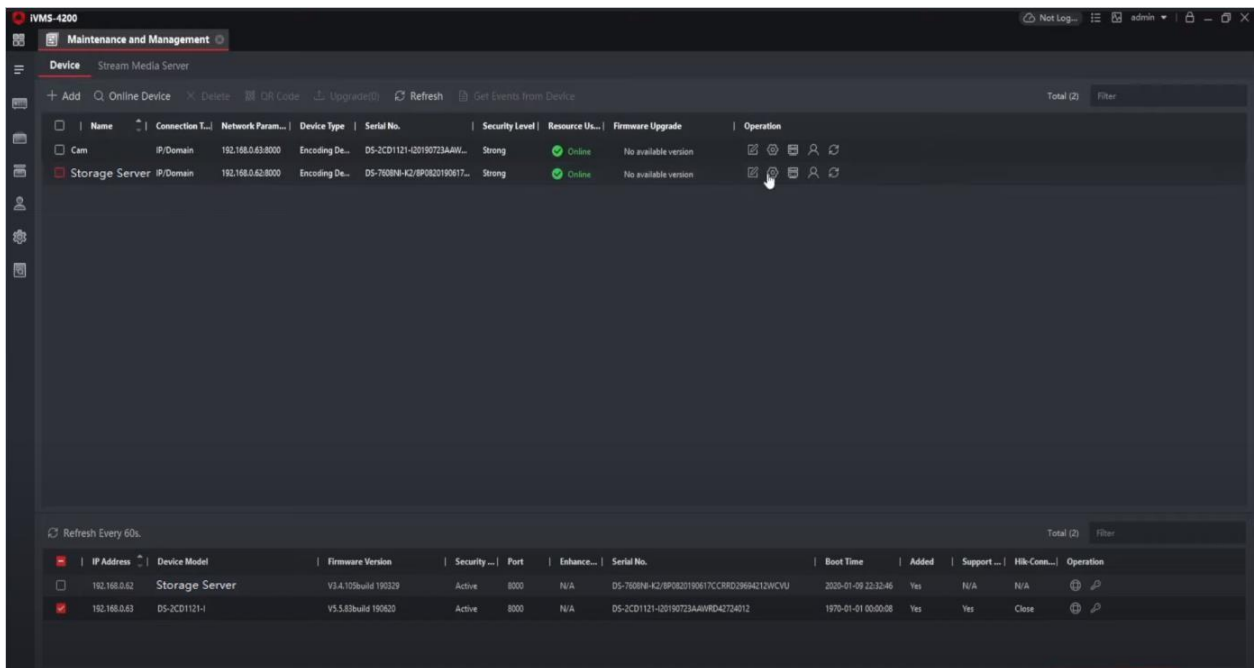


Рисунок 4.21 – Вікно менеджера пристроїв.

Тепер щоб активувати запис камер на сервер треба перейти у вкладку Storage Schedule, вибрати потрібну нам камеру та вказати у пункті Storage

Server наш записуючий пристрій, та щоб запис відбувався цілодобово треба в пункті Schedule Template вибрати опцію All-day Template, як показано на рис. 4.22.

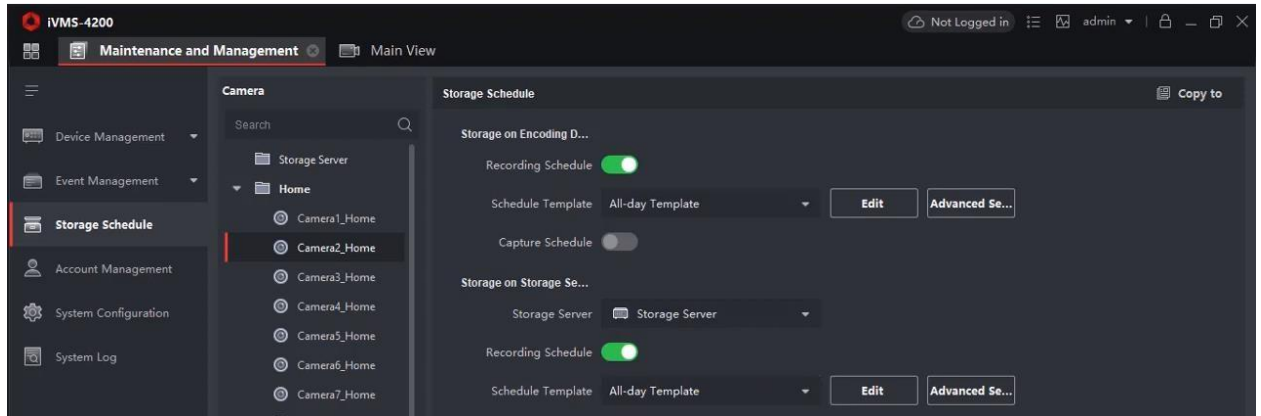


Рисунок 4.22 – Налаштування шляху запису пристроїв.

Після налаштування камер переходимо у головне меню, як показано на рис 4.23 та знаходимо вкладку Main View.

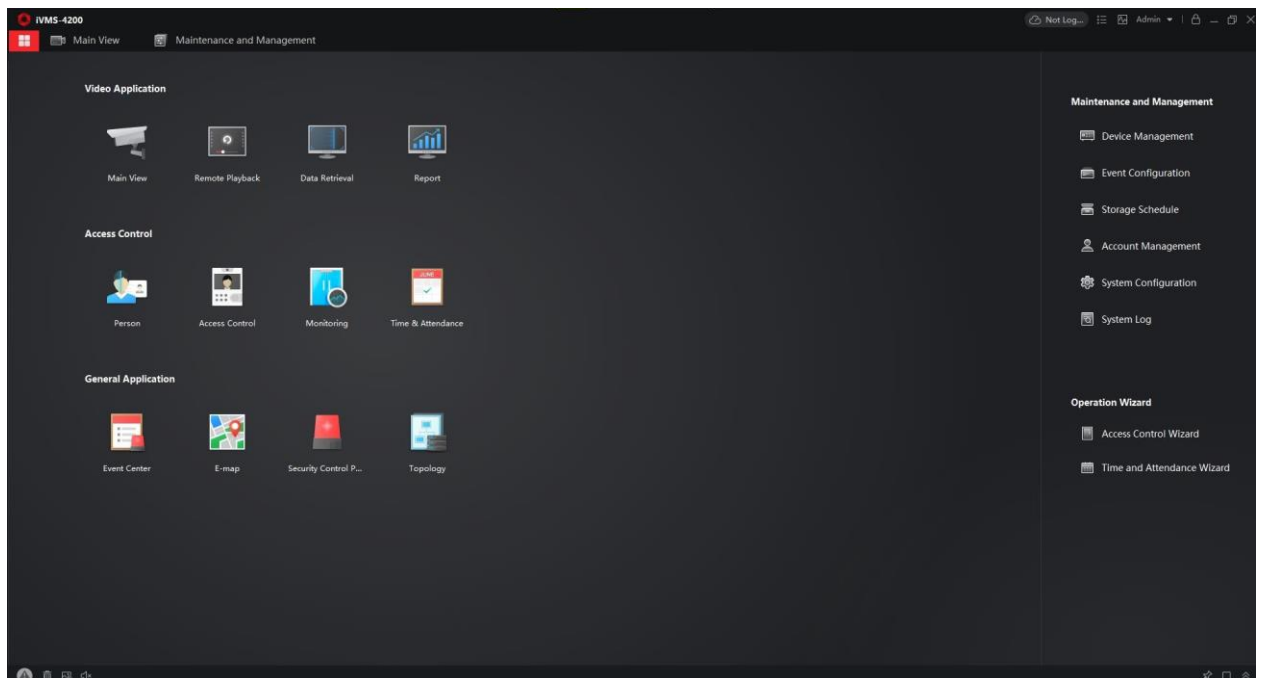


Рисунок 4.23 - Головне меню iVMS-4200

У цій вкладці можливо переглядати камери у режимі онлайн,

потрібно тільки вибрати потрібну камеру у бічній вкладці, як показано на рис. 4.24.

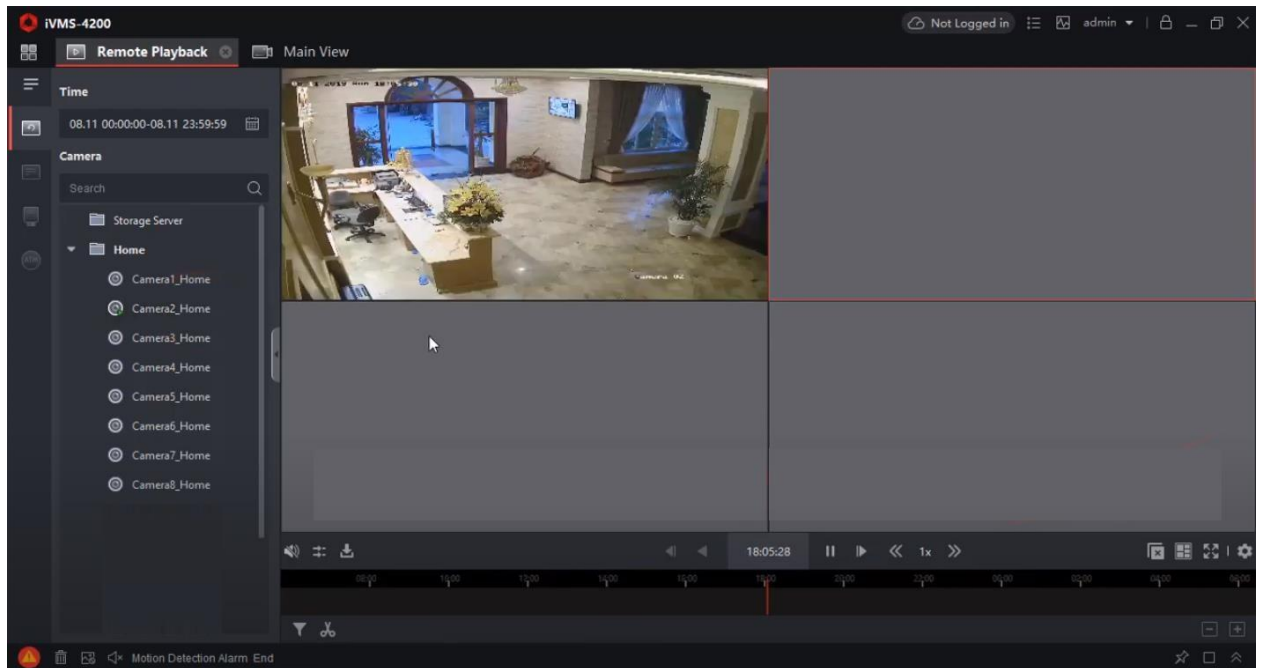


Рисунок 4.24 – Вікно перегляду камер

Тепер додаємо термінал розпізнавання лиць, в цій же програмі iVMS 4200. Для цього знову переходимо в головне меню, яке показано на рис. 4.25 та вибираємо пункт Maintenance and Management.

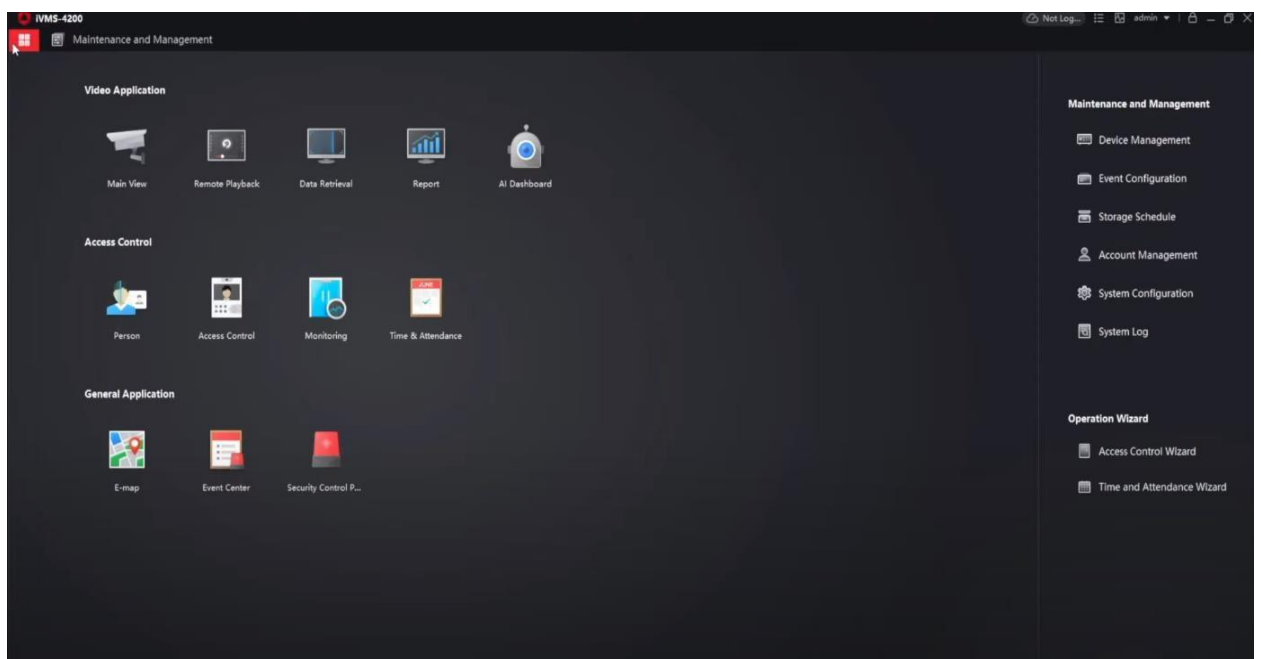


Рисунок 4.25 - Головне меню iVMS-4200

У вкладці online device натискаємо add та додаємо наш термінал, його ім'я, ір-адресу, порт, логін і пароль, як показано на рис. 4.26.

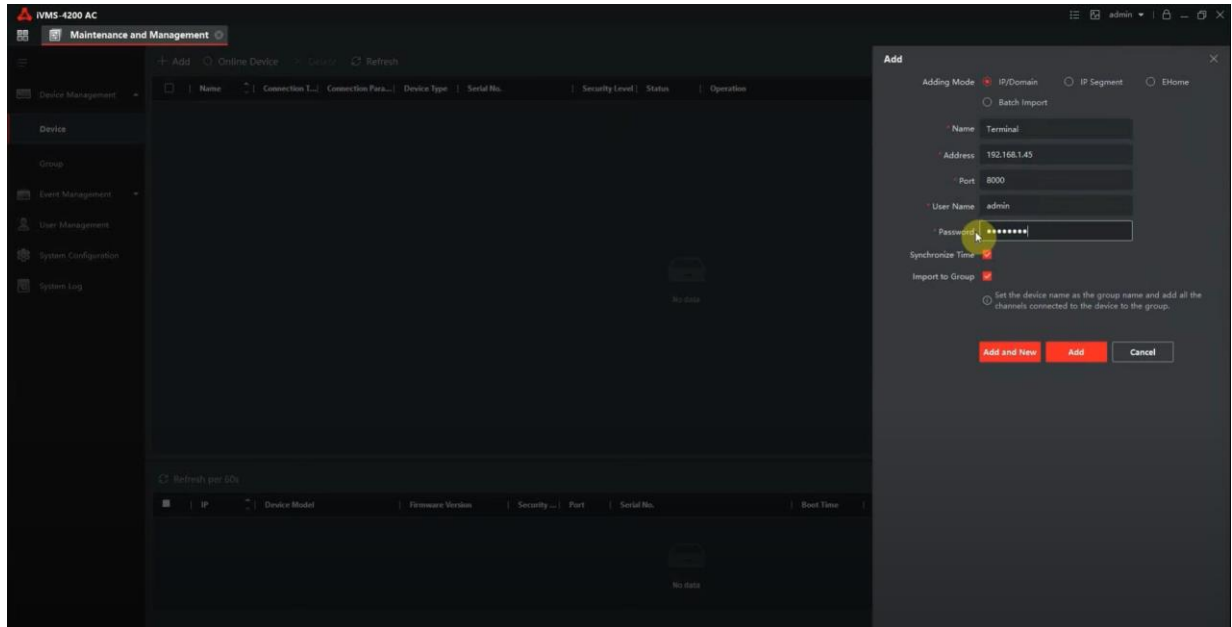


Рисунок 4.26 – Додавання терміналу

Як показано на рис. 4.27 напроти нашого терміналу вказаний зелений статус online.

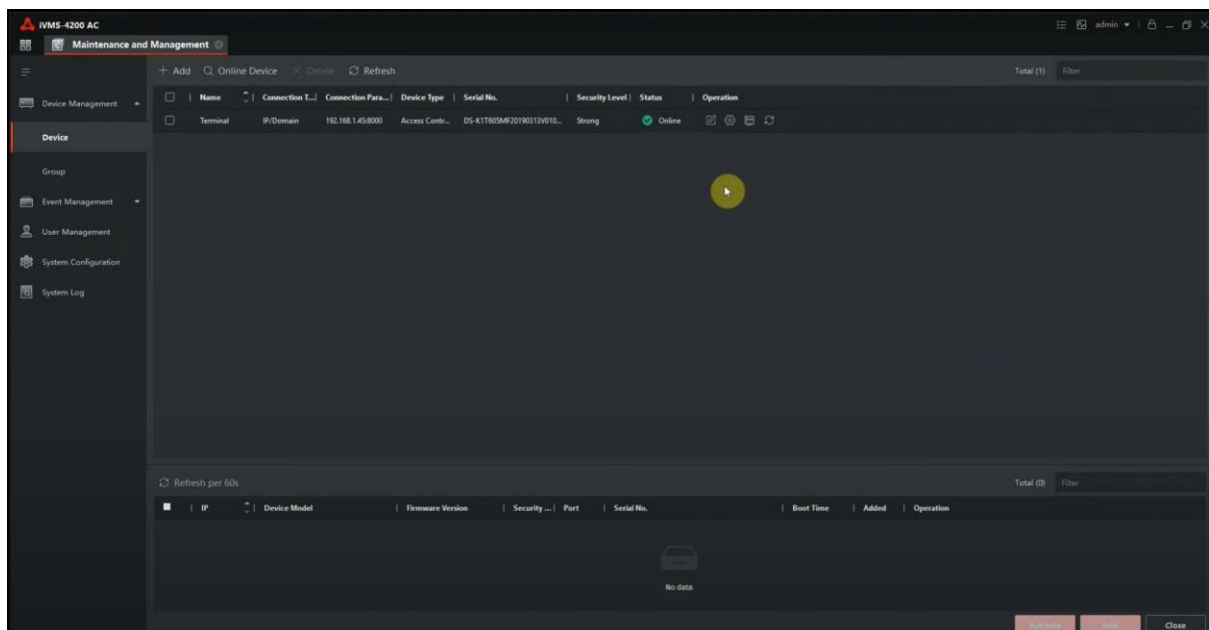


Рисунок 4.27 – Вікно менеджера пристроїв.

Переходимо до головного меню, та натискаємо на вкладку Person. В ній натискаємо на add та заповнюємо особисту інформацію відвідувача: ім'я, стать, email, телефон, номер особистої картки пропуску. У вкладці Add face додаємо особисту фотографію відвідувача, як показано на рис 4.28.

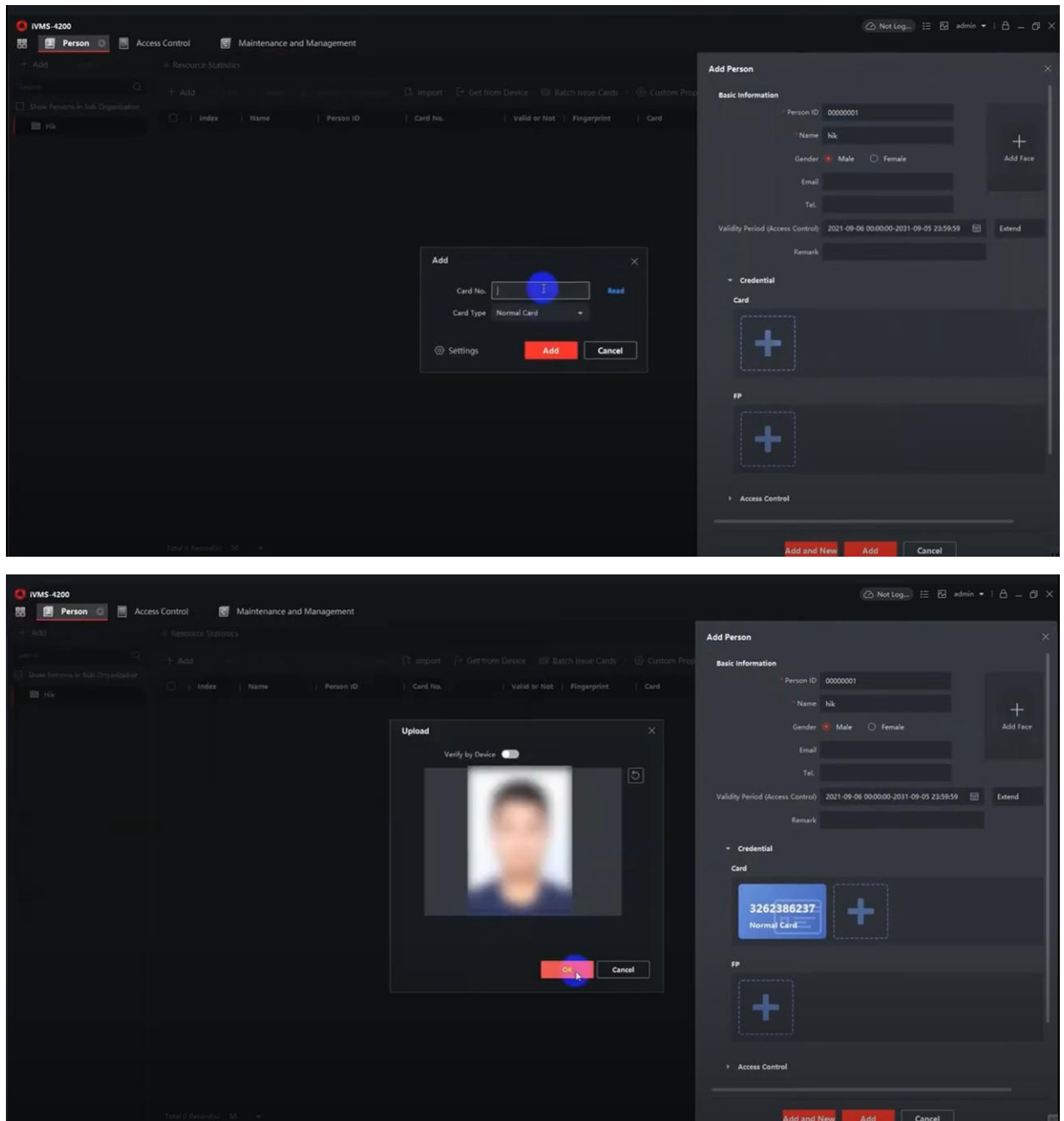


Рисунок 4.28 – Додавання профілю відвідувача.

Після додаємо всі профілі відвідувачів у вкладці Access Control, як показано на рис 4.29.

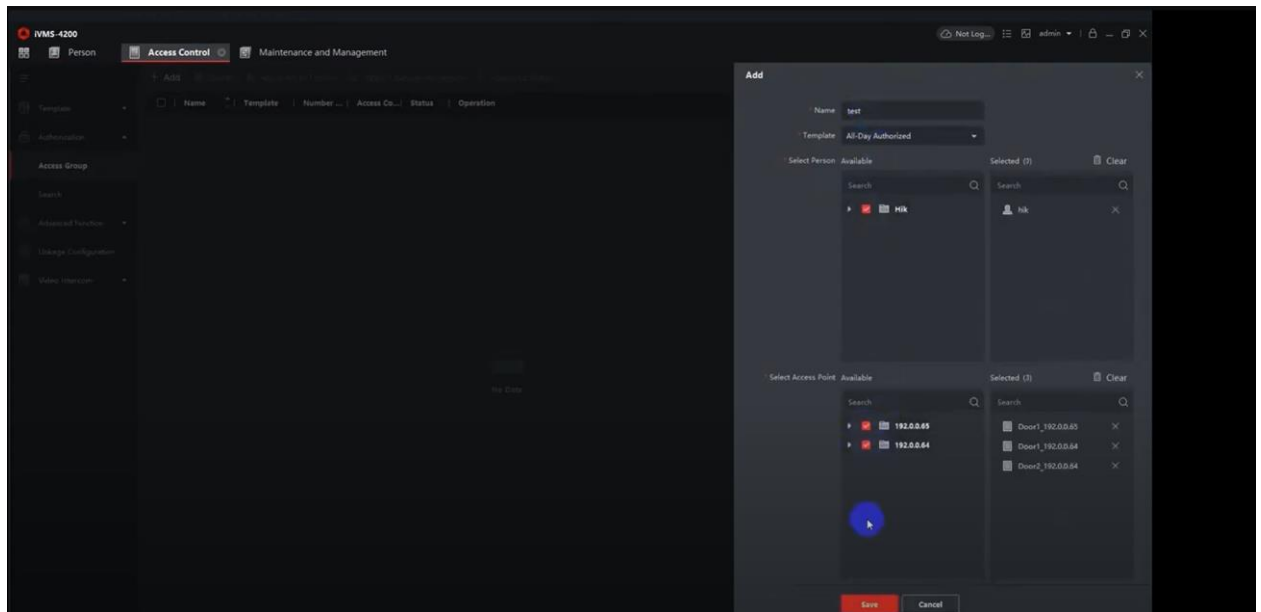


Рисунок 4.29 – Створення групи відвідувачів у вкладці Access Control

Після успішного налаштування системи біометричного контролю доступу та відеоспостереження Hikvision, вони будуть забезпечувати підвищений рівень безпеки та автоматизації управління доступом. Ця інтеграція дозволяє ефективно контролювати вхід до приміщень, ідентифікувати користувачів за біометричними даними та здійснювати моніторинг у реальному часі, що сприяє безпеці та прозорості навчального процесу.

4.3 Встановлення та налаштування навчального середовища Moodle на локальний сервер навчального закладу.

Moodle є ідеальним вибором для ролі навчального середовища в українському навчальному закладі завдяки своїм численним перевагам. Платформа має відкритий код, що забезпечує відсутність витрат на ліцензії та можливість адаптації під потреби конкретного закладу. Вона повністю відповідає українським освітнім стандартам.

Система пропонує широкий набір інструментів для дистанційного навчання, таких як завдання, тести, форуми та інтерактивні матеріали, а також автоматизацію перевірки тестів і надання зворотного зв’язку. Вона легко інтегрується з популярними сервісами, зокрема Zoom, Google Drive.

Moodle є гнучким і масштабованим рішенням, яке підходить як для малих шкіл, так і для великих університетів. Крім того, платформа вже широко використовується в українських навчальних закладах, що дозволяє скористатися досвідом колег, готовими шаблонами курсів і рекомендаціями. Завдяки своїй доступності, функціональності та відповідності сучасним потребам, Moodle є найкращим вибором для організації навчального процесу в Україні.

В якості локального серверу можливо використовувати ідентичний ПК, який було підібрано для систем контролю доступу та відеоспостереження, проте краще зекономити на меншому за обсягом жорсткому диску.

Спочатку, треба завантажити останню версію Moodle з офіційного сайту, як показано на рис. 4.30.

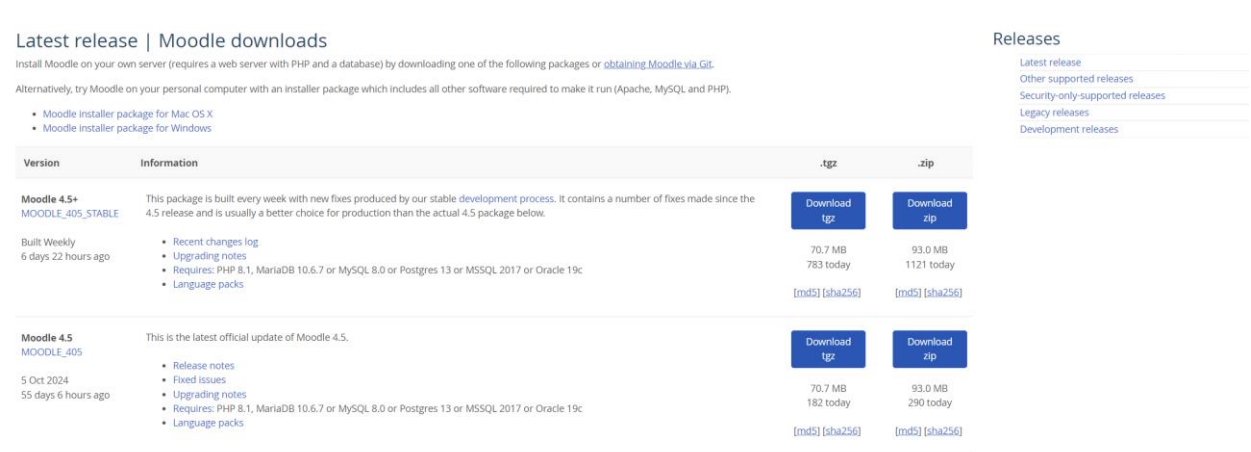


Рисунок 4.30 – Сторінка завантаження Moodle.

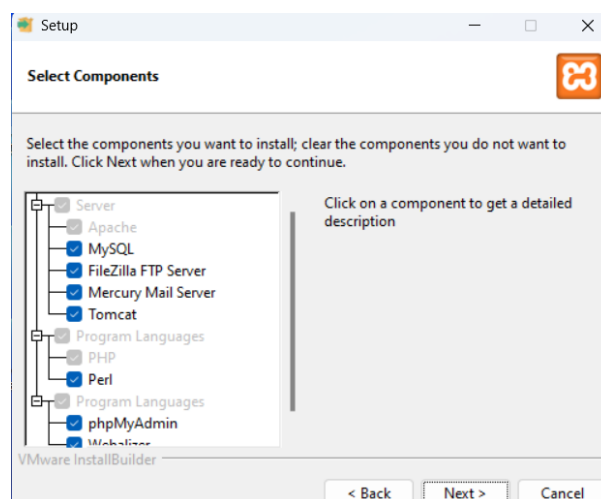
Завантажуємо ХАМРР з офіційного сайту, як показано на рис 4.31. ХАМРР - це повністю безкоштовний і простий в установці дистрибутив

Apache, який включає MariaDB, PHP та Perl. XAMPP створений з відкритим вихідним кодом, щоб бути надзвичайно простим у встановленні та використанні.



Рисунок 4.31 – Сторінка завантаження XAMPP

Встановлюємо XAMPP , як показано на рис 4.32.



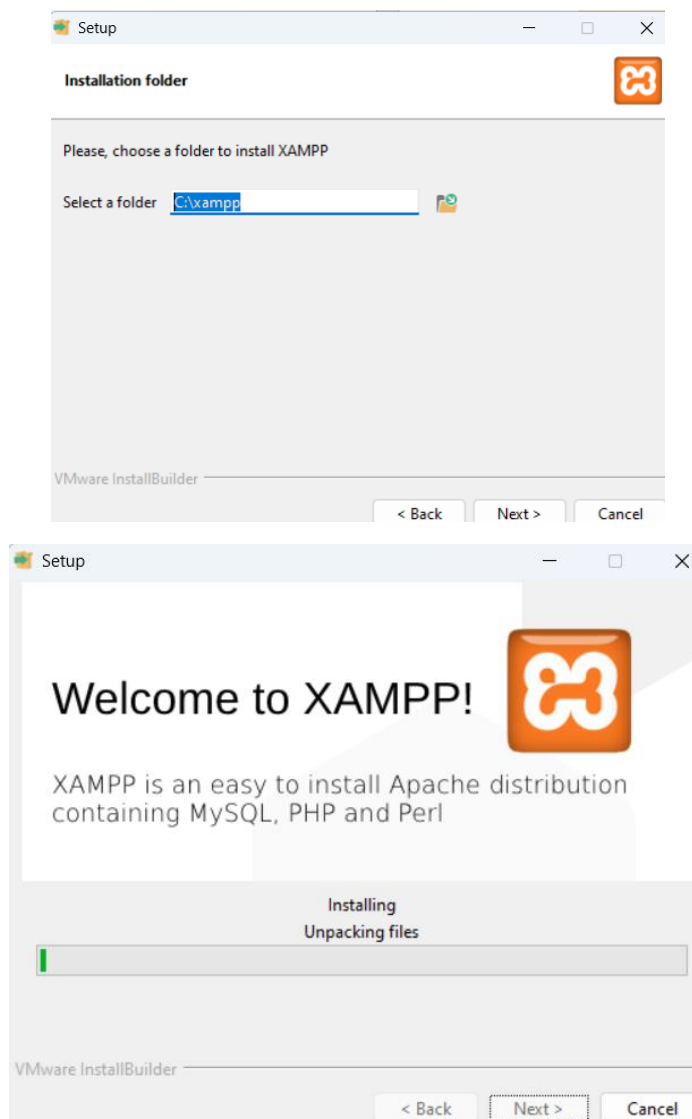


Рисунок 4.32 – Процес встановлення XAMPP.

Після встановлення програми, відкриваємо і за допомогою її встановлюємо Apache та MySQL, як показано на рис. 4.33.

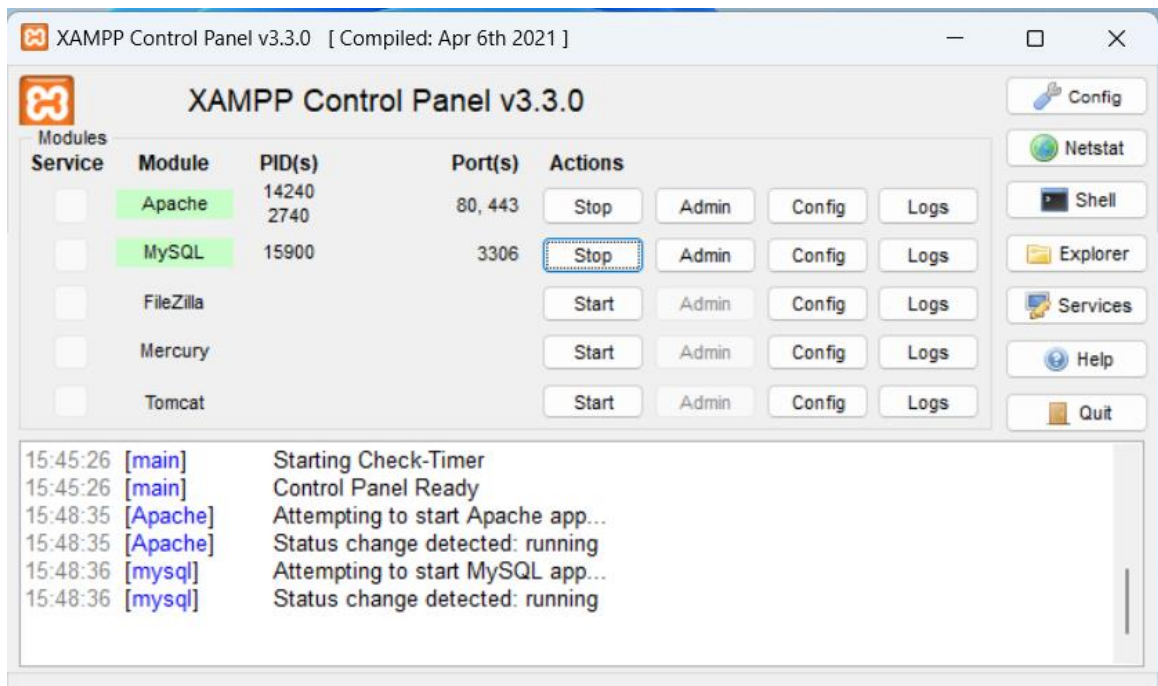


Рисунок 4.33 – Процес встановлення Apache та MySQL в XAMPP.

Перевіряємо роботу XAMPP Apache та phpMyAdmin, після встановлення через localhost, як показано на рис 4.34.

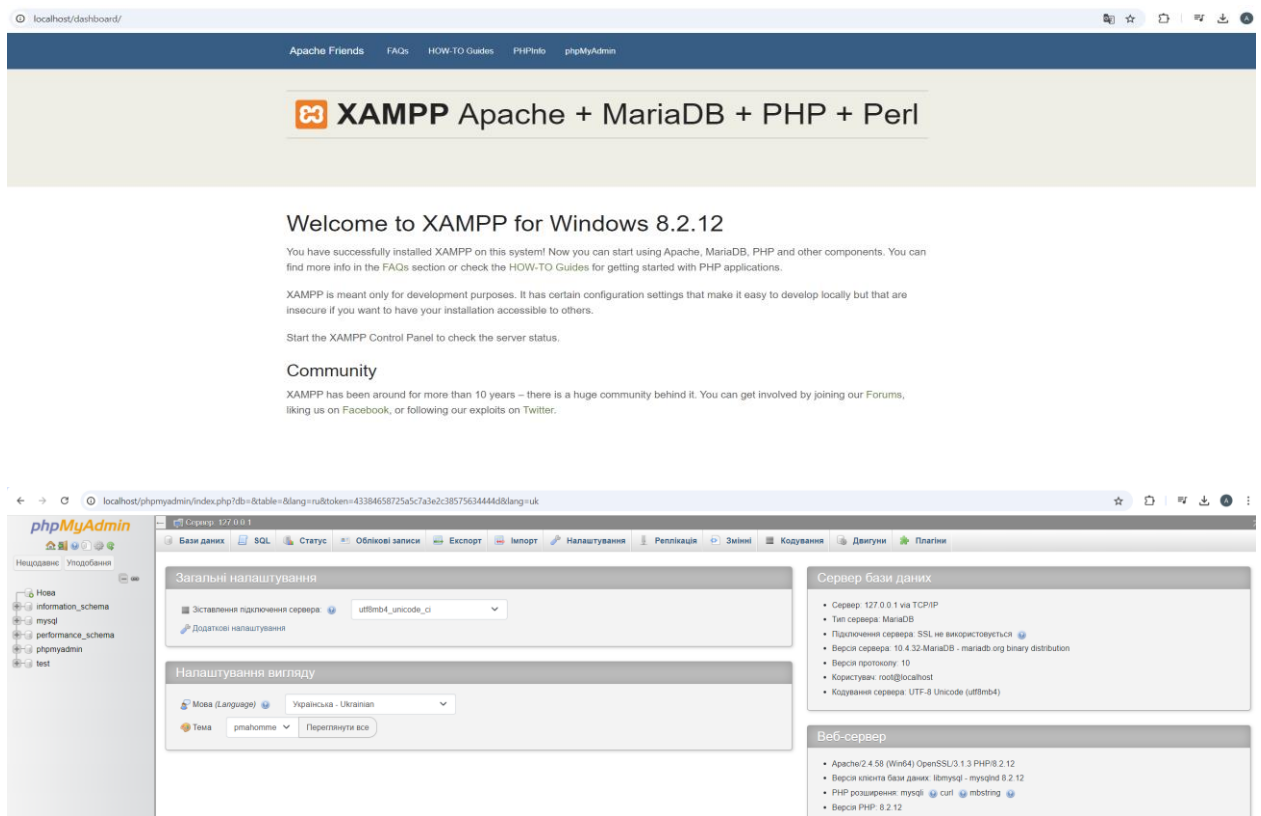
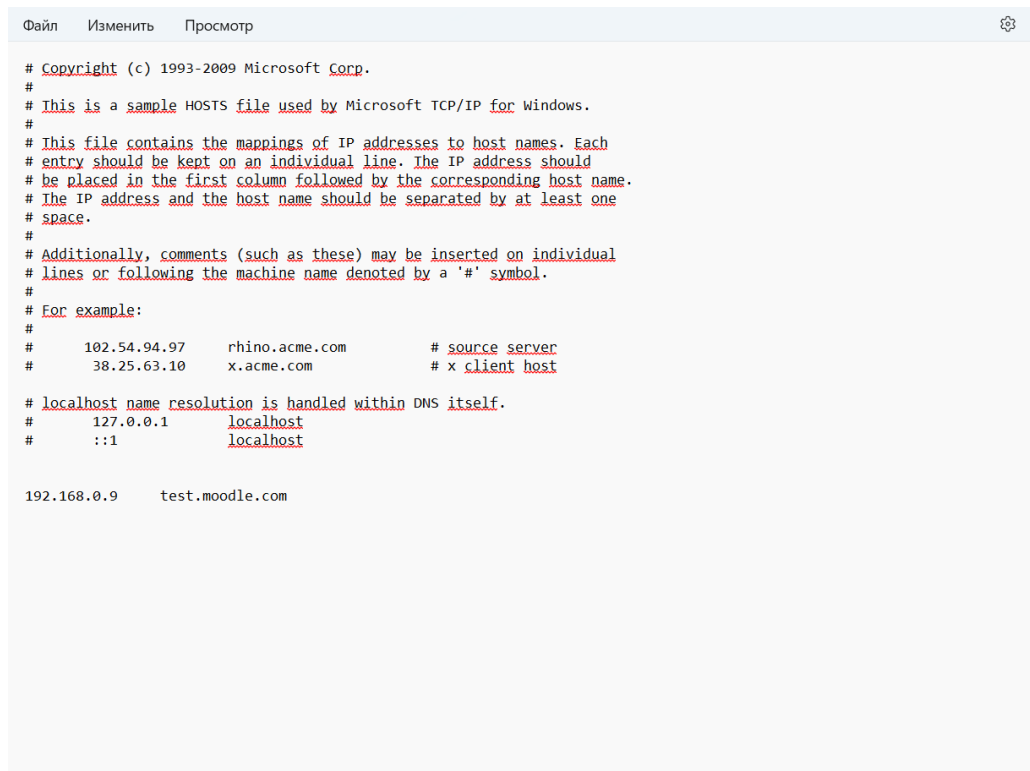


Рисунок 4.34 – Локальна веб сторінка XAMPP Apache та phpMyAdmin.

Так як сервер локальний, створюємо унікальний домен найпростішим шляхом. За адресою C:\Windows\System32\drivers\etc, відкриваємо файл hosts. Та вписуємо ip нашого сервера та новий домен, як показано на рис. 4.35. Це найпростіший варіант, та він потребує редагування файлу hosts на всіх комп'ютерах у нашій локальній мережі, краще прописати домен у маршрутизаторі з DNS сервером локальної мережі.



```

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost

192.168.0.9      test.moodle.com

```

Рисунок 4.35 – Редагування файлу hosts

Після цього, розпаковуємо архів Moodle за шляхом C:\xampp\htdocs, як показано на рис. 4.36.

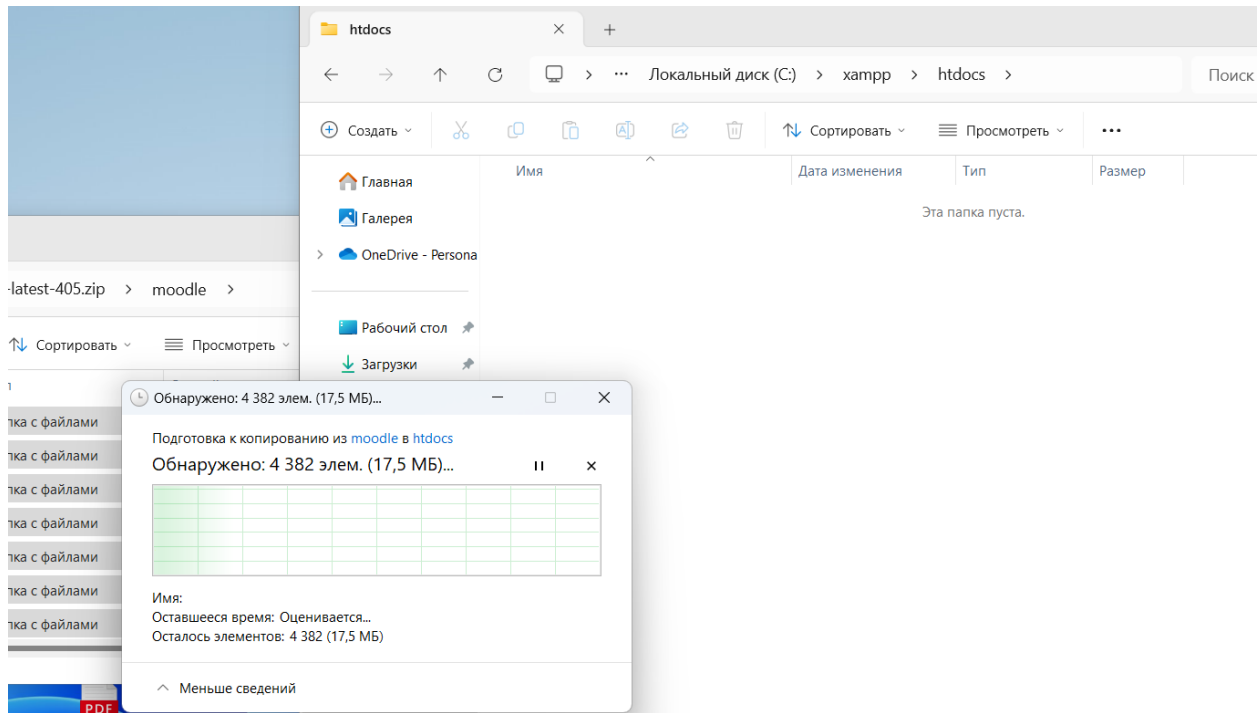
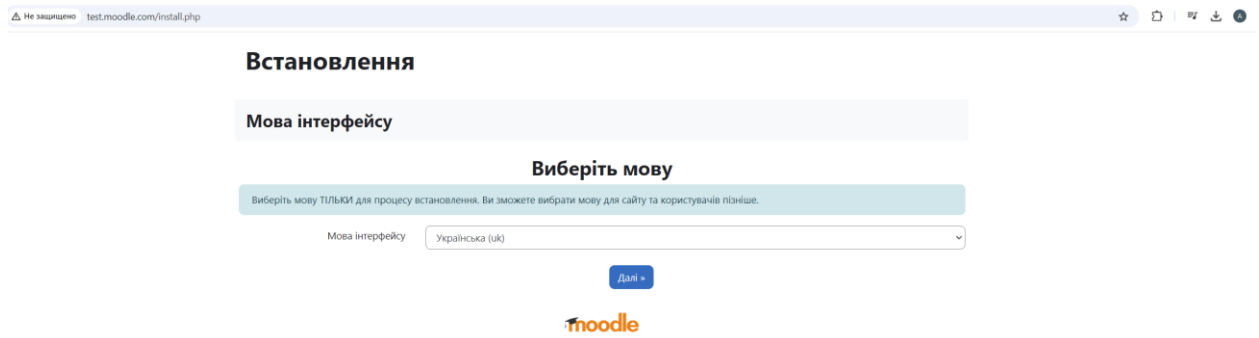


Рисунок 4.36 – Розпаковка файлів Moodle.

Заходимо на сторінку нашого серверу, тепер це сторінка налаштування Moodle, обираємо українську мову, та обираємо шлях для файлів, як показано на рис 4.37.



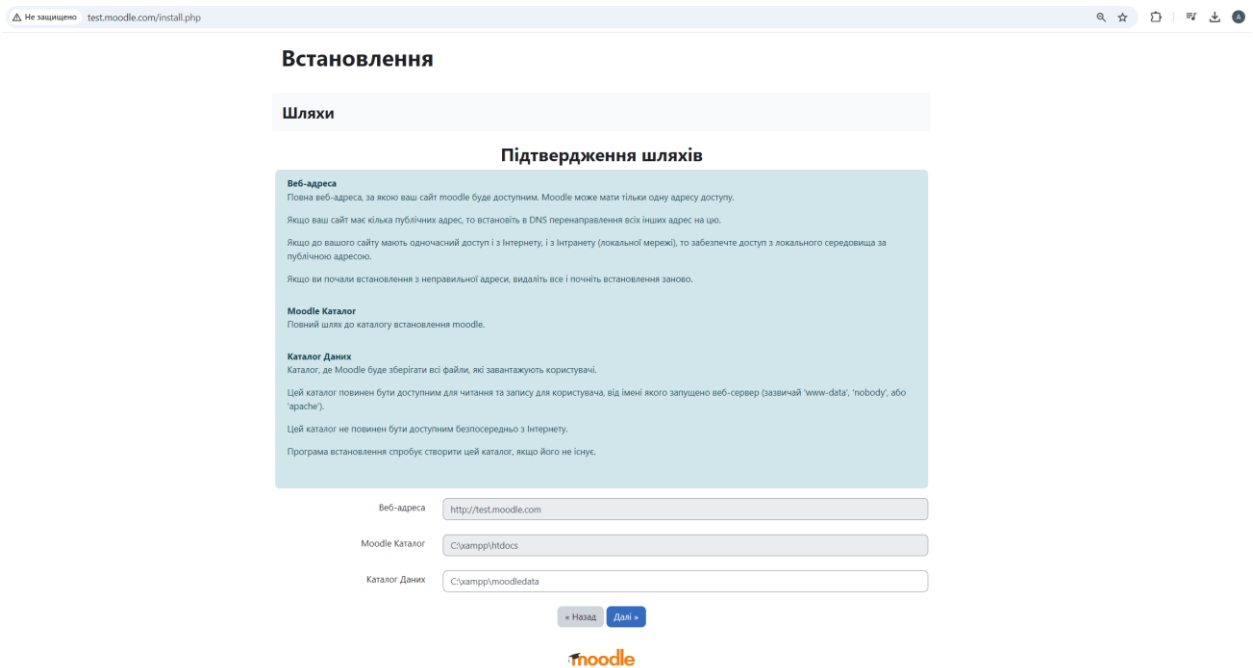


Рисунок 4.36 – сторінка налаштування Moodle.

Обираємо драйвер бази даних, залишаємо поліпшений MySQL, який стояв за замовчуванням, як показано на рис. 4.37.

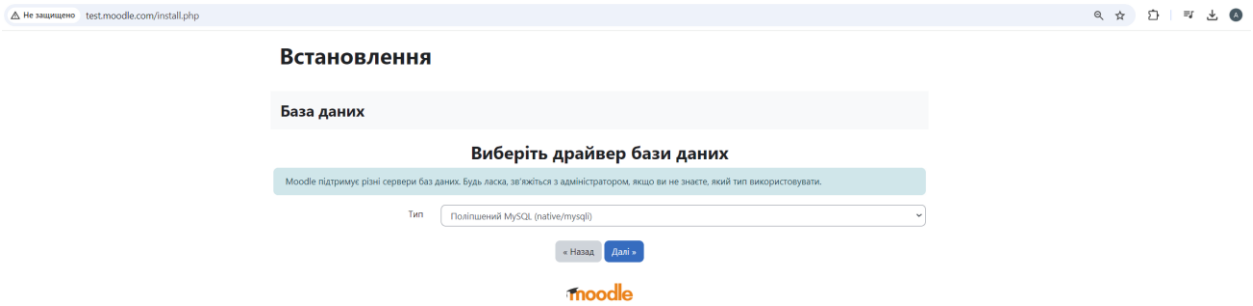


Рисунок 4.37 – сторінка налаштування Moodle.

Налаштовуємо базу даних, та послідовно заповнюємо вільні поля. У файлі `my.ini` шукаємо порт, ім'я користувача `root` за замовчуванням, пароль залишаємо пустим, як показано на рис 4.38.

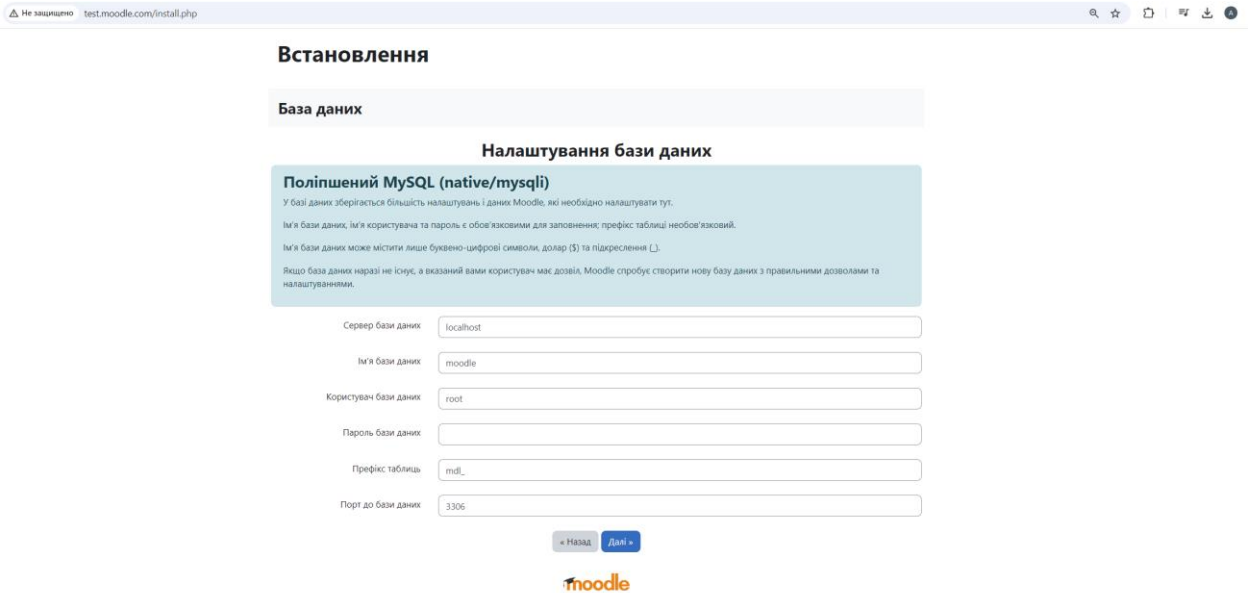


Рисунок 4.38 – сторінка налаштування Moodle.

Переходимо до сторінки налаштувань серверу, яка показує що треба ще встановити для коректної роботи Moodle, як показано на рис 4.39.

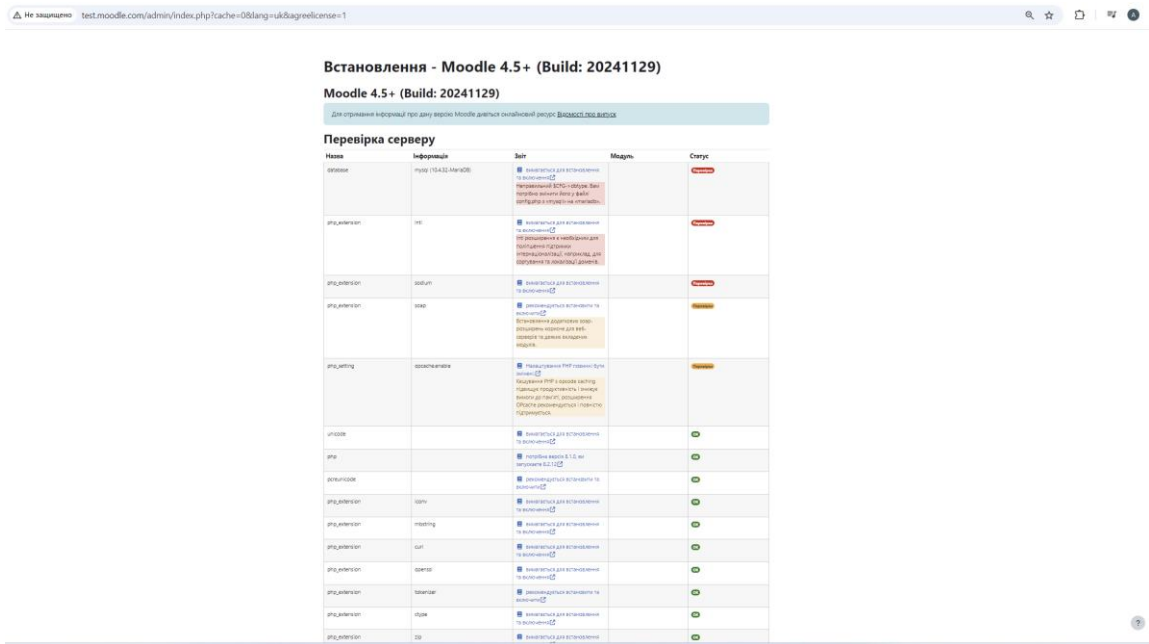
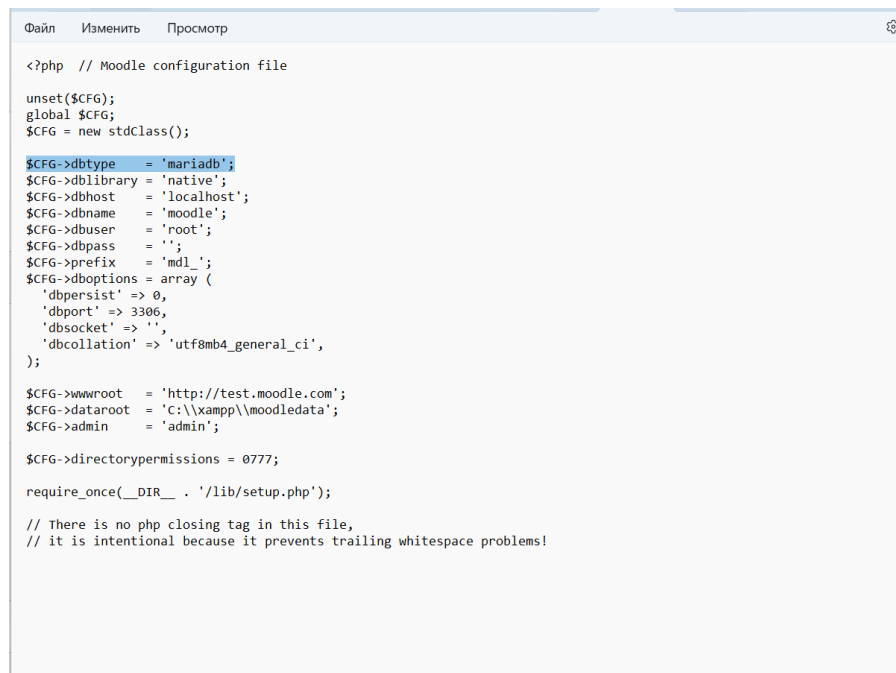


Рисунок 4.39 – сторінка налаштування Moodle.

За шляхом C:\xampp\htdocs, відкриваємо файл config.php, та починаємо виправляти помилки. \$CFG->dbtype = 'mysqli' змінюємо на \$CFG->dbtype = 'mariadb', як показано на рис 4.40.



```

<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype = 'mysqli';
$CFG->dblibrary = 'native';
$CFG->dbhost = 'localhost';
$CFG->dbname = 'moodle';
$CFG->dbuser = 'root';
$CFG->dbpass = '';
$CFG->prefix = 'mdl_';
$CFG->dboptions = array (
    'dbpersist' => 0,
    'dbport' => 3306,
    'dbsocket' => '',
    'dbcollation' => 'utf8mb4_general_ci',
);

$CFG->wwwroot = 'http://test.moodle.com';
$CFG->dataroot = 'C:\\xampp\\moodledata';
$CFG->admin = 'admin';

$CFG->directorypermissions = 0777;

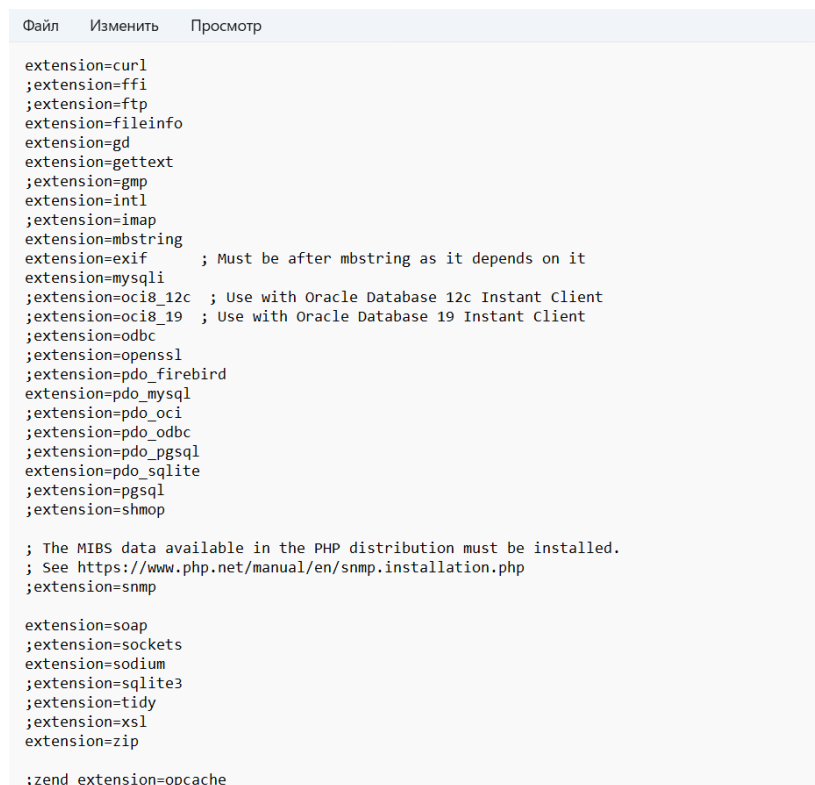
require_once(__DIR__ . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!

```

Рисунок 4.40 – файл config.php.

У програмі ХАМРР, натискаємо config навпроти Apache, та вибираємо файл php.ini, та видаляєм крапку з комою перед таким extension як: zip, gd, intl, soap, sodium, як показано на рис. 4.41. В цьому ж файлі змінюємо max_input_vars = 1000 на max_input_vars = 5000.



```

extension=curl
;extension=ffi
;extension=ftp
extension=fileinfo
extension=gd
extension=gettext
;extension=gmp
extension=intl
;extension=imap
extension=mbstring
extension=exif ; Must be after mbstring as it depends on it
extension=mysqli
;extension=oci8_12c ; Use with Oracle Database 12c Instant Client
;extension=oci8_19 ; Use with Oracle Database 19 Instant Client
;extension=odbc
;extension=openssl
;extension=pdo_firebird
extension=pdo_mysql
;extension=pdo_oci
;extension=pdo_odbc
;extension=pdo_pgsql
extension=pdo_sqlite
;extension=pgsql
;extension=shmop

; The MIBS data available in the PHP distribution must be installed.
; See https://www.php.net/manual/en/snmp.installation.php
;extension=snmp

extension=soap
;extension=sockets
extension=sodium
;extension=sqlite3
;extension=tidy
;extension=xsl
extension=zip

;zend_extension=opcache

```

Рисунок 4.41 – файл php.ini.

Якщо все виправлено, то побачимо такий напис, як на рис. 4.42, натискаємо продовжити йдемо далі.

php_extension	hash	вимагається для встановлення та включення		OK
php_extension	fileinfo	вимагається для встановлення та включення		OK
php_extension	sodium	вимагається для встановлення та включення		OK
php_extension	exif	рекомендується встановити та включити		OK
php_setting	memory_limit	рекомендоване значення виявлено		OK
php_setting	file_uploads	рекомендоване значення виявлено		OK

Інші перевірки

Інформація	Звіт	Модуль	Статус
site not https	якщо цей тест не пройшов, то це вказує на потенційну проблему Виявлено, що ваш сайт не захищений за допомогою HTTPS. Настійно рекомендується перенести свій сайт на HTTPS для підвищення безпеки та поліпшення інтеграції з іншими системами.		Перевірка

Всі серверні залежності відповідають мінімальним вимогам.

Продовжити

Рисунок 4.41 – сторінка налаштування Moodle.

Після встановлення Moodle, переходимо на сторінку реєстрації, як головного адміністратора і заповнюємо всі необхідні поля, як показано на рис. 4.42.

testmoodle.com/user/editadvanced.php?id=2

Встановлення

На цій сторінці вам необхідно заповнити профіль головного адміністратора, який матиме повний контроль над сайтом. Впевніться, що вказали безпечний пароль, поле та відповідний e-mail. Після це ви зможете додавати нових адміністраторів.

Розгорнути всі

Основне

Ім'я входу

admin

Оберіть спосіб ідентифікації

Ручна реєстрація

Ваш пароль повинен мати принаймні 8 символів, принаймні 1 цифру, принаймні 1 букву великого регістру, принаймні 1 функцію верхнього регістру, принаймні 1 спеціальний символ, таке як !, - або #

Новий пароль

Припустити зайняти пароль

Підтвердити

Скопіювати

Ім'я

Олександр

Електронна пошта

robobits22@ukr.net

Видимість електронної пошти

Видно для всіх

Місто

Київ

Країна

Україна

Часовий пояс

Європейський

Опис

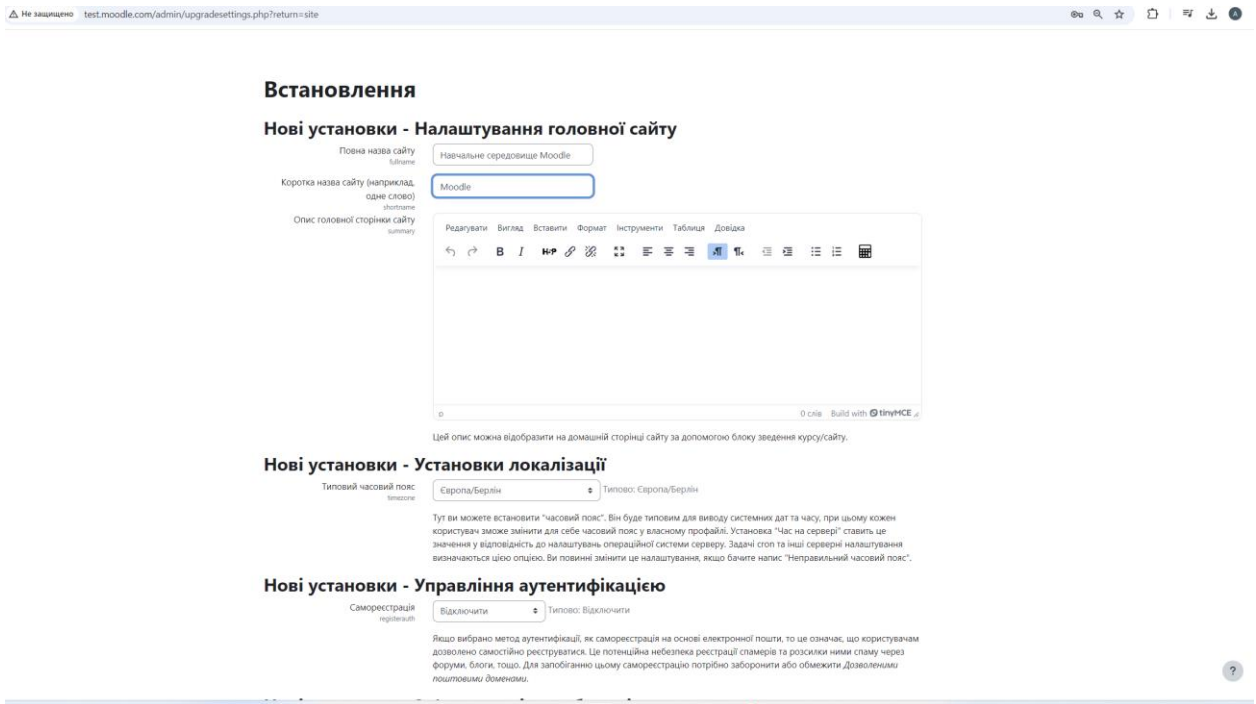


Рисунок 4.42 – сторінка налаштування Moodle.

Після всіх налаштувань, переходимо на головну сторінку Moodle, навчальне середовище успішно встановлено, як показано на рис 4.43.

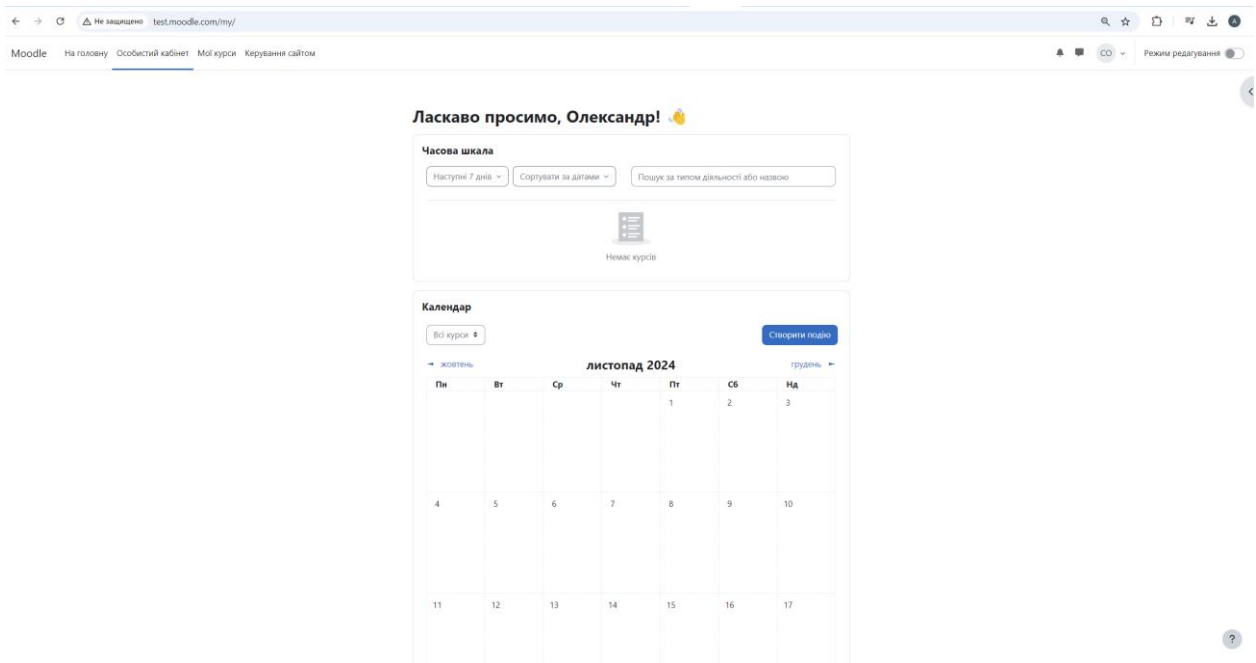


Рисунок 4.43 – головна сторінка Moodle.

Після успішного встановлення Moodle на сервер і входу як адміністратор ви отримали повний контроль над платформою. Тепер ви можете створювати навчальні курси, розміщувати матеріали, текстові, відео, презентації, налаштовувати тести та завдання, а також управляти ролями користувачів, зокрема студентів і викладачів. Система готова до інтеграції з іншими сервісами, що дозволяє створити повноцінне навчальне середовище для ефективної організації освітнього процесу.

ВИСНОВКИ

Інформаційно-навчальне середовище з системою ідентифікації для закладів освіти є важливим кроком у підвищенні безпеки та ефективності навчального процесу. У ході виконання роботи було проведено аналіз сучасних технологій відеоспостереження, систем біометричного контролю доступу та методів ідентифікації особи, що дозволило визначити їхні ключові особливості, переваги та недоліки.

На практичному рівні було здійснено вибір та обґрунтування обладнання для побудови системи безпеки навчального закладу. Вибір обладнання, такого як IP-камери Hikvision DS-2CD2143G0-IS, обґрунтований їхньою надійністю, доступною ціною, підтримкою офіційного програмного забезпечення та сумісністю з іншою продукцією виробника.

Побудова локальної мережі на базі PoE-комутаторів забезпечує живлення та передачу даних по одному кабелю Ethernet, що є технологічно зручним та економічно вигідним рішенням. Центральний сервер виконує роль відеореєстратора для камер, платформи для навчання та управління терміналом розпізнавання облич, що спрощує інфраструктуру та підвищує загальну продуктивність системи. Це дозволяє знизити витрати, оскільки відпадає необхідність у додаткових відеореєстраторах або контролерах для системи контролю доступу.

Запропоноване інформаційно-навчальне середовище з інтегрованими системами безпеки може значно підвищити рівень захищеності учасників навчального процесу, сприяти автоматизації рутинних завдань і забезпечити гнучке управління навчальним процесом. Впровадження таких рішень відповідає сучасним вимогам до цифровізації освіти і створює основу для подальшого розвитку технологій у сфері навчання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Гуцалюк А. В., Кириченко І. М. Інтеграція інформаційних технологій у навчальні процеси [Текст] / А. В. Гуцалюк, І. М. Кириченко. – Київ: Вид-во «Наука», 2021.
2. Анохін С. Ю. Системи відеоспостереження в сучасних умовах [Текст] / С. Ю. Анохін. – Харків: Вид-во ХНУРЕ, 2020.
3. Петрова І. М. Технології розпізнавання облич: алгоритми та практичні рішення [Текст] / І. М. Петрова. – Київ: Основа, 2022.
4. Hikvision. Продукти та рішення для відеоспостереження і контролю доступу [Текст] / Hikvision. – 2023. – Режим доступу: www.hikvision.com.
5. Михайлова І. В. Інформаційно-навчальні середовища: моделювання і впровадження [Текст] / І. В. Михайлова. – Львів: ЛНУ імені Івана Франка, 2021.
6. Moodle Docs. Система управління навчанням Moodle [Текст]. – Режим доступу: <https://docs.moodle.org>.
7. ISO/IEC 19794-5:2011. Biometric Data Interchange Formats – Face Image Data [Текст]. – Geneva: ISO, 2011.
8. Турчак В. І., Ковальчук С. В. Сучасні тенденції у проектуванні навчальних середовищ [Текст] / В. І. Турчак, С. В. Ковальчук. – Київ: НТУУ «КПІ», 2020.
9. Shukla D., Jain A. Face Recognition Systems: An Overview [Text] / D. Shukla, A. Jain // International Journal of Computer Science. – 2020. – Vol. 5, Issue 3.
10. Fielding R. T., Taylor R. N. Architectural Styles and the Design of Network-Based Software Architectures [Text] / University of California, Irvine. – 2000.
11. Jain A. K., Ross A., Nandakumar K. Introduction to Biometrics [Text] / A. K. Jain, A. Ross, K. Nandakumar. – Springer, 2011.
12. Preece J., Sharp H., Rogers Y. Interaction Design: Beyond Human-Computer

Interaction [Text] / J. Preece, H. Sharp, Y. Rogers. – Wiley, 2015.

13. Ahmed S. M., Kamarul B. H. Implementation of Biometric Systems in Education [Text] / S. M. Ahmed, B. H. Kamarul // Journal of Educational Technology. – 2019.

14. Kim H. K., Kim J. H. Video Surveillance Technology for Security Applications [Text] / H. K. Kim, J. H. Kim // Journal of Computer Systems. – 2021.

15. UNESCO. A Guide to Digital Learning Environments [Text]. – Paris: UNESCO, 2021.

16. Український стандарт ДСТУ ISO/IEC 2382-37:2017. Біометрія. Терміни та визначення [Текст]. – Київ: УкрНДІСЕ, 2017.

17. Al-Hassan M., Al-Hussein M. Analyzing the Effectiveness of Facial Recognition in Smart Education Systems [Text] / M. Al-Hassan, M. Al-Hussein // Smart Learning Environments. – 2020.

18. Luu K., Savvides M., Chikkerur S. Face Recognition Systems: Challenges and Recent Advances [Text] / K. Luu, M. Savvides, S. Chikkerur. – IEEE, 2021.

19. Tavani H. T. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing [Text] / H. T. Tavani. – Wiley, 2013.

20. Антоненко В. П. Системи біометричної ідентифікації: принципи роботи та перспективи використання [Текст] / В. П. Антоненко. – Київ: Техніка, 2019.

21. Zhang D., Wang Y. Handbook of Biometrics [Text] / D. Zhang, Y. Wang. – Springer, 2020.

22. Li S. Z., Jain A. K. Handbook of Face Recognition [Text] / S. Z. Li, A. K. Jain. – Springer, 2021.

23. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) Reports [Text]. – 2023. – Режим доступу: <https://www.nist.gov>.

24. Євтух М. Б. Сучасні технології у навчанні: інтерактивні платформи і системи безпеки [Текст] / М. Б. Євтух. – Київ: Освіта, 2022.

25. Zhang Z., Zhao W. Biometrics and Privacy Protection in Digital Education [Text] / Z. Zhang, W. Zhao // Journal of Educational Security. – 2021.
26. Hikvision. Керівництво з встановлення та налаштування систем розпізнавання облич [Текст] / Hikvision. – 2022. – Режим доступу: www.hikvision.com.
27. Бакай О. С. Навчальні платформи: аналіз можливостей Moodle [Текст] / О. С. Бакай. – Тернопіль: ТНПУ, 2021.
28. International Telecommunication Union (ITU). The Role of ICT in Education: Global Reports [Text]. – Geneva: ITU, 2021.
29. Al-Khoury A. M. Biometric Technologies and Applications [Text] / A. M. Al-Khoury. – International Journal of Digital Information. – 2018.
30. Мінченко В. О., Коробов Д. І. Проектування інформаційних систем в освіті [Текст] / В. О. Мінченко, Д. І. Коробов. – Київ: Вид-во НТУУ «КПІ», 2020.
31. Novak J., Gowin D. B. Learning How to Learn: Theory and Practice of Concept Mapping [Text] / J. Novak, D. B. Gowin. – Cambridge University Press, 2015.
32. Eysenbach G. Data Security and Ethical Considerations in Biometric Learning Environments [Text] / G. Eysenbach // Journal of Educational Ethics. – 2022.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ