ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Система контролю і управлінням доступом з використанням відеонагляду та штучного інтелекту»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

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

_____ Дмитро Зеленський
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти
групи АРДМ-62
Дмитро Зеленський

Керівник: Лариса ДАКОВА

Рецензент: _____

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Електронні комунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Зеленському Дмитру Миколайовичу

1. Тема кваліфікаційної роботи: «Система контролю і управлінням доступом з використанням відеонагляду та штучного інтелекту»,
керівник кваліфікаційної роботи Лариса ДАКОВА, к.т.н., доцент,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 р. №320.

2. Строк подання кваліфікаційної роботи 25.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Підвищення ефективності системи контролю і управління доступом.
2. Особливості та параметри інтеграції відеонагляду з технологіями штучного інтелекту.
3. Основні функції та архітектура сучасних СКУД.
4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Аналіз методів забезпечення безпеки та ефективності роботи систем контролю і управління доступом.

2. Оптимізація функціонування СКУД із використанням відеонагляду та технологій штучного інтелекту.

3. Методи підвищення точності ідентифікації, аналізу поведінки та автоматизації процесів управління доступом у сучасних системах.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання 27.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	27.10.24	Викон.
2.	Аналіз методів забезпечення безпеки та ефективності роботи систем контролю і управління доступом	31.10.24	Викон.
3.	Оптимізація функціонування СКУД із використанням відеонагляду та технологій штучного інтелекту	15.11.24	Викон.
4.	Методи підвищення точності ідентифікації, аналізу поведінки та автоматизації процесів управління доступом у сучасних системах	29.11.24	Викон.
5.	Висновки, вступ, реферат	11.12.24	Викон.
6.	Розробка презентації	18.12.24	Викон.

Здобувач вищої освіти Дмитро ЗЕЛЕНСЬКИЙ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Лариса ДАКОВА

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Зеленського Дмитра Миколайовича

на тему: «Система контролю і управлінням доступом з використанням відеонагляду та штучного інтелекту»

Актуальність:

Сучасні системи контролю та управління доступом (СКУД) активно інтегрують технології відеоспостереження та штучного інтелекту (ШІ) для підвищення рівня безпеки та ефективності управління доступом на об'єктах різного призначення.

Використання ШІ дозволяє автоматизувати процеси розпізнавання облич, аналізу поведінки та виявлення підозрілих дій, що сприяє оперативному реагуванню на потенційні загрози.

Поєднання відеоспостереження з інтелектуальними алгоритмами обробки даних забезпечує більш точний контроль за переміщенням осіб та транспортних засобів, а також дозволяє зменшити вплив людського фактора на прийняття рішень.

Позитивні сторони:

1. Проведено аналіз підвищення ефективності систем контролю доступу за рахунок інтеграції відеонагляду і штучного інтелекту.
2. Розглянуто можливості автоматизації процесів ідентифікації та моніторингу, включаючи розпізнавання облич і поведінкових моделей.

Недоліки:

1. Не проведено аналізу продуктивності систем при роботі з великими обсягами відеоданих у реальному часі.
2. Не розглянуто альтернативи інтеграції різних технологій, зокрема інших методів біометричної аутентифікації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач ЗЕЛЕНСЬКИЙ Дмитро Миколайович заслуговує присвоєння кваліфікації: «Магістр з телекомунікацій та радіотехніки».

Рецензент: _____

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

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Зеленський Д.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Система контролю і управлінням доступом з використанням відеонагляду та штучного інтелекту

Кваліфікаційна робота і рецензія додаються.

В.о. директора ННІТ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Зеленський Дмитро Миколайович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Зеленського Дмитра Миколайовича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Лариса ДАКОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Зеленський Д.М.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 96 стор., 40 рис., 7 табл., 18 дж.

Мета роботи – підвищення ефективності системи контролю і управління доступом за рахунок впровадження технологій відеоспостереження та штучного інтелекту, зокрема вдосконалення алгоритмів розпізнавання облич, аналізу поведінки і прийняття рішень.

Об'єкт дослідження – процес управління доступом і моніторингу територій з використанням інтелектуальних відеоаналітичних систем.

Предмет дослідження – моделі та алгоритми автоматизації та підвищення точності роботи СКУД на основі використання технологій відеонагляду та штучного інтелекту.

Короткий зміст роботи: у магістерській роботі досягнуто наступних результатів: у першому розділі проаналізовано основні аспекти штучного інтелекту, включаючи його історичний розвиток та ключові етапи становлення технології. Розглянуто галузі застосування ШІ, а також вразливості й недоліки, що можуть впливати на його ефективність. У другому розділі досліджено СКУД на базі ШІ, розглянуто її основні завдання, технологічні особливості сучасних систем, їхні компоненти, застосування біометричних технологій та аксесуарів. У третьому розділі розглянуто процес проєктування та впровадження систем безпеки на конкретному об'єкті. Описано ключові етапи, зокрема проєктування серверної кімнати, розробку систем відеонагляду та контролю доступу. Детально висвітлено налаштування й монтаж обладнання для відеонагляду та охоронної системи. Також проведено розрахунок загальної вартості впроваджених систем безпеки.

КЛЮЧОВІ СЛОВА: ШТУЧНИЙ ІНТЕЛЕКТ; ВІДЕОНАГЛЯД, СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ, БЕЗПЕКА, ДАТЧИК, ОХОРОНА, ПРОЄКТУВАННЯ

ABSTRACT

Text part of the master's qualification work: 96 pages, 40 pictures, 7 table, 18 sources.

The purpose of the work - high efficiency of the access control and control system through the introduction of video surveillance and artificial intelligence technologies, in particular, improved face recognition algorithms, behavior analysis and decision-making.

Object of research – access control and territory monitoring process using intelligent video analytics systems.

Subject of research – models and algorithms for automation and improving the accuracy of ACS operation based on the use of video surveillance and artificial intelligence technologies.

Summary of the work: the following results were achieved in the master's thesis: the first section analyzes the main aspects of artificial intelligence, including its historical development and key stages in the formation of technology. The fields of application of AI are considered, as well as vulnerabilities and disadvantages that can affect its effectiveness. In the second section, ACS based on AI is investigated, its main tasks, technological features of modern systems, their components, the use of biometric technologies and accessories are considered. The third section discusses the process of designing and implementing security systems at a particular facility. The key stages are described, in particular the design of the server room, the development of video surveillance and access control systems. The settings and installation of equipment for video surveillance and security system are covered in detail. The total cost of the implemented security systems was also calculated.

KEYWORDS: ARTIFICIAL INTELLIGENCE; VIDEO SURVEILLANCE, ACCESS CONTROL AND CONTROL SYSTEM, SAFETY, SENSOR, SECURITY, DESIGNING

ЗМІСТ

ВСТУП 9

1. ШТУЧНИЙ ІНТЕЛЕКТ. ІСТОРІЯ ТА ПРАКТИКА ВИКОРИСТАННЯ 10

1.1 Розвиток штучного інтелекту: історичний огляд 10

1.2 Провідні галузі застосування штучного інтелекту 14

1.3 Експлуатація ШІ в сфері безпеки 19

1.4 Вразливі місця та недосконалості ШІ 22

2. СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ ШІ 26

2.1 Основні завдання СКУД 26

2.2 Технологічні особливості сучасних СКУД 30

2.2.1 Структурні компоненти систем управління доступом 30

2.2.2 Біометрія в системах безпеки 36

2.2.3 Аксесуари для СКУД 41

2.3 Особливості монтажу СКУД 44

2.4 Інтеграція ШІ в автоматизовані системи управління доступом 49

3. ПОБУДОВА СХЕМИ ТА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПУ З ВИКОРИСТАННЯМ ШІ ТА ВІДЕОНАГЛЯДУ 53

3.1 Інформація про об’єкт 53

3.2 Проєктування систем безпеки 58

3.2.1 Серверна кімната 58

3.2.2 Розробка системи відеонагляду 60

3.2.3 Розробка системи контролю доступом 65

3.3 Налаштування та монтаж обладнання з відеонагляду 69

3.4 Налаштування та монтаж обладнання охоронної системи 84

3.5 Розрахунок загальної вартості системи 89

ВИСНОВКИ 93

ПЕРЕЛІК ПОСИЛАНЬ 95

ДЕМОНСТРАТИВНІ МАТЕРІАЛИ 97

ВСТУП

Сучасні виклики у сфері інформаційної безпеки, охорони об’єктів та забезпечення контролю доступу вимагають використання інноваційних підходів. В наш час швидкий розвиток технологій штучного інтелекту (далі – ШІ) та комп’ютерного зору відкриває безліч нових можливостей для вдосконалення систем відеоспостереження та управління доступом, що робить їх незамінним інструментом при побудові та організації безпекових заходів у повсякденному житті. Поєднання цих технологій дозволяє автоматизувати процеси аналізу відео, ідентифікації об'єктів і суб'єктів, а також прийняття рішень у режимі реального часу. Вивчення удосконалених систем контролю доступу з використанням ШІ є актуальним напрямком досліджень, оскільки воно сприяє підвищенню ефективності охорони об’єктів, мінімізації людського фактора та швидкому реагуванню на потенційні загрози.

Дана дипломна робота присвячена дослідженню та розробці системи контролю і управління доступом (далі – СКУД) з використанням штучного інтелекту та відеоспостереження.

Метою даної роботи є розробка концепції та практичних підходів до створення СКУД з інтеграцією відеоспостереження, яка базується на технологіях штучного інтелекту. В роботі розглядаються основні принципи побудови цих систем, їхні функціональні можливості, перспективи впровадження, можливі ризики, недоліки та випробовування з якими можуть стикатись кінцеві користувачі.

Актуальність теми обумовлена необхідністю створення інтелектуальних систем безпеки, здатних адаптуватися до мінливих умов та забезпечувати високий рівень надійності за мінімальних витрат ресурсів. У роботі також аналізуються переваги та потенційні ризики, пов’язані з використанням ШІ у сфері контролю доступу. Ця магістерська робота спрямована на внесок у розвиток систем безпеки нового покоління, які можуть стати основою для широкого впровадження в різних галузях – від корпоративного середовища до критично важливих інфраструктур.

1. ШТУЧНИЙ ІНТЕЛЕКТ. ІСТОРІЯ ТА ПРАКТИКА ВИКОРИСТАННЯ

1.1 Розвиток штучного інтелекту: історичний огляд

Поняття штучного інтелекту з’явилося ще в 1950-х роках, і основна проблематика з того часу змінилась не суттєво. Наукова фантастика познайомила світ з концепцією роботів із штучним інтелектом і на той час зародок штучного інтелекту був асимільований ентузіастами того періоду.

Одним з таких людей був Алан Тюрінг, молодий британський ерудит, який досліджував математичні можливості штучного інтелекту. Тюрінг припускав, що якщо люди використовують розум для розв'язання завдань та прийняття рішень, то і машини повинні робити те ж саме. Ця ідея встала в основу його статті 1950 року "Обчислювальна техніка та інтелект", в якій він описав, як створювати розумні машини та як перевіряти їх інтелект.

Перш за все, для матеріалізації ідей Тюрінга були необхідні значні зміни в комп'ютерних технологіях, через те, що до 1949 року в комп'ютерах була відсутня критична вимога до інтелекту – вони не могли зберігати команди та були призначені виключно для виконання. Крім того, на початку 1950-х обчислювальна техніка була надзвичайною розкішшю. Оренда комп'ютера могла коштувати до 200 000 доларів на місяць, що робило його доступним лише для престижних університетів та великих технологічних компаній. Розробка штучного інтелекту потребувала не лише підтвердження концепції, а й підтримки інвесторів, щоб переконати джерела фінансування в її доцільності.

Дартмутська конференція 1956 року є визначальною подією в історії ШІ. Це був літній дослідницький проєкт, який відбувся в 1956 році у Дартмутському коледжі в Нью-Гемпширі, США. Це була перша конференція, яка об’єднала дослідників з різних галузей дослідження – інформатики, математики, фізики та інших – з метою дослідити потенціал синтетичного інтелекту (терміну ШІ ще не існувало). Участь взяли Джон Маккарті, Марвін Мінський та інші визначні

науковці й дослідники. Учасники конференції обговорили широкий спектр тем, пов’язаних з ШІ, серед яких обробка природної мови, розв’язання задач та машинне навчання. Вони також проклали дорожню карту для дослідження ШІ, включно з розробкою мов програмування та алгоритмами для створення інтелектуальних машин. Ця конференція вважається визначальною подією в історії ШІ, оскільки тоді зародилась галузь та поняття «Штучний інтелект». Дартмутська конференція мала значний вплив на загальну історію ШІ. Вона допомогла започаткувати галузь дослідження ШІ та сприяла розвитку нових технологій. Учасники виклали бачення щодо ШІ, що включало створення інтелектуальних машин, які б могли міркувати, думати та спілкуватися, як люди. Після конференції Джон Маккарті та його колеги розробили першу мову програмування ШІ – LISP. Ця мова стала основою досліджень ШІ й існує досі. Однією з найважливіших спадщин Дартмутської конференції є розробка тесту Тюрінга. Тюрінг запропонував ідею тесту, який визначатиме, чи машина здатна демонструвати поведінку, яку не розрізнити від людської. Цю концепцію обговорили на конференції та вона стала центральною ідеєю в галузі дослідження ШІ. Сьогодні тест Тюрінга залишається важливим орієнтиром для вимірювання прогресу досліджень ШІ.

1957 – 1974 роки стали періодом розквіту штучного інтелекту. Комп’ютери могли зберігати все більше інформації, ставали швидшими, дешевшими та доступнішими. Так само, покращувались алгоритми машинного навчання – комп’ютерні програми все краще справлялись з розв’язанням задач, а в 1966 році було навіть створено першого віртуального співрозмовника – Елізу, яка стала прототипом сучасних чат-ботів та віртуальних асистентів. Діалогове вікно «Елізи» зображене на рис. 1.1.

Про перші досягнення алгоритмів штучного інтелекту виявили численні труднощі на шляху до справжнього машинного інтелекту. Найзначнішою проблемою стала недостатня обчислювальна потужність. Наприклад, для того щоб діяти як віртуальний співрозмовник, машина повинна була запам'ятовувати значення багатьох слів та розуміти їх значення в різних комбінаціях. Комп’ютери того часу не мали змоги зберігати необхідні обсяги інформації і обробляти їх зі

швидкістю, достатньою для цих завдань. Таким чином, високий інтерес поступово змінився розчаруванням, фінансування зменшилось, а кількість досліджень знизилася, внаслідок чого період з 1974 року до початку 1980-х років отримав назву першої "зими" штучного інтелекту.

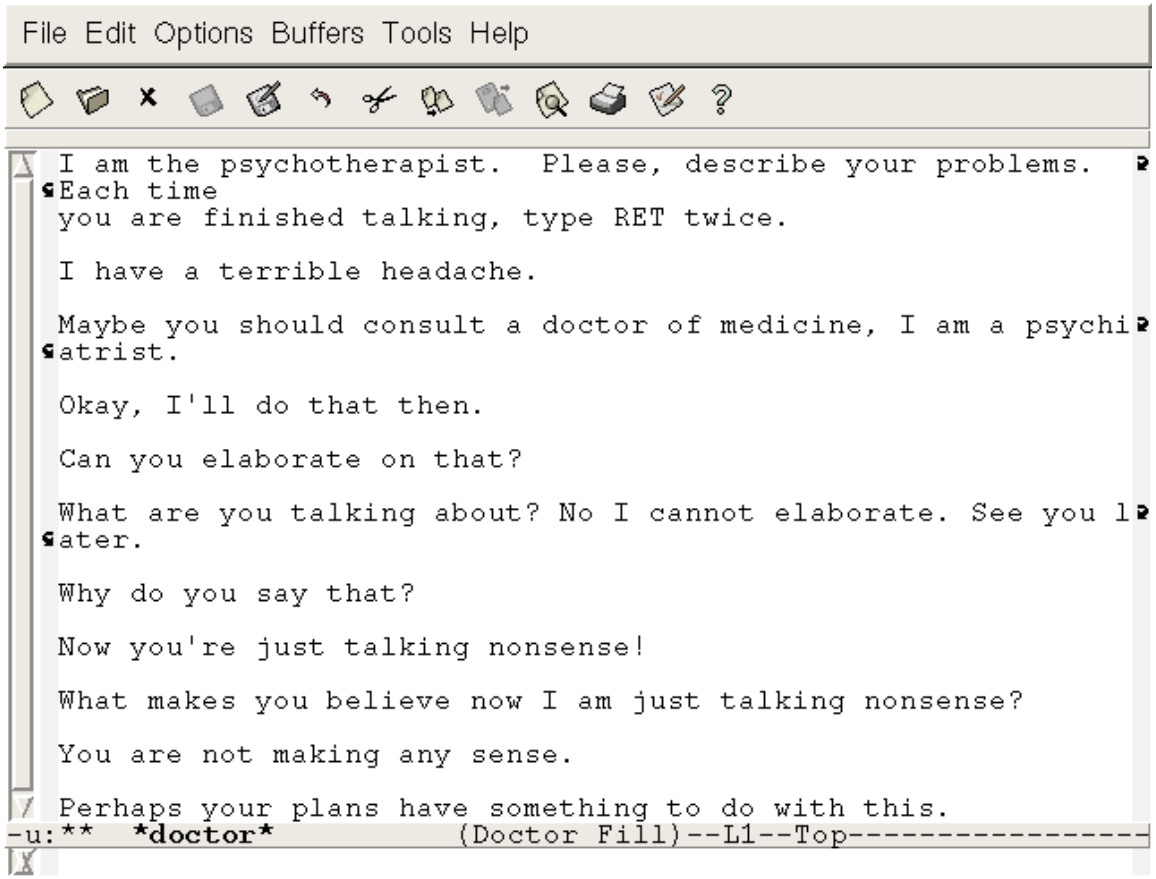


Рисунок 1.1 Діалогове вікно програми «ELIZA»

Після цього настала коротка пауза у відновленні інтересу до технологій машинного навчання, коли з'явилися перші експертні системи, здатні імітувати процес прийняття рішень, характерний для людей-експертів. Японія та Великобританія, зацікавлені в таких технологіях, розпочали активне фінансування цієї галузі. Однак, вже у 1987 році розпочалася друга "зима" штучного інтелекту, що тривала до 1993 року. Протягом 1990-х і 2000-х років штучний інтелект продовжував розвиватися, незважаючи на відсутність державного фінансування та значної уваги з боку суспільства. Велику роль у розвитку технологій машинного

навчання стали відігравати великі технічні компанії, які досягли значних успіхів у створенні розумних машин. Зокрема, у 1997 році комп'ютерна програма від IBM перемогла діючого чемпіона світу з шахів Гарі Каспарова[1]. У тому ж році в Windows було інтегровано програмне забезпечення для розпізнавання мови, розроблене компанією Dragon Systems, а у 2001 році команда дослідників з MIT представила першого соціального робота на ім'я Kismet, який навчався розпізнавати людські емоції. Здавалося, що немає жодного завдання, яке б не під силу було розв'язати машинам.

У 2010-х роках спостерігався значний прогрес у обробці природної мови, що дало змогу розробляти дедалі складніші й розумніші користувацькі інтерфейси, такі як Siri, Google Assistant і Amazon Alexa. Також було проведено велику кількість досліджень у сфері машинного навчання, нейронних мереж і глибинного навчання, що сприяло створенню нових моделей із високою точністю у розпізнаванні зображень і голосу.

Останнім досягненням у сфері створення штучного інтелекту став людиноподібний робот на ім’я Софія, він був створений гонконзькою компанією Hanson Robotics і досяг досить високої популярності в засобах інформації завдяки своїй подібності до людини (за основу її зовнішності було взято акторку Одрі Гепберн), набору мімічних реакцій із 60 емоцій і неоднозначним висловлюванням під час публічних дискусій. Деякі експерти заперечують, що робота можна назвати штучним інтелектом. За словами керівника лабораторії штучного інтелекту компанії «Facebook», робот Софія – це чат бот, який за допомогою технології розпізнавання мови Google розпізнає питання за ключовими словами та підбирає найбільш слушну відповідь із визначеної бази.

Як виявилось – основна проблема комп'ютерної пам'яті, яка стримувала нас тридцять років тому, більше не є суттєвою. Закон Мура, який стверджує, що обсяги пам'яті та швидкість комп'ютерів подвоюються щорічно, нарешті досяг рівня, а в багатьох випадках навіть перевищив наші потреби.

1.2 Провідні галузі застосування штучного інтелекту

Сьогодні концепція використання технологій ШІ набуває великої популярності. Такі системи використовують різноманітні алгоритми, методи машинного навчання, глибокого навчання, нейронних мереж, генерацію контенту та інші підходи для аналізу даних, прийняття рішень, розпізнавання образів, мови та вирішення складних задач у реальному часі. Вони здатні імітувати розумові функції: навчання, сприйняття й аналіз природної мови, планування та взаємодія з оточенням. Хоча штучний інтелект і може спричинити скорочення робочих місць, але він здатен збільшити глобальний ВВП. За результатами дослідження Goldman Sachs[2], це зростання становитиме 7% (або майже на $7 трлн) упродовж наступних 10 років. Крім того, ШІ підвищить темпи зростання продуктивності на 1,5%.

На сьогоднішній день технології штучного інтелекту використовуються практично в усіх відомих звичайній людині сферах: автоматизація бізнесу, роботи державних установ, виробництва, торгівлі, логістики, освіти, медицини та навіть у повсякденному житті. Ефективність ШІ постійно зростає завдяки вдосконаленню нейромереж і збільшенню обсягів пам’яті. Спочатку передбачалося, що ШІ виконуватиме лише базові завдання, переклад текстів, розпізнавання об’єктів і слів. Однак тепер зрозуміло, що його потенціал майже необмежений, і він далі прогресує в своєму розвитку та інтеграції в різні аспекти нашого життя. Нижче в табл. 1.1 будуть наведені сфери в яких застосовується ШІ та реальний приклад використання.

Таблиця 1.1

Сфери застосування ШІ

Креативні індустрії (маркетинг, медіа)	Користувачі можуть ставити запитання чат-ботам й швидко отримувати відповіді, генерувати тексти для статей, соцмереж, складати вірші та оповідання тощо. ШІ може надавати персоналізовані рекомендації щодо контенту, виявляти шахрайські дії з користувацькими акаунтами (наприклад, аналізувати дані й знаходити аномалії в діях клієнтів), а також передбачати поведінку, що спрощує ухвалення стратегічних рішень, планування контенту. Штучний інтелект уже може виконувати багато завдань менеджерів із маркетингу, і робити це значно швидше. Особливо перспективним є застосування ШІ для таргетованих рекламних кампаній, коли потрібно передбачати поведінку споживача з великою точністю.
Фінанси	Сучасні інструменти на базі ШІ здатні за лічені секунди обробляти величезні обсяги даних, що в свою чергу дозволяє компаніям приймати обґрунтовані рішення в реальному часі, що критично важливо в умовах швидко змінюваного ринку, а також передчасно виявляти шахраїв і оптимізувати свої інвестиції.

Продовження таблиці 1.1

Медицина	Для цієї сфери застосування технологій штучного інтелекту особливо актуальні його здібності збирати, аналізувати інформацію та робити логічні висновки. Завдяки цьому його можна використовувати для встановлення діагнозу, реєстрації даних, виконання функції асистента лікаря. Крім цих обов'язків ШІ можна доручити визначення схильності пацієнта до розвитку конкретних патологій, прогнозування перебігу захворювань хронічного типу, раннє виявлення хвороби.
Освіта	Сьогодні перед освітою стоїть важливе завдання впровадження адаптивного навчання та систем прокторингу[3]. Штучний інтелект покликаний автоматизувати процес підбору навчальних матеріалів і методів викладання, які максимально відповідають індивідуальним потребам кожного учня. Це дозволить зробити навчання більш доступним і ефективним для учнів із різними здібностями та стилями сприйняття інформації.

Продовження таблиці 1.1

Освіта	Системи прокторингу використовуються для забезпечення чесності під час іспитів. Вони контролюють поведінку студентів, аналізують дані з камер і виявляють будь-які відхилення чи спроби обману, які можуть бути непомітними для людини. Це особливо актуально в умовах дистанційного навчання, де студенти часто намагаються обійти технологічні бар'єри. Проте не всі аспекти освіти можуть бути автоматизовані. Велика роль у процесі навчання залишається за викладачем. Навіть найсучасніший ШІ поки що не може повністю замінити живого педагога, оскільки освіта – це не лише передача знань, але й розвиток особистості, який вимагає людського підходу.
Транспорт і логістика	Машинне навчання вже допомогло зробити управління ланцюжком постачання безперебійним процесом. Роботи на складах сортують і пакують товари, а алгоритми ШІ будують оптимальні маршрути доставки замовлень.

Продовження таблиці 1.1

Транспорт і логістика	На черзі – революція автономних транспортних засобів. Tesla, Uber, Volvo, Volkswagen та інші компанії активно вкладаються в інновації, які згодом замінять водіїв-людей. Також вже сьогодні у різних країнах досліджують використання ШІ для оптимізації руху громадського транспорту та управління світлофорами.

Також ШІ має великий потенціал застосовуватися в різних галузях, які можуть здатися неочевидними. Менш популярні області, де ШІ може знайти своє застосування наведені нижче в табл. 1.2.

Таблиця 1.2

Незвичайні сфери застосування ШІ

Спорт	ШІ має великий потенціал для аналізу масштабних даних, пов’язаних зі спортивними подіями, тренувальними процесами та фізичною підготовкою спортсменів, що може позитивно впливати на їх результати.
Охорона навколишнього середовища	Штучний інтелект здатний забезпечувати моніторинг стану довкілля, прогнозувати кліматичні зміни, підвищувати енергоефективність та оптимізувати процеси управління відходами.

Продовження таблиці 1.2

Туризм	Може використовуватися для персоналізації сервісів, надання рекомендацій щодо вибору подорожей і готелів, автоматичного перекладу, а також аналізу великих обсягів даних про клієнтів.
Мистецтво	Використовується для створення музики, літератури та інших видів творчості. Він здатний аналізувати різні стилі, генерувати нові композиції та створювати унікальні художні роботи.
Археологія	ШІ може допомогти у автоматичному перекладі текстів, аналізі лінгвістичних особливостей мови, відновленні пошкоджених артефактів та дослідженні історичних джерел.

1.3 Експлуатація ШІ в сфері безпеки

Штучний інтелект змінює ландшафт безпеки, перетворюючи системи спостереження на проактивні, інтелектуальні структури. Завдяки можливостям машинного навчання, комп'ютерного зору та аналізу великих обсягів даних, інтеграція ШІ в системи безпеки відкриває нові перспективи для автоматизації й оптимізації процесів, які раніше вимагали значних людських ресурсів. Однією з основних переваг використання ШІ є здатність таких систем працювати у режимі реального часу, забезпечуючи моніторинг та аналіз ситуації без участі оператора.

Але разом із зростанням можливостей зростає і складність, особливо стосовно питань конфіденційності. Інтеграція ШІ у системи фізичної безпеки вимагає етичного підходу, що передбачає врахування приватності користувачів ще

на етапі проєктування. Виробники й інтегратори рішень усе більше орієнтуються на відповідальне використання ШІ, приділяючи увагу захисту персональних даних і виконанню нормативних вимог. Функції, засновані на штучному інтелекті, включають технології, які мінімізують ризики витоку даних і сприяють дотриманню безпеки. Наприклад, об'єктний захист конфіденційності дозволяє контролювати доступ до чутливої інформації, забезпечуючи її надійний захист без шкоди для ефективності системи. У таких рішеннях закладається фундамент відповідальності, де захист приватності є не лише технічним завданням, а й ключовим принципом. Системи на основі ШІ покликані не лише підвищувати ефективність безпеки, але й забезпечувати довіру користувачів.

Гарною можливістю проявити себе штучному інтелекту в ролі «охоронця» – є його участь в боротьбі з кібератаками. Незважаючи на те, що постійно з’являються нові методи атак, організації часто зосереджують свої зусилля на наступному шкідливому (зловмисному) програмному забезпеченні. Воно може ховатися в законних джерелах або приєднуватися до файлів. Існує багато типів зловмисного програмного забезпечення для виконання різноманітних цілей кіберзлочинності, таких як реплікація або шифрування файлів, блокування законного доступу користувачів або викрадення конфіденційних даних. Хоча багато кібератак походять із зовнішніх джерел, в організаціях існують навмисні та ненавмисні загрози. Ці люди можуть мати доступ до мережі та конфіденційних даних і можуть вирішити продати їх заради фінансової вигоди. Ненавмисні внутрішні загрози часто пов’язані з недбалістю. Нові кіберзагрози постійно вдосконалюються, тому організації повинні використовувати передові технології, щоб протистояти цим загрозам.

Штучний інтелект може змінити спосіб боротьби з кіберзагрозами, створивши більш передбачуваний ландшафт кібербезпеки. Спочатку, ШІ використовував прості правила для відстеження мережевого трафіка та дій користувачів. Ці правила, створені людьми, допомагали виявляти підозрілу активність, але мали обмеження. Згодом, наприкінці 20-го століття, ШІ став більш розвиненим завдяки прогресу в машинному навчанні. Тепер він може самостійно

встановлювати правила, зменшуючи потребу в ручному введенні даних. Використання алгоритмів глибокого навчання дозволило йому ефективніше виявляти потенційні загрози, роблячи кібербезпеку більш надійною. Сучасний генеративний штучний інтелект забезпечує багато переваг у сфері кібербезпеки, від автоматизації повторюваних завдань і зменшення людських помилок до використання прогнозової аналітики для підтримки виявлення загроз, бо він постійно навчається на основі попереднього досвіду, адаптуючи свої захисні механізми до нових загроз.

Щодо фізичної безпеки – камери зі штучним інтелектом виявляють потенційні інциденти безпеки з неперевершеною точністю. Виявляючи випадки порушення, такі як проникнення людей у заборонені зони, залишені без нагляду об’єкти або підозрілу поведінку, ці системи значно зменшують кількість помилкових спрацьовувань і дають змогу швидко реагувати. Інтеграція камер на базі ШІ з іншими системами безпеки представляє значний крок вперед в інтелектуальних рішеннях безпеки. Використання алгоритмів ШІ дозволяє камерам точно виявляти різноманітні події безпеки, такі як виявлення руху в неправильному напрямку, виявлення осіб, що безцільно вештаються і розпізнавання підозрілих транспортних засобів, зі значно вищим рівнем точності. У разі виявлення таких подій камери зі штучним інтелектом можуть оперативно запускати відповідні тривоги.

Захист конфіденційності має бути інтегрованим у технології вже на етапі їх проєктування, а не залишатися додатковою опцією. Цей підхід дозволяє створювати системи, які відповідають сучасним вимогам до безпеки, забезпечуючи одночасно високу ефективність та дотримання прав користувачів. Співпраця з організаціями, що слідкують за впровадженням таких нормативних актів, як GDPR чи Закон ЄС про штучний інтелект[4], є важливою складовою цього процесу, такі компанії демонструють не лише прозорість і відповідальність, а й інтегрують чіткі принципи етики у процес створення своїх рішень. Надалі одним з основних напрямів у розвитку систем безпеки є гармонійне поєднання штучного інтелекту з традиційними системами відеоспостереження. Однак це має відбуватися з

урахуванням довгострокової відповідності стандартам захисту даних, бо майбутнє фізичної безпеки залежить від інноваційного підходу до її реалізації, де технології не тільки підвищують рівень захисту, але й формують довіру з боку суспільства.

З огляду на поточну ситуацію в країні, перспективи використання штучного інтелекту в сфері безпеки для України є значущими, особливо в контексті сучасних викликів і зростаючої ролі цифрових технологій. На даний момент ШІ активно використовується для захисту критично важливої інфраструктури, банківських систем, державних реєстрів і персональних даних громадян. У військовій сфері його застосовують для аналізу даних розвідки, автоматизації управління дронами та вдосконалення систем протиповітряної оборони.

1.4 Вразливі місця та недосконалості ШІ

На перший погляд може здаватися, що на даному етапі розвитку ШІ несе в собі лише користь та є постачальником гарних вражень, проте у кожного явища, чи-то події є зворотний бік, попри великий та цікавий потенціал ШІ, для його нешкідливого та відповідального використання важливо усвідомлювати й враховувати його обмеження та ризики.

З проблемами штучного інтелекту можуть стикатися як звичайні люди, так і керівники підприємств, заможні особи або посадовці, відповідальні за ухвалення важливих рішень. Інтеграція штучного інтелекту в бізнес-операції вимагає значних початкових інвестицій. Це стосується придбання передових технологій, розвитку надійної інфраструктури та найму кваліфікованих фахівців, здатних розробляти, впроваджувати та обслуговувати системи штучного інтелекту. Малі та середні підприємства, зокрема, можуть вважати ці початкові витрати непомірно високими, що може стати потенційною перешкодою для широкого впровадження. Заохочення людських лінощів.

ШІ робить людей лінивими, автоматизуючи більшу частину роботи за допомогою своїх додатків[5]. Легкість, з якою виконуються рутинні завдання, може викликати почуття самозаспокоєності, що потенційно знижує схильність

людей до активної участі у вирішенні проблем, критичного мислення або прагнення до постійного вдосконалення.

Зараз існує суспільна думка, що ШІ може забрати велику частину робочих місць. І дійсно, можливості ШІ у автоматизації – підвищують ефективність, що веде за собою все менше втручання людини, що в свою чергу спричиняє серйозну проблему в стандартах зайнятості. Завдання, які є рутинними і легко автоматизуються, можуть призвести до зменшення шансів на працевлаштування на певні посади. Основними представниками таких професій є люди з обмеженими можливостями, яким і так нелегко працевлаштуватись. Є підозра, що в майбутньому переважна кількість організацій прагнутиме замінити мінімально кваліфікованих працівників роботами зі штучним інтелектом, які можуть виконувати аналогічну роботу з більшою ефективністю.

Безсумнівно, машини перевершують людей у виконанні завдань, що потребують максимальної ефективності, проте вони не здатні замінити людський зв’язок, який є основою згуртованої команди. Штучний інтелект обмежений у розумінні складного людського контексту, що впливає на його ефективність у ряді ситуацій. Машинам складно інтерпретувати емоції, культурні особливості та соціально-етичні дилеми. Це обмеження стає критичним у випадках, коли для прийняття правильних рішень необхідне глибоке розуміння людських аспектів.

Також, не зважаючи на те, що штучний інтелект демонструє високу майстерність у обробці даних та виконанні чітко заданих завдань, йому бракує творчості й інтуїції, які є невід’ємною частиною людського прийняття рішень. Машини здатні виконувати лише ті функції, для яких вони спроектовані або запрограмовані, а все, що виходить за ці межі, може призводити до помилок або нерелевантних результатів.

Надмірна довіра до систем штучного інтелекту призводить до залежності, яка несе в собі потенційні пастки. Несправності або помилки в системах ШІ можуть призвести до операційних збоїв, що ставить під сумнів надійність процесів, керованих штучним інтелектом. Необхідно досягти ретельного балансу, щоб ШІ доповнював людські здібності, не ставлячи під загрозу загальну стійкість системи.

Існує декілька правил та тез, що розкривають правильний шаблон поведінки з системами штучного інтелекту:

а) хоча ШІ може бути дуже корисним, важливо аналізувати та перевіряти отриману від нього інформацію. Річ у тім, що штучний інтелект не завжди розуміє задачу, яку йому ставлять. Це залежить від точності запитання, тож потрібно бути готовим до того, що його відповідь вас розчарує або навіть введе в оману;

б) перш ніж звертатися до штучного інтелекту за допомогою, варто спробувати вирішити задачу самостійно. Якщо надмірно покладатися на його підтримку та знання, є ризик втратити здатність думати самостійно при виконанні базових задач;

в) штучний інтелект знає лише те, що в нього заклали розробники, тож він обмежений в ухваленні оптимальних рішень. Тому потрібно бути обачливим і обережними при його використанні, враховувати, але не покладатися на його відповіді на 100%;

г) штучний інтелект не завжди може повністю врахувати людські емоції, контекст або інші нюанси, що можуть мати значення для прийняття правильних рішень, особливо коли йдеться про етичні аспекти.

У 2020-х роках швидкий розвиток моделей генеративного штучного інтелекту на основі глибокого навчання, зокрема тих, що перетворюють текст на зображення, викликав питання про те, як законодавство щодо авторського права регулює навчання та використання таких технологій[6]. Через обмежену судову практику, ця сфера залишається невизначеною, і основне питання полягає в тому, чи має місце порушення авторських прав, коли ШІ навчається або використовується. Популярні моделі глибокого навчання зазвичай тренуються на великих наборах медіафайлів з інтернету, багато з яких захищені авторським правом. Оскільки процес збору даних часто включає копіювання таких творів, це може порушувати право власника авторського права контролювати відтворення його роботи, якщо використання не підпадає під винятки, передбачені законодавством конкретної юрисдикції. Крім того, використання вихідних даних для генерації може також порушувати авторське право, і розробники ШІ можуть

бути притягнуті до «спільної відповідальності» за таке порушення. У деяких випадках моделі глибокого навчання можуть «запам'ятовувати» частини свого навчального набору і відтворювати їх під час генерації, що також може вважатися порушенням авторських прав. Розробники зазвичай вважають це небажаним (оскільки це є ознакою перенавчання), і є суперечки щодо того, наскільки це поширено в сучасних системах. Компанія OpenAI[7] стверджує, що «правильно налаштовані системи ШІ зазвичай не відтворюють в своєму вихідному коді незмінені дані з конкретних творів». Під час навчання статистичних моделей, на яких працює ШІ, ці системи можуть імітувати стиль окремих авторів, що присутні в навчальних даних. Наприклад, генеративна модель зображень, як-от Stable Diffusion[9], може відтворювати стилістичні особливості художника, як Пабло Пікассо (включаючи мазки пензля, використання кольору, перспективу тощо), і користувач може створити запит типу «астронавт на коні в стилі Пікассо», щоб змусити модель згенерувати нове зображення, застосовуючи цей стиль до будь-якого об'єкта. Однак загальний стиль художника зазвичай не підпадає під захист авторським правом.

2. СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ НА БАЗІ ШІ

2.1 Основні завдання СКУД

Системи контролю та управління доступом виконують важливу функцію постачання безпеки та організації доступу на об’єкти. Завдяки своїм багатофункціональним можливостям, вони знаходять застосування в різних галузях – від комерційних офісів до стратегічних об’єктів. Ідентифікація осіб є найголовнішою функцією та задачею СКУД, вона дозволяє системі визначити, хто саме намагається отримати доступ до об'єкта чи зони. Для цього використовуються різноманітні ідентифікатори: від простих магнітних карт і PIN-кодів до сучасних біометричних методів. Біометричні технології, включаючи розпізнавання облич, відбитків пальців і райдужної оболонки ока, забезпечують високий рівень точності та унеможливлюють передачу ідентифікатора іншій особі. Згідно з дослідженнями, такі системи здатні досягати точності ідентифікації до 99%, що робить їх незамінними для використання у середовищах із підвищеними вимогами до безпеки. Контроль доступу дозволяє налаштувати гнучкі права доступу для кожного користувача залежно від його ролі, часу доби або рівня дозволів. Це дуже зручно та актуально для великих організацій, де співробітники працюють у різних відділах і повинні мати доступ лише до певних зон. Системи також можуть обмежувати доступ у реальному часі, наприклад, під час надзвичайних ситуацій або виявлення порушень безпеки.

Ведення журналу подій забезпечує ретельний контроль над усіма діями, пов’язаними з доступом, СКУД автоматично фіксує інформацію про те, хто, коли і куди входив або намагався увійти. Ці дані зберігаються у захищених базах і можуть бути використані для аналізу поведінки, розслідування інцидентів або складання звітів. У поєднанні з аналітичними алгоритмами, журнал подій дозволяє виявляти швидко виявляти потенційні загрози і допомагати швидше їх усувати.

Інтеграція з суміжними системами безпеки дозволяє створювати комплексні рішення, що об’єднують СКУД із відеоспостереженням, сигналізацією, пожежною безпекою чи системами розумних будинків. Такий підхід дозволяє оперативно реагувати на загрози, наприклад, активувати блокування дверей у разі пожежної тривоги або включати камери у разі несанкціонованого доступу.

Моніторинг присутності в зоні контролю забезпечує постійне відстеження переміщень співробітників або відвідувачів. Ця функція дозволяє отримувати точні дані про кількість осіб на об’єкті, що особливо важливо під час евакуацій або надзвичайних ситуацій. СКУД та її інтеграція в існуючу інфраструктуру підприємства швидко окупається завдяки ефективному контролю за дисципліною персоналу, такі системи використовуються для табелювання робочого часу, допомагаючи роботодавцям автоматично фіксувати години приходу і відходу працівників, затримки на обідах чи технічних перервах, сприяючи підвищенню відповідальності працівників. СКУД також підвищує рівень контролю подій на об’єкті. Наприклад, охоронно-пожежна сигналізація реагує на несанкціоновані спроби доступу в захищені зони, автоматично ставить безлюдні території під охорону та забезпечує розблокування дверей під час евакуації. Системи контролю доступу забезпечують комплексний захист території завдяки програмним і технічним елементам, які дозволяють ефективно контролювати охоронюваний об’єкт.

Технології шифрування даних та створення унікальних ключів доступу запобігають спробам підробки чи дублювання карт і кодів, це гарантує, що доступ до об’єкта отримають лише авторизовані особи, виключаючи ризик використання фальшивих ідентифікаторів. СКУД є складним і багатофункціональним інструментом, який забезпечує безпеку об’єктів і ефективний контроль доступу. Їхнє вдосконалення, включаючи використання штучного інтелекту для аналізу поведінкових даних, відкриває нові горизонти у сфері безпеки.

Використання СКУД вимагає суворого дотримання законодавчих норм, особливо щодо безпеки самої системи та захисту персональних даних. Конфіденційність інформації також має залишатися пріоритетом, щоб уникнути

порушень, які можуть призвести до штрафів. При проєктуванні та монтажі системи необхідно враховувати вимоги до її встановлення, забезпечуючи відповідність усім чинним законам. Слід приділити дотриманню правил збору, зберігання та обробки персональної інформації, адже більшість країн вимагає особливого захисту таких даних, система має повністю відповідати державним стандартам і нормам, а також потребує оформлення всієї необхідної документації.

Стабільність та відповідність роботи СКУД законодавчим вимогам забезпечують своєчасні перевірки її функціонування. Потрібно регулярно перевіряти стан усіх компонентів системи, таких як зчитувачі карток, контролери, електронні замки та інші пристрої системи, щоб вчасно виявляти можливі збої чи зношення деталей, які впливають на функціональність. Не менш важливо підтримувати актуальність програмного забезпечення (далі – ПЗ), що керує системою, адже оновлення здебільшого усувають вразливості, підвищують продуктивність і додають нові корисні функції.

Перевірка баз даних користувачів та прав доступу запобігає несанкціонованим спробам проникнення і дає змогу адаптувати систему до потреб організації, наприклад можна робити такі «перевірки» щомісяця, або після влаштування нового співробітника, або звільнення колишнього. Слід також не забувати забезпечувати чистоту обладнання, оскільки пил і бруд можуть негативно позначитися на точності роботи зчитувачів та механічних компонентів.

Окрім базових принципів, технічне обслуговування систем контролю та управління доступом можна доповнити кількома важливими аксіомами, які підвищать ефективність і надійність роботи системи. По-перше, слід приділяти увагу кабельній інфраструктурі. Періодична перевірка стану кабелів на наявність механічних пошкоджень, наприклад від гризунів, чи слідів зносу допоможе уникнути раптових збоїв у роботі обладнання. Важливо також стежити за правильністю підключення, особливо якщо в систему додаються нові компоненти. По-друге, рекомендується мати запасні частини для основного обладнання, такого як зчитувачі карток, реле або модулі живлення. Це дозволить оперативно замінити зламаний компонент без значних затримок у роботі системи, без виникнення

зайвих інцидентів. Також зважаючи на становище в енергетичній інфраструктурі потрібно постійно продумувати можливості підключення резервного енергозабезпечення, наскільки це можливо. Ще одне корисне правило – регулярно аналізувати журнали подій системи. Це дозволяє виявити незвичайну активність, спроби несанкціонованого доступу або інші потенційні загрози. Такі дані допомагають швидше реагувати на проблеми і покращувати загальну безпеку.

На мою думку, одним із найважливіших і найефективніших підходів є організація уроків, семінарів чи презентацій для навчання співробітників, які користуються СКУД або відповідають за її обслуговування. Глибше розуміння принципів роботи системи та її функціонування допомагає мінімізувати людські помилки, які часто стають причиною збоїв. Також важливим є регулярний аудит обладнання та програмного забезпечення, що дозволяє оцінити, чи відповідає система сучасним вимогам. У разі виявлення її застарілості слід розглянути модернізацію, яка допоможе впровадити новітні технології та значно підвищити рівень безпеки, але це може вартувати чимало коштів.

Оновлення обладнання систем контролю та управління часто стає складним фінансовим викликом для компаній, що потребує детального планування. На перший погляд, такі витрати можуть здатися значним навантаженням на бюджет, але у перспективі вони зазвичай виправдовують себе економічними перевагами. Сучасне обладнання, завдяки своїй підвищеній надійності та енергоефективності, дозволяє суттєво скоротити витрати на ремонт і технічне обслуговування. Варто зазначити, що впровадження сучасних технологій, наприклад, біометричних систем або мобільних ідентифікаторів, значно спрощує управління доступом, одночасно скорочуючи витрати на навчання персоналу та адаптацію системи до нових умов. Окрім цього, оновлення обладнання дозволяє мінімізувати ризики, пов’язані зі збитками від несанкціонованого доступу чи технічні збої.

Початкові витрати на придбання нового обладнання, впровадження програмного забезпечення та навчання персоналу можуть здатися недоцільними, але існують ефективні підходи для їх оптимізації. Один із таких способів – модульне оновлення систем, яке дозволяє поступово замінювати окремі

компоненти, рівномірно розподіляючи фінансове навантаження у часі. Окрім цього, інвестиції у модернізацію часто можуть частково компенсуватися через податкові пільги або участь у державних програмах підтримки безпеки.

2.2 Технологічні особливості сучасних СКУД

2.2.1 Структурні компоненти систем управління доступом

Система контролю і управління доступом складається з низки ключових компонентів, кожен з яких виконує важливу функцію для налагодження безпеки та організації доступу. Основу таких систем становлять ідентифікатори, які використовуються для розпізнавання користувачів. Крім того, ідентифікаторами можуть слугувати біометричні дані, такі як відбитки пальців, венозний малюнок долоні чи геометрія обличчя. Біометрія має суттєву перевагу над традиційними засобами, оскільки виключає можливість передачі ідентифікатора іншим особам і підвищує рівень безпеки. Існує кілька типів ідентифікаторів, кожен з яких має свої переваги та сфери застосування. Одним із найпоширеніших типів є безконтактні ідентифікатори, які передають дані за допомогою радіочастотної ідентифікації (RFID). Це зручний і доступний спосіб ідентифікації, що широко використовується в офісах, на підприємствах і в громадських установах. Пластикові картки, такі як EM-Marine або Mifare[10], є стандартом для безконтактної ідентифікації RFID. Прикладом Mifare-зчитувача є зчитувач безконтактних карт Hikvision DS-K1101M, що зображений на рис. 2.1. EM-Marine працює на частоті 125 кГц і є одним з найстаріших стандартів. Картки цього типу використовують просту радіочастотну ідентифікацію для передачі даних між карткою та зчитувачем. Вони є доступними і широко використовуються в різноманітних системах, але мають обмежену дальність зчитування та низький рівень безпеки. Оскільки дані не шифруються, вони можуть бути вразливими до копіювання або підробки. Mifare, у свою чергу, працює на частоті 13.56 МГц, що дозволяє досягати більшої швидкості передачі даних і дальності зчитування.



Рисунок 2.1 Зчитувач Hikvision DS-K1101M

Окрім того, технологія Mifare надає кращий рівень безпеки. Наприклад, картки Mifare Classic використовують шифрування для захисту даних, а новіші моделі, такі як Mifare Plus та Mifare DESFire, забезпечують ще більш складні механізми захисту, що робить їх більш надійними для використання в системах з високими вимогами до безпеки.

Крім карток, популярними є брелоки, які зручно носити, прикріпивши їх до ключів, вони мають вигляд звичних нам ключів від домофону. Для зручності у носінні, наприклад, в готелях або спортзалах, використовуються браслети. Іншим типом є традиційні ідентифікатори, які включають механічні ключі та магнітні картки. Магнітні картки, що використовують магнітну смугу для зчитування даних, є менш надійними через ризик пошкодження і зносу, або копіювання, але все ще застосовуються в деяких системах доступу. Ще одним варіантом є комбіновані ідентифікатори, які поєднують кілька методів ідентифікації для підвищення рівня безпеки, наприклад, одночасне використання картки і відбитка. Вибір типу ідентифікатора залежить від рівня безпеки, який потрібно забезпечити, а також від специфіки об’єкта чи організації.

Дані, що містяться в ідентифікаторі, зчитуються спеціальними пристроями, які передають інформацію до контролера для прийняття рішення про надання доступу. Зчитувачі[11] можуть бути різних типів залежно від виду ідентифікатора: для безконтактних карток, для дальньої ідентифікації, а також біометричні зчитувачі для аналізу відбитків пальців, геометрії обличчя або венозного малюнка. Одним із найбільш поширених є кодовий зчитувач з клавіатурою, приклад якого зображений на рис. 2.2.



Рисунок 2.2 Зчитувач з кодовою клавіатурою Seven CR-778

Цей пристрій дозволяє користувачеві набирати таємний код на клавіатурі для доступу до приміщення. В основному такі зчитувачі використовуються на об'єктах, де не потрібен високий рівень захисту, наприклад, на дитячих майданчиках чи в інших публічних місцях. Вони відзначаються бюджетністю та простотою у використанні, однак їхній основний недолік – ненадійність. Якщо хтось дізнається або підслухає код, він зможе вільно отримати доступ до об'єкта в будь-який час. Крім того, неможливо контролювати, хто саме та коли скористався кодом. Наступним типом є RFID-зчитувачі, для доступу необхідно піднести до зчитувача картку, брелок або браслет. Принцип роботи подібний до кодових зчитувачів, однак RFID-система є більш надійною, оскільки створити дублікат картки складніше, ніж запам'ятати код. Крім того, картки можна зашифрувати, що додає

рівень безпеки. Ці зчитувачі часто використовуються в спортивних комплексах, аквапарках та інших громадських закладах. Однак, їхнім недоліком є те, що картки чи брелоки можуть губитися, ламатися або забуватися вдома, що може створити незручності для користувачів. Одним з надійніших варіантом вважаються біометричні зчитувачі, вони забезпечують високий рівень безпеки, оскільки біометричні дані неможливо підробити або втратити. Але як і у всіх в цього методу є і свої недоліки – у холодну пору року або при наявності травм на пальцях система може працювати некоректно. Крім того, процес сканування біометрії може бути довгим, що іноді викликає затримки при доступі. Одним з найновіших видів зчитувачів вважається геометричний, який часто використовує розпізнавання обличчя. Зараз найбільше його використовують в мобільних пристроях. Геометричні зчитувачі забезпечують дуже високий рівень безпеки та працюють швидко, навіть при наявності головних уборів чи в слабкому освітленні, завдяки використанню нейронних мереж. Зазвичай такі системи мають два типи камер – теплову та для сканування обличчя, що дозволяє запобігти підробці за допомогою фотографій. До його мінусів можна віднести його високу вартість та вимогливість до точного внесення даних у базу, що потребує особистої присутності користувача. Крім того, система може не працювати з обличчям в масці, що є важливим у певні періоди, наприклад, під час карантину.

Важливим елементом СКУД є виконавчі пристрої, які забезпечують фізичну перешкоду доступу до контрольованих зон. Ці пристрої виконують не лише функцію обмеження доступу, а й сприяють організації руху, підвищенню рівня безпеки та забезпеченню точного обліку осіб, які входять чи виходять з території. Серед ключових типів виконавчих пристроїв можна виділити електрозамки та турнікети[12], кожен із яких має свої особливості та доцільність застосування залежно від специфіки об'єкта.

Електрозамки бувають двох основних типів – електромагнітні та електромеханічні. Електромагнітні замки працюють за принципом утримання дверей за допомогою магнітного поля. Їхня конструкція включає магнітну пластину, яка утримується на металевій поверхні за допомогою струму. Вони

ідеально підходять для внутрішніх приміщень, таких як офісні кабінети, навчальні аудиторії або склади, де потрібен швидкий і зручний доступ для великої кількості людей. Проте через залежність від електроживлення такі замки можуть бути вразливими у разі перебоїв електропостачання, тому їх часто доповнюють аварійними джерелами живлення. Електромеханічні замки, на відміну від магнітних, працюють на основі механічного замикаючого механізму, який приводиться в дію за допомогою електричного сигналу. Вони більш універсальні, оскільки підходять як для внутрішніх, так і для зовнішніх дверей. Завдяки стійкості до погодних умов їх часто використовують на входах до житлових будинків, виробничих підприємств або складських комплексів. Електромеханічні замки забезпечують вищий рівень безпеки, оскільки навіть при відсутності струму вони залишаються замкненим.

Турнікети забезпечує контрольований доступ та обмеження потоку людей, їх конструкція дозволяє пропускати лише одну людину за раз, що робить турнікети ідеальним рішенням для об'єктів, де важливий точний облік відвідувачів. Наприклад, турнікети широко використовуються в метро, спортивних аренах, великих офісах, виробничих підприємствах і навчальних закладах. Завдяки цьому пристрою можна не тільки обмежити доступ, але й реєструвати час входу та виходу кожної людини, що актуально для автоматизації системи обліку робочого часу співробітників. Залежно від типу турнікета – роторний, повноростовий або розсувний, їх можна адаптувати для різних умов. Наприклад, повноростові турнікети забезпечують вищий рівень безпеки, оскільки унеможливлюють проникнення через них без авторизації, ідеально підходячи для стратегічних об’єктів або підприємств із суворим режимом охорони. Натомість роторні моделі більше орієнтовані на зони з високою прохідністю, де важливо забезпечити швидкий рух людей, наприклад, у бізнес-центрах чи торгових комплексах.

Контролери виконують функції управління всіма іншими елементами системи. Залежно від умов використання та специфіки об’єкта, контролери поділяються на автономні та мережеві. Кожен із цих типів має свої переваги, недоліки та підходить для різних сфер застосування. Автономні контролери

працюють незалежно від центральної системи управління. Вони не потребують підключення до мережі, що робить їх досить простими у встановленні та експлуатації. Налаштування автономних контролерів здійснюється локально для кожного пристрою. Наприклад, додавання нових користувачів або змінення параметрів доступу виконується безпосередньо на місці, зазвичай за допомогою спеціального програматора, пульта або навіть введення даних через клавіатуру. Основна перевага автономних контролерів – це доступна ціна та відсутність необхідності в складному програмному забезпеченні. Вони є чудовим вибором для невеликих об'єктів, де не потрібно інтеграції з іншими системами чи здійснення централізованого моніторингу, автономні контролери ідеально підходять для установки на дверях квартир, приватних будинків, невеликих офісів або складів. Проте автономні системи мають і свої недоліки, вони обмежені в можливостях масштабування та інтеграції. Якщо потрібно керувати кількома точками доступу одночасно, їхнє локальне налаштування може стати трудомістким. Крім того, відсутність централізованого моніторингу робить автономні контролери менш ефективними для великих підприємств або об’єктів із підвищеними вимогами до безпеки. Мережеві контролери, на відміну від автономних, забезпечують можливість об’єднання кількох пристроїв в єдину інтегровану систему. Прикладом мережевого контролеру є U-Prox IP400[13], який зображений на рис. 2.3.



Рисунок 2.3 Мережевий контролер доступу U-Prox IP400

Цей тип контролерів працює через підключення до локальної мережі або інтернету, що дозволяє здійснювати централізоване керування всією системою. Управління мережевими контролерами відбувається за допомогою спеціалізованого програмного забезпечення, яке дозволяє не лише додавати або змінювати користувачів, але й у режимі реального часу відстежувати всі події в системі. Мережеві контролери мають низку переваг, вони забезпечують високу зручність управління, адже всі налаштування можуть виконуватися з одного централізованого пункту, навіть дистанційно, мережеві рішення дозволяють легко масштабувати систему, додаючи нові точки доступу без значних зусиль, вони забезпечують високий рівень безпеки, оскільки всі події, такі як спроби несанкціонованого доступу або технічні збої, можуть бути оперативно виявлені і зафіксовані. Завдяки інтеграції з сучасними технологіями, мережеві контролери часто використовуються в поєднанні з біометричними зчитувачами, системами відеоспостереження та іншими елементами автоматизації.

2.2.2 Біометрія в системах безпеки

Двофакторна аутентифікація вже стала звичною для більшості користувачів, коли йдеться про доступ до банківських сервісів чи облікових записів. Цей метод вимагає підтвердження особи за допомогою двох різних облікових даних, наприклад, введення пароля та отримання коду через SMS. Аналогічний принцип застосовується у системах управління доступом до будівель, де для входу на територію або до приміщення необхідно підтвердити свою особу одним або декількома способами. Сучасні системи контролю доступу використовують широкий спектр облікових даних, серед яких особливе місце займає біометрія – унікальні фізичні характеристики людини. Поєднання біометричних параметрів із традиційними методами, як картки доступу чи пін-коди, дозволяє значно підвищити ефективність систем безпеки. Використання мультимодальних технологій, які об’єднують кілька типів даних, забезпечує найкращі результати, адже вони дозволяють адаптувати систему до конкретних потреб і підвищити

рівень захисту завдяки багатофакторній аутентифікації, яка може включати три й більше рівнів перевірки. Це стало можливим завдяки здешевленню технологій та їхній доступності навіть для невеликих компаній. Найпоширенішими методами біометричної ідентифікації є сканування відбитків пальців, розпізнавання обличчя та аналіз сітківки ока. Відбитки пальців давно стали стандартом завдяки своїй надійності та зручності, особливо після їх інтеграції в мобільні пристрої[16]. Розпізнавання обличчя поступово стає невід'ємною частиною систем контролю доступу, а під час пандемії Covid-19 ця технологія допомагала навіть відстежувати контакти між людьми. Сканування сітківки ока вважається одним із найточніших методів, адже узори кровоносних судин є унікальними для кожної людини. Біометричні системи працюють за простим принципом: користувач реєструє свої фізичні дані, які зберігаються у зашифрованому вигляді в базі даних. Під час ідентифікації отримані «живі» дані порівнюються зі збереженими шаблонами. Для більшого захисту біометрія може поєднуватися з іншими формами аутентифікації, наприклад, пін-кодами чи картками доступу.

Камери з функцією розпізнавання обличчя є сучасним інструментом для ідентифікації та аналізу облич людей. Їхній принцип роботи базується на збиранні зображень за допомогою оптичних сенсорів, після чого ці дані обробляються алгоритмами розпізнавання, система визначає області на відео, де потенційно може бути обличчя, а нейронні мережі глибокого навчання аналізують ці зображення. Мережі складаються з багатьох шарів, кожен із яких виконує окремі операції для виділення ключових ознак, таких як контури чи розташування рис обличчя. Згодом ці ознаки використовуються для класифікації й ідентифікації особи. Для виявлення обличчя система аналізує кожен кадр відео окремо, що особливо ефективно в умовах швидкого руху чи змін масштабу зображення. Після цього визначаються унікальні характеристики: форма обличчя, положення очей, носа, рота та інші риси.

На основі цих даних створюється біометричний профіль – цифрове представлення фізичних характеристик людини. Він містить параметри, як-от відстань між очима, форму носа, кут нахилу голови, форму щелепи та інші унікальні риси. Такі профілі застосовуються не лише у сфері безпеки, але й,

наприклад, у фінансовій галузі для автентифікації.

Наступним кроком система порівнює створений біометричний профіль із даними, що зберігаються в базі. Це порівняння може здійснюватися різними способами: за допомогою пошукових запитів, візуального аналізу, математичних алгоритмів або статистичних моделей. Візуальне порівняння є найбільш поширеним і передбачає зіставлення зображень із бази з отриманим зображенням. Математичні методи, своєю чергою, застосовують алгоритми машинного навчання, які виділяють унікальні ознаки для точнішого порівняння. Головною перевагою біометричних профілів є їхня висока точність та унікальність. Після завершення процесу ідентифікації система приймає рішення про подальші дії. Це може бути відкриття дверей, увімкнення сигналу тривоги або інші дії залежно від сценарію використання. До мінусів можна віднести, що точність розпізнавання може знижуватися за умов слабкого освітлення або при зміні зовнішнього вигляду людини, тому задля максимальної ефективності таких систем важливо створити сприятливі умови для їхньої роботи та враховувати можливі недоліки під час впровадження, такі як погане освітлення або зміни зовнішнього вигляду людини.

Ідентифікація особи за відбитками пальців зарекомендувала себе як один із найефективніших методів, завдяки чому вона широко використовується в різних сферах. Головними перевагами цієї технології є висока точність і надійність ідентифікації, дешева ціна готових рышень та простота процесу сканування.

Доступна вартість терміналів сприяє їхньому широкому застосуванню, особливо для виконання базових завдань. Найпростіші дактилоскопічні пристрої зручні у використанні й не потребують значних фінансових вкладень.

Унікальність папілярного візерунка кожної людини полягає в тому, що малюнки ліній не повторюються, відрізняючись завершеннями, розгалуженнями та характерними точками. Це робить технологію ідеальною як для розкриття злочинів, так і для контролю доступу співробітників на підприємствах.

Однак одним із недоліків такої технології є чутливість сканерів до невеликих пошкоджень шкіри, таких як тріщини чи порізи. На виробництвах, де працівники взаємодіють із хімічними речовинами чи отримують дрібні опіки, система може

давати збої, що призводить до відмови у доступі. Для таких умов рекомендовано використовувати термінали вищої якості, які здатні враховувати подібні обмеження і розпізнавати відбитки навіть за наявності незначних ушкоджень. Альтернативним рішенням є дублюючі системи ідентифікації, які можуть включати розпізнавання за малюнком вен, геометрією обличчя або використання безконтактних карт.

Технологія розпізнавання райдужної оболонки ока стає дедалі популярнішою у світі, її активно використовують комерційні та державні установи для різних цілей, включаючи контроль доступу та управління робочим часом. Сканування райдужки часто плутають зі скануванням сітківки ока, хоча це різні технології.

Система розпізнавання райдужної оболонки аналізує кольорову частину ока, розташовану навколо зіниці, яку можна побачити без спеціального обладнання, тоді як сітківка є внутрішньою частиною ока, що складається з кровоносних судин і фоторецепторів. Процес розпізнавання райдужки включає зчитування текстури оболонки за допомогою інфрачервоних світлодіодів і подальше перетворення даних у цифровий код. Цей код порівнюється з шаблонами, збереженими в базі, для ідентифікації особи. Райдуга містить більше даних, ніж відбиток пальця чи інші біометричні ознаки, що робить цю технологію надзвичайно точною та комфортною для користувачів, оскільки не потребує фізичного контакту. Технології сканування райдужної оболонки знаходять застосування в аеропортах, таких як Schiphol в Амстердамі, де за їх допомогою здійснюють прискорений паспортний контроль для екіпажів і частих пасажирів. У Канаді вони використовуються в десятках аеропортів для авторизації персоналу.

Незважаючи на свої переваги, такі системи мають обмеження, наприклад, неможливість працювати з непрозорими контактними лінзами, хоча прозорі лінзи не є перешкодою для сканування.

Розпізнавання голосу є ще однією популярною та конкурентоспроможною біометричною технологією. Її основні переваги: безконтактність, простота використання та відносно низька вартість. Для роботи системи створюється цифровий профіль голосу, який зберігається в базі даних. Це дозволяє здійснювати

ідентифікацію за допомогою унікальних характеристик мовлення. Технологію активно застосовують для банківських операцій, відновлення доступу до акаунтів та перевірки ідентичності. Голосові системи також використовуються в мобільних і портативних пристроях для контролю доступу на склади чи до робочих зон. Однак точність таких систем залежить від умов: якість запису, фоновий шум і навіть стан здоров’я можуть впливати на результат.

Електронний підпис – це ще один цікавий спосіб ідентифікації, який базується на криптографії. Приклад такого зчитувача[14] зображений на рис. 2.4.



Рисунок 2.4 Пристрій захоплення електронного підпису Centerm A10

Приватний і публічний ключі дозволяють забезпечити цілісність даних та підтвердити їхню автентичність. Система створює хеш-код даних, який шифрується приватним ключем і перевіряється за допомогою публічного. Ця технологія широко використовується для авторизації у СКУД, підписання електронних документів, а також захисту журналів доступу. Застосування електронного підпису спрощує управління документами, скорочує витрати на їхнє зберігання та забезпечує можливість дистанційного підписання, що особливо актуально для віддаленої роботи або розподілених команд. Це дозволяє уникати фізичної присутності та сприяє ефективному функціонуванню системи без втрати безпеки чи конфіденційності.

Адміністрування таких систем є дуже зручним, оскільки доступ можна

швидко надати чи скасувати через програмне забезпечення. Користувачам не потрібно носити з собою картки чи запам’ятовувати пін-коди, такі системи дозволяють заощадити, скоротивши витрати на персонал служби безпеки та заміну фізичних носіїв доступу.

2.2.3 Аксесуари для СКУД

Будь-яка система контролю доступу неможлива без важливих аксесуарів, які забезпечують її ефективну роботу. Одними із ключових елементів є кнопки виходу, які застосовуються для відкриття дверей, воріт, шлагбаумів або хвірток.

Кнопки виходу бувають різних типів залежно від принципу роботи. Нормально відкриті (NO) кнопки функціонують шляхом замикання контакту, що робить їх сумісними з електромеханічними замками, засувками та контролерами. Нормально закриті (NC) кнопки працюють на розмикання і зазвичай використовуються разом із магнітними замками. Найпопулярнішими є універсальні кнопки (NC/NO), які можуть працювати як на замикання, так і на розмикання, забезпечуючи універсальність та сумісність із будь-якими системами контролю доступу.

Схематичне позначення, та умовний принцип роботи[15] зображений на рис. 2.5.

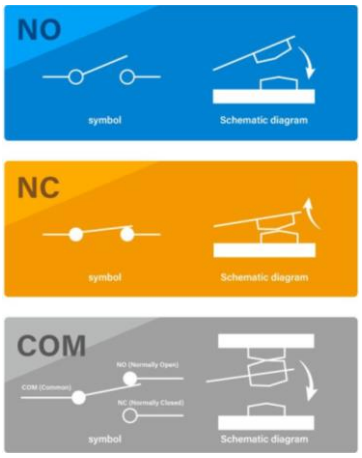


Рисунок 2.5 Принцип роботи контактної групи NC/NO

Крім того, кнопки розрізняються за способом активації. Для роботи механічної кнопки достатньо натиснути на корпус, сенсорні кнопки, натомість, спрацьовують при легкому дотику до поверхні, змінюючи опір контролера і відкриваючи двері. Безконтактні кнопки, обладнані інфрачервоним датчиком, реагують на наближення руки. Такий підхід забезпечує високу гігієнічність, адже пристрій не потребує фізичного контакту, достатньо лише провести рукою перед кнопкою, щоб двері відчинилися. Безконтактні кнопки особливо актуальні у громадських місцях, таких як медичні установи, офіси з великою кількістю співробітників або об’єкти громадського харчування, де мінімізація контакту з поверхнями є критично важливою.

Також важливим аксесуаром окрім кнопки є дверні доводчики. Їхня функція полягає у тому, щоб автоматично закривати двері після того, як людина їх відчинила. Це запобігає випадковому залишенню дверей відчиненими, що є важливим для підтримання безпеки та ефективності роботи системи. Доводчики часто використовуються на входах до офісів, складів, банків, медичних закладів. Наприклад, у банках вони допомагають гарантувати, що двері до сховищ або касових приміщень завжди будуть зачинені. У медичних закладах доводчики запобігають проникненню сторонніх осіб до обмежених зон, таких як операційні або стерильні кімнати. У поєднанні кнопки виходу та дверні доводчики формують комплексне рішення, яке покращує безпеку, комфорт і функціональність будь-якої системи контролю доступу.

Електромагнітні замки [16] та ригелі використовуються в системах безпеки для обмеження доступу до приміщень або територій. Електромагнітні замки функціонують завдяки електромагнітним силам, що утримують двері закритими, коли на замок подається електричний струм. Принцип їх роботи полягає в тому, що електромагнітна котушка генерує сильне магнітне поле, яке притягує металеву пластину, що встановлена на дверях. Це дає можливість замку утримувати двері замкненими, поки не буде подано сигнал для їх відкриття. Будова електромагнітного замка зображена на рис. 2.6.



Рисунок 2.6 Будова електромагнітного замка

Для досягнення максимальної безпеки необхідно забезпечити, щоб і замок, і його кронштейн знаходилися у внутрішньому захищеному просторі на дверях та вікнах, на які буде встановлено магнітний замок. Необхідно подбати про те, щоб кабелі не мали доступу зовні. Загальне емпіричне правило полягає в тому, що електромагніт повинен бути прикріплений до внутрішньої частини корпусу рами, а відповідна частина також повинна бути прикріплена до внутрішньої частини, але на поверхні, що відкривається.

При виборі магнітного пристрою основними факторами залишаються умови експлуатації та сила утримання. Для вуличної хвіртки блок має бути вологостійким і добре переносити температурні перепади, найдорожчі моделі одержали корпус із антивандальним покриттям. На міжкімнатні двері або меблеві шафи встановлюються компактні замки з невеликим та вологозахищеним корпусом. Сила утримання вказується на те, наскільки надійно зачиняються двері, і найкраще орієнтуватися на матеріал виготовлення самого полотна та на його вагу. Так, для меблів достатньо пристрою з показниками кілька кілограмів, але для вуличної металевої хвіртки краще придбати пристрій з силою утримання від 200 кг.

Ригелі, в свою чергу, є механізмами, що забезпечують додаткову безпеку, коли замок закритий. Вони працюють як додаткові запори або штифти, які фіксують двері в закритому положенні, це дає змогу забезпечити більшу стійкість системи, оскільки навіть якщо замок буде зламано, ригель продовжить утримувати двері на місці.

2.3 Особливості монтажу СКУД

Вибір обладнання для СКУД є складним і багатогранним процесом, який залежить від безлічі специфічних факторів для кожного конкретного об'єкта. Перед початком проєктування необхідно враховувати такі аспекти, як кількість співробітників, кількість і тип точок проходу (односторонні або двосторонні), а також вимоги щодо протипожежної безпеки й організації евакуації у разі надзвичайної ситуації. Одним з найпростіших пристроїв, який можна віднести до такої системи, є домофон або відеодомофон[17]. Однак великому підприємству, офісної будівлі такого девайса недостатньо, потрібна більш функціональна система СКУД. Вона забезпечує стеження і контроль доступу на об’єкт згідно з визначеними умовами.

Монтаж СКУД також потребує врахування низки нюансів. Наприклад, контролери слід встановлювати у захищених зонах, щоб запобігти умисних диверсій. Шини передачі даних між контролером і зчитувачем повинні мати оптимальну довжину, рекомендовану виробником, і бути екранованими у разі підвищеного рівня електромагнітних перешкод.

Програмне забезпечення СКУД виконує функції управління системою та збору даних. Воно забезпечує гнучке налаштування контролерів, ведення бази даних користувачів, моніторинг точок доступу, облік робочого часу й формування звітів. Щоб підвищити ефективність системи, потрібно інтегрувати її з іншими системами безпеки, такими як відеоспостереження або пожежна сигналізація. Наприклад, у разі пожежі програмне забезпечення може автоматично відключити замки, забезпечуючи швидку евакуацію, або заблокувати доступ при активації охоронної сигналізації.

Створення такої системи починається з підготовки, цей етап охоплює обстеження об’єкта, де потрібно встановити СКУД, його оцінку і проєктування та

узгодження з замовником, другим етапом є власне монтаж системи, він охоплює установку необхідного обладнання, прокладку кабелів і з’єднання всіх вузлів один з одним.

Завершальним етапом є введення системи в експлуатацію. Тут проводиться повне налаштування роботи системи, створюються ключі для персоналу. Це можуть бути прості електромагнітні варіанти або ключ-карти, а можуть бути й більш складні ключі, коли для доступу потрібно відсканувати біометричні дані: відбиток пальця, сітківку ока. Також проводиться інструктаж співробітників і служби безпеки. Зазвичай СКУД містить ще й систему пожежної безпеки (датчики диму і системи пожежогасіння), відеоспостереження (в цьому випадку встановлюються камери відеоспостереження, відеореєстратори для певної кількості камер, тощо) і сигналізацію, яка сповіщає про несанкціонований доступ на об’єкт.

Всі СКУД можна поділити на автономні та мережеві. Нюанси установки багато в чому залежать від того, до якого типу належить система. Автономні СКУД Такий варіант зазвичай застосовується для контролю доступу в невеликому приміщенні. Призначення автономної системи полягає в забезпеченні доступу в приміщення або на територію співробітників і мешканців, а також заборону проникнення сторонніх осіб. Встановлюється вона, як правило, на центральні та запасні виходи.

Існує декілька варіантів виконання таких СКУД, так малі автономні системи можуть бути: з одним зчитувачем, використовуються для невеликих організацій зі штатом в 1000 осіб максимум. У цьому випадку ставиться автономний зчитувач (з кодом або можливістю використовувати ключ-карту), електромагнітний замок і кнопка виходу. Ідеально підійде для використання в під’їздах багатоквартирних будинків і на входах в невеликі офісні будівлі. З двома зчитувачами, більш захищений варіант, зчитувачі встановлюються з двох сторін дверей. Щоб увійти та вийти знадобиться використовувати карту або код доступу. Кнопка виходу же встановлюється в прихованому місці, щоб тільки охорона могла випускати з будівлі гостей. З урахуванням робочого часу, цей тип системи є найбільш складним та захищенним. Він містить два абсолютно однакових зчитувача, контролер, а також ПК з програмним забезпеченням, за допомогою якого і здійснюється облік. Крім того, є електромагнітний замок і кнопка виходу. Алгоритм майже не

відрізняється від попереднього, проте за допомогою ПЗ можна порівнювати особу, що увійшла на територію, з оригінальним фото на карті доступу. До того ж програма дає можливість складати розклад робочих, а також вихідних днів і свят. Це дозволяє блокувати двері у позаробочий час. Крім того, для комфортного контролю доступна можливість завантаження планів будівель в комп'ютер.

Ці системи універсальні, тому можна їх не прив'язувати тільки для людей та дверей, а наприклад використати шлагбауми та турнікети.

Оскільки автономні СКУД не вимагають створення цілої мережі модулів, то їх встановлення та налаштування займає всього лише кілька днів. Мережеві СКУД Це більш просунуті системи, які підійдуть великим підприємствам. Найчастіше такі системи створюються на базі внутрішньої мережі організації. Якщо ж мережі немає, тоді для побудови СКУД ще й прокладають кабелі, які з'єднують обладнання. Налаштування такої системи є досить складним процесом, оскільки необхідно інтегрувати й об'єднати між собою систему відеоспостереження, пожежної безпеки, а також охоронну систему (це якраз і є контролери, зчитувачі й т. п.). Варто відзначити, що бездротові системи контролю та управління доступом використовують інтернет. Це скорочує час на підключення девайсів, однак налаштування ускладнюється.

Класична мережева система складається з головного і другорядних контролерів, в якій перший контролює другі, а також з персонального комп'ютера (далі – ПК). При цьому другорядні контролери відповідають за роботу периферійних девайсів: шлагбаумів, зчитувачів, замків, турнікетів. Кількість таких пристроїв напряму пов'язана з кількістю дверей. Комп'ютера (або декількох ПК) зі спеціальним, серверним або ж клієнтським, програмним забезпеченням. Комп'ютер з ПЗ серверного типу з'єднується з головним контролером, задля можливості переглядати інформацію з усіх другорядних контролерів, блокувати та відкривати двері, складати картотеку співробітників і т. д. Інші ж ПК в такій мережі підключаються саме до комп'ютера з серверним ПЗ. На такі другорядні комп'ютери ставиться ПЗ другого типу – клієнтське. З його допомогою не можна вносити зміни в налаштування системи, але можна переглядати дані про її стан.

Важливо, що як і автономні, мережеві СКУД також можуть включати й облік робочого часу.

Система обліку робочого часу завдяки спеціальному програмному забезпеченню автоматично підраховує загальну кількість годин, яку відпрацьовує кожен співробітник організації. Крім того, враховуються й відпустки, лікарняні, відгули, а також прогули та запізнення. Для фіксації часу приходу та виходу кожного співробітника використовується спеціальний ідентифікатор: карта, відбиток пальця, геометрія долоні, райдужка ока. Від застосовуваного ідентифікатора залежить, яке саме ПЗ буде використовуватися для обліку. Установка системи з урахуванням робочого часу дозволяє поліпшити трудову дисципліну і спростити підготовку звітності.

Система контролю й управління доступом передбачає монтаж різних пристроїв. Контролери зазвичай монтуються в розподільних коробках всередині приміщення. Такі коробки забезпечують комфортну установку, а також зручність подальшого обслуговування контролера. Іноді замість них використовуються штатні корпуси, комутаційні шафи. Що стосується зчитувача, то для установки цього елемента СКУД стіну наскрізь свердлять за допомогою бура. Річ у тому, що зчитувачі встановлюються з двох сторін: зовні та всередині приміщення. Від зчитувачів до контролера прокладають кабелі. Вони можуть бути встановлені в стіні або ж прокладені в кабель-каналі. Як уже було згадано, іноді СКУД передбачає установку тільки одного зчитувача – зовні об’єкту, що охороняється.

Створення та побудова системи контролю та управління доступом вимагає й установки виконавчих девайсів: шлагбаумів, турнікетів, хвірток, електромагнітних замків, електромеханічних засувок. Останні два елементи зі списку встановлюються так, що всі активні компоненти ставляться на одвірок, а на рухому частину дверей монтуються металеві пластини та накладки.

Для невеликих офісів, приватних і багатоквартирних будинків, квартир установка домофона або ж відеодомофона вже є константою, яка дозволить забезпечити комфорт та безпеку. Класичний домофон складається з зовнішньої панелі доступу, а також домофонної трубки для передачі сигналу, яка

встановлюється всередині приміщення. Зовнішня панель складається з клавіш набору, замку і магніту. Що стосується відеодомофона, то такий пристрій мало чим відрізняється від класичного. Єдина різниця – камера спостереження на зовнішній панелі, а також панель виклику, яка ставиться всередині квартири або будинку.

Спочатку прокладається кабель і монтуються комутаційні блоки. Дроти можуть бути прокладені всередині стін (якщо в будинку є система міжповерхових стояків, призначених для кабельних систем) або по поверхні стін. У другому випадку дроти захищають спеціальними коробами. Що стосується розташування комутаційних блоків, то воно залежить від технічних особливостей приміщення. Зазвичай вони монтуються в закритих нішах. Якщо мова про багатоповерхівки, то може бути встановлений 1 блок комутації на кілька поверхів, або ж на кожному поверсі буде розташовуватися по блоку.

У старих будинках двері рідко відповідають сучасним вимогам безпеки, та й магнітний замок на них поставити не можна. У цих випадках дерев’яні двері знімають, а замість них встановлюють металеві. Іноді старі двері зміцнюють: обшивають їх вагонкою. Важливо пам’ятати, що вагонка – не найнадійніший метод, оскільки під впливом погодних умов обшиті двері все одно можуть деформуватися, що призведе до поступового погіршення роботи домофонної системи.

Встановлення замка здійснюється строго по центру дверного полотна. Монтаж основної панелі здійснюється шляхом врізання у вхідні двері, згодом до неї приєднують електронний блок. Якщо домофон встановлюється в багатоквартирному будинку, тоді трубки та блоки ставляться в кожну квартиру, і в кожну квартиру підводять кабелі. При встановленні відеодомофона передбачається, що у квартирі ставиться не тільки абонентська трубка і блок, але й відеопанель. Монтаж БЖ здійснюється поряд з підключенням домофонної мережі до електрики. В приватних будинках з великою прилеглою територією іноді встановлюється декілька панелей. Наприклад, одна з них ставиться з боку воріт, а друга – безпосередньо біля входу в будинок.

Завершальним етапом виступає налаштування, тут вносяться ключові

параметри, здійснюється перевірка працездатності встановленої системи, враховується конфігурація панелі й призначених для користувача девайсів.

2.4 Інтеграція ШІ в автоматизовані системи управління доступом

Інтеграція штучного інтелекту в системи контролю доступу радикально змінює підхід до безпеки, дозволяючи створювати більш адаптивні, точні та інтелектуальні рішення. На даний момент одним із найбільш розповсюджених напрямів є використання технологій комп'ютерного зору для розпізнавання облич. Алгоритми глибокого навчання забезпечують точне визначення особистості навіть у складних умовах, таких як погане освітлення або часткове закриття обличчя.

Дослідження в університетах, таких як MIT, підтверджують, що сучасні системи розпізнавання мають точність до 99,8%, що робить їх ефективними навіть у масштабних установах, наприклад, аеропортах чи на підприємствах із великою кількістю співробітників.

З 2020 року дискусії про необхідність обмеження чи заборони використання технологій розпізнавання облич стали важливим аспектом обговорень щодо конфіденційності, етики та політики штучного інтелекту. Основна критика цих систем часто базується на твердженні, що вони демонструють низьку точність, особливо для жінок і представників меншин. Такі звинувачення викликають питання про наукову основу цих тверджень та реальну ефективність технологій. Насправді будь-яка біометрична технологія, включаючи розпізнавання облич, має певний рівень похибки. Ця похибка може бути зумовлена умовами зйомки, такими як освітлення, розмиття зображення або кут камери. Попри це, сучасні системи досягли значних успіхів. Наприклад, багато передових технологій розпізнавання облич сьогодні демонструють точність понад 99%, навіть для демографічно різноманітних груп. Це показники, які відповідають або перевищують рівень точності автоматизованих систем розпізнавання відбитків пальців чи райдужної оболонки ока, що вважаються золотим стандартом біометричних систем. Хоча попередні покоління технологій дійсно стикалися з труднощами у стабільності

роботи для різних демографічних груп, нові дослідження та оновлення алгоритмів значно підвищили їхню надійність. Проте твердження про "вроджену упередженість" технологій розпізнавання облич часто базуються на застарілих, неправильно інтерпретованих або нерелевантних даних. Найактуальніші звіти, включаючи урядові оцінки США, підтверджують, що сучасні технології розпізнавання облич є надзвичайно точними та ефективними. Це робить їх не лише прийнятними для комерційних чи урядових програм, але й дозволяє впроваджувати їх у масштабних інфраструктурних рішеннях.

Технології розпізнавання облич стають все більш точними й ефективними, хоча жоден алгоритм не може гарантувати 100% безпомилковість. Сучасні дослідження свідчать, що навіть за наявності демографічних відмінностей у точності, загальний рівень роботи алгоритмів залишається вражаюче високим. Наприклад, найефективніші алгоритми досягають точності розпізнавання до 98-99,4% навіть у великих базах даних, які містять до 12 мільйонів зображень. Такі показники підтверджуються оцінками Національного інституту стандартів і технологій США (NIST), що вже понад 20 років проводить незалежну оцінку продуктивності систем розпізнавання облич. Технології активно використовуються в критично важливих сферах, таких як перевірка міжнародних мандрівників на кордонах США. Зокрема, у програмах, які реалізує митна і прикордонна служба США, технології розпізнавання облич застосовуються у 238 аеропортах світу, включаючи 38 американських. Біометрична система дозволила перевірити понад 300 мільйонів мандрівників і виявити понад 1800 випадків, коли люди намагалися в’їхати до США за підробленими документами. Ринок технологій розпізнавання облич є глобальним і конкурентним. Постачальники працюють над вдосконаленням алгоритмів, забезпечуючи точність та ефективність незалежно від демографічних характеристик користувачів. Висока точність систем можлива завдяки використанню даних із широкого кола джерел і налаштуванню алгоритмів для роботи в різних умовах, таких як контроль на кордонах, правоохоронні органи або комерційні програми. Незважаючи на прогрес, необхідні постійні дослідження й оновлення алгоритмів для усунення залишкових проблем. Такі ініціативи

допомагають уникати ризиків, пов’язаних із демографічними упередженнями, і забезпечують стабільну продуктивність технологій навіть у складних умовах.

Ще один перспективний підхід – аналіз поведінки за допомогою ШІ, зараз його лише починають впроваджувати та тестувати в складних умовах, але він має велике майбутнє. Алгоритми можуть відслідковувати аномальні дії: наприклад, спробу підібрати пароль, використання чужого бейджа чи тривале перебування у зоні доступу без дозволу. У дослідженні, проведеному компанією IBM, було показано, що такі системи дозволяють знизити ризик внутрішніх загроз на 60%, адже вони не просто фіксують факт доступу, а й аналізують його контекст. Компанія нічого не втрачає, бо не штучному інтелекту не потрібно платити заробітню плату, це просто разова інвестиція, яка з високою вірогідністю окупить себе за короткий проміжок часу.

До розряду цікавих підходів можна віднести голосову ідентифікацію. Завдяки алгоритмам розпізнавання мовлення та голосу, система може визначати особистість на основі унікальних акустичних характеристик. Університет Карнегі-Меллон працює над створенням таких рішень для організацій, які потребують високий рівень безпеки і готові пробувати нове. Як вже було досліджено раніше, поєднання голосової ідентифікації з іншими біометричними методами ідентифікації дозволяє створити багаторівневу систему автентифікації.

Останнім ноу-хау в світі технології є застосування ШІ для адаптивного управління доступом та персоналом. Наприклад, в офісах система може аналізувати графіки співробітників, прогнозувати, коли конкретна особа може знадобитися в певній зоні, або тимчасово обмежувати доступ, якщо виявлено якісь розбіжності, негаразди та підозрілі дії. У практичному кейсі компанії Microsoft хмарна система доступу, підсилена ШІ, дозволила не тільки знизити адміністративні витрати, але й оперативно реагувати на загрози, завдяки чому вдалося уникнути кількох спроб несанкціонованого проникнення. Крім цього, інтеграція ШІ дозволяє аналізувати великі масиви даних для створення прогнозів.

У великій інфраструктурі, як, наприклад, на заводах Tesla, системи ШІ допомагають виявляти потенційні ризики, наприклад, некоректно працюючі двері

чи картки, що були продубльовані з метою лиходійства. Цим всім займається суперкомп’ютер Dojo[18], що зображений на рис. 2.7, який обробляє дані з багатокамерних систем для створення тривимірної моделі простору. Вони також використовуються для оцінки загального рівня безпеки на об’єкті, що дозволяє активно та ефективно усувати можливі слабкі місця. Крім того, Tesla використовує штучний інтелект у профілактичному обслуговуванні, щоб контролювати стан обладнання та прогнозувати збої до їх виникнення, мінімізуючи простої та забезпечуючи безперервне виробництво.



Рисунок 2.7 Одна комірка суперкомп’ютера Dojo

3. ПОБУДОВА СХЕМИ ТА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПУ З ВИКОРИСТАННЯМ ШІ ТА ВІДЕОНАГЛЯДУ

3.1 Інформація про об’єкт

Для демонстрації розташування системи біометричного контролю доступу з використанням штучного інтелекту насамперед було розроблено план-схему офісу підприємства (вигляд зверху), яке спеціалізується на роздрібній торгівлі, за допомогою програми ArchiCAD. План території зображений на рис. 3.1.

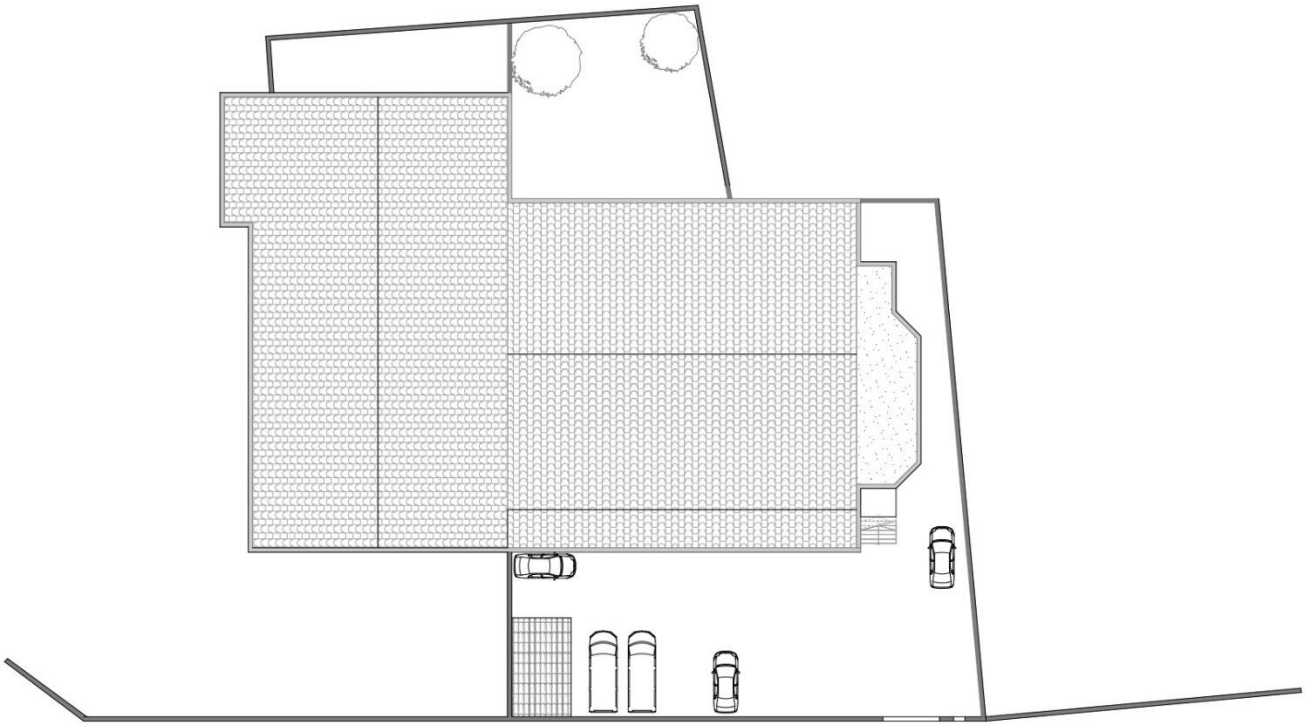


Рисунок 3.1 План території офісу

Це реальний кейс, в якому замовник попросив забезпечити офіс СКУД з рахуванням робочого часу, доступом певних осіб до зазначених приміщень, відкриття воріт за допомогою камери з розпізнаванням номерних знаків, системою відеонагляду з певними особливостями, параметрами, та бюджетом.

За знімком із супутника, що зображений на рис. 3.2, видно, що приміщення офісу ділиться на 2 будівлі, одна з яких знаходиться на території іншого підприємства.



Рисунок 3.2 Знімок об’єкту на карті

Лицьова частина території виходить на проїжджу частину, вся територія охоплена парканом заввишки 3 метри, на кутах встановлені металеві трубки заввишки 4 м (заздалегідь продумано для камер відеоспостереження).

Загальна площа території сягає близько 1470 м^2, офісу – 641,2 м2. Присутній 1 заїзд для автомобілів із автоматичними воротами та 1 вхідні двері для відвідувачів та персоналу. Всередині є парковка з місцями для 11 автомобілей та гаражем для 1-го автомобіля.

Також було розроблено генеральний план офісу підприємства, з розрізом кімнат, за допомогою програми ArchiCad. Генеральний план зображений на рис. 3.3.

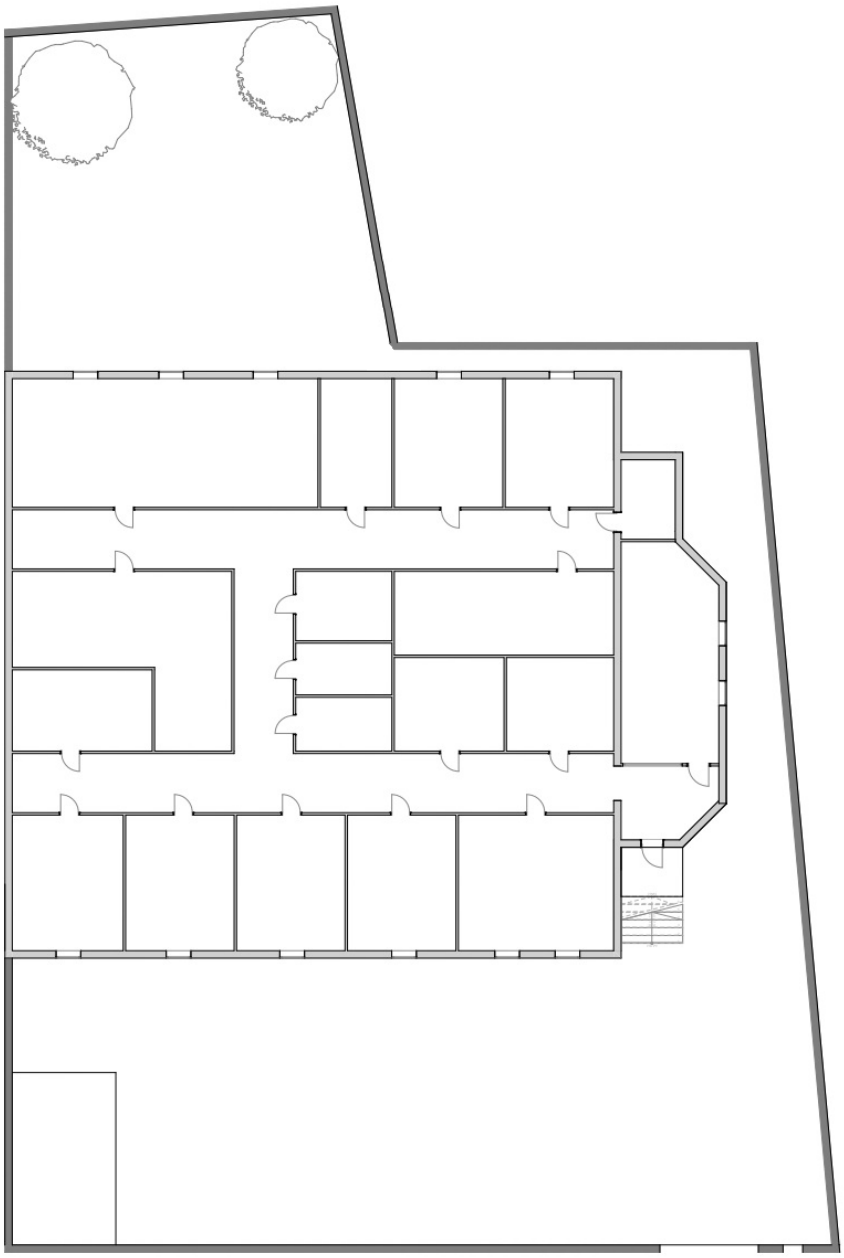


Рисунок 3.3 Генеральний план території офісу

Загалом в приміщенні розташовано 19 окремих кімнат, не включаючи коридори загального користування. Висота стелі – 5 метрів, виконана з бетонного перекриття, а також влаштована підвісна система Армстронг з висотою 3 метри, стіни з цегли та перегородки з гіпсокартону.

Середня квадратура приміщень коливається від 15м^2 до 30м^2. Є 1 основний вхід до всіх кімнат, через контрольно-пропускний пункт (далі – КПП) з охороною.

Майже у всіх кімнатах є вікна, окрім вбиралень та серверної кімнати, як показано на рис. 3.4. Об’єкт знаходиться в експлуатації, тому сантехнічні та електричні роботи вже виконані, протипожежна сигналізація відсутня.

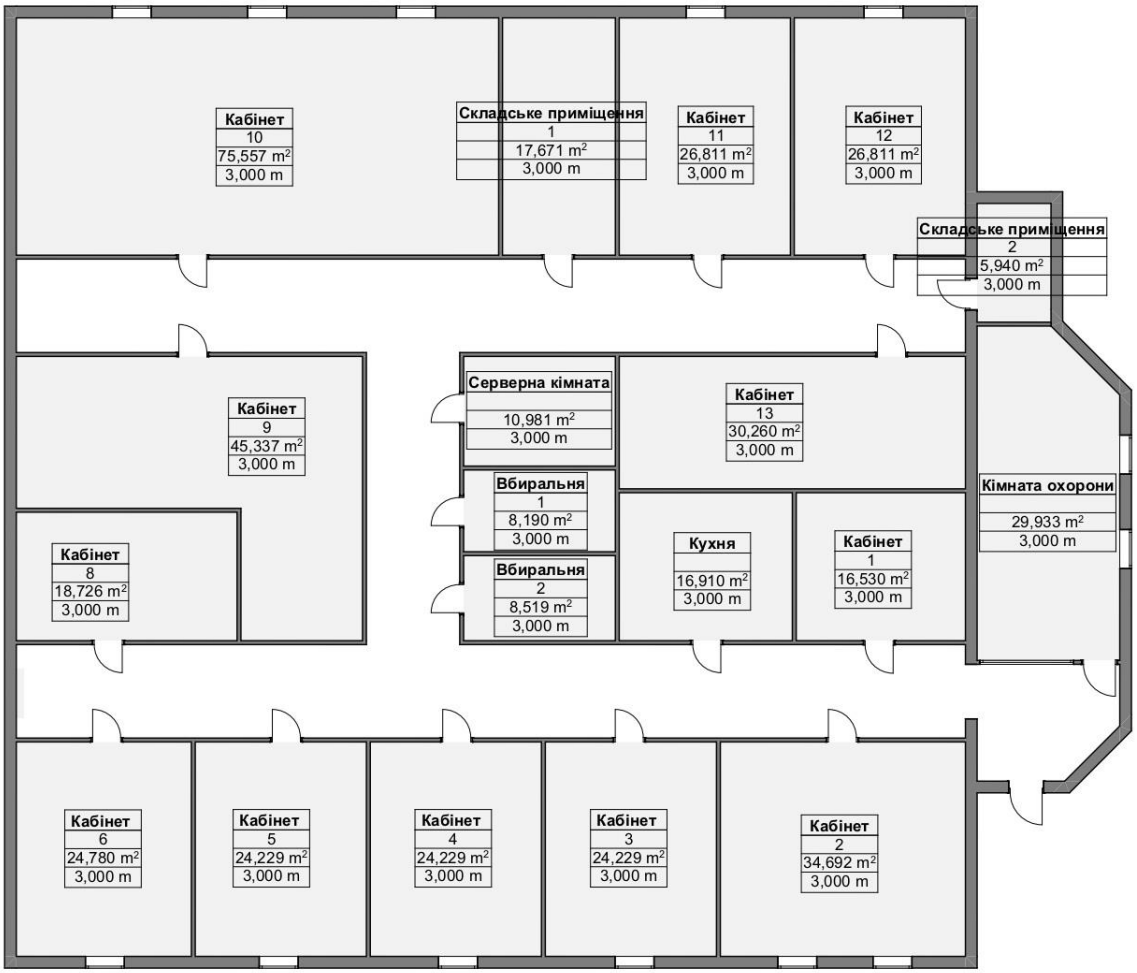


Рисунок 3.4 План офісів з розмірами

Метою цієї роботи є розробка плану, організація процесу та створення інструкцій для встановлення систем відеоспостереження та контролю доступу з інтеграцією штучного інтелекту.

Основну частину виконання роботи, її реалізації та налагодження системи буде відбуватись на вулиці, в серверній кімнаті, в кімнаті охорони, КПП та кабінеті директора, тому що там будуть знаходитись найважливіші вузли керування інформаційними системами, а також основні вимоги замовника. З

рештою кімнат будуть відбуватись однотипні та швидкі налагодження, тому про них буде менше згадано в цій роботі.

В табл. 3.1 показано призначення приміщення за номером на плані.

Таблиця 3.1

Призначення приміщень за нумерацією

Номер приміщення на плані	Призначення
1	Кімната охорони
2	Кабінет №01
3	Кабінет №02
4	Кухня
5	Кабінет №03
6	Кабінет №04
7	Кабінет №05
8	Кабінет №06
9	Вбиральня
10	Серверна кімната
11	Кабінет №08
12	Кабінет №09
13	Кабінет №10
14	Складське приміщення №1
15	Кабінет №11
16	Кабінет №12
17	Кабінет №13
18	Складське приміщення №2
19	Гараж

3.2 Проєктування систем безпеки

3.2.1 Серверна кімната

Проєктування ключових рішень у системах безпеки завжди розпочинається з визначення місця встановлення комунікаційної шафи або прокладання кабельних мереж.

Під час вибору місця для розміщення обладнання необхідно враховувати чималу кількість факторів. У випадку з цією будівлею, завдяки особливостям її проєктування, можна помітити на плані виділену серверну кімнату. Ця кімната оснащена системою кондиціонування та вентиляції, і повинна мати обмежений доступ та відкриватися лише оператором відеоспостереження, директором та охоронцем. Тому для розміщення обладнання обираємо саме це приміщення, як зазначено на рис. 3.5. Кожне відвідування серверної кімнати (далі – СК) повинно відбуватися в супроводі уповноваженої особи, щоб у разі виникнення непередбачених ситуацій або проблем забезпечити оперативне та правильне їх вирішення. Для додаткового контролю повинен вестись та прослідковуватись електронний журнал відвідувань.



Рисунок 3.5 Місце розміщення комунікаційної шафи

Для правильного облаштування серверної кімнати необхідно врахувати кілька ключових аспектів. Приміщення повинно мати оптимальне розташування, щоб забезпечити зручний доступ для обслуговування обладнання, але при цьому

доступ до нього має бути обмеженим для сторонніх осіб.

Зазвичай розмір кімнати підбирають відповідно до обсягу обладнання, з урахуванням можливості його майбутнього розширення. Необхідно забезпечити стабільне електропостачання із застосуванням джерел безперебійного живлення (далі – ДБЖ) для захисту серверів від перебоїв та стрибків у мережі. Також приміщення слід оснастити системою пожежогасіння, яка є безпечною для електронного обладнання, найкращим варіантом буде обладнати серверну газовими установками. Також варто передбачити організовану кабельну систему, використовуючи маркування і кабель-менеджмент, щоб спростити обслуговування в разі зміни спеціального працівника або обслуговуючої фірми. Особливу увагу слід приділити захисту серверної кімнати від зовнішніх загроз, таких як затоплення або крадіжки, тому рекомендується встановити датчики вологості, протікання, а також сигналізацію. Усі ці заходи забезпечують надійну роботу обладнання і зменшують ризики простоїв через несправності чи аварійні ситуації.

Щоб спростити організацію локальної обчислювальної мережі, серверну варто розміщувати в приміщенні, яке знаходиться в центральній частині офісу. Оптимальна висота стель у такій кімнаті повинна бути не менше 2,5 метра, що дозволить зручно встановити серверні стійки та забезпечити ефективне відведення тепла від обладнання. Відсутність вікон у цьому приміщенні є додатковою перевагою: у спекотну погоду кімната не буде перегріватися, а також підвищується рівень захисту від незаконного втручання.

Серверне приміщення має бути захищене від пилу та шкідливих речовин, які можуть негативно впливати на роботу та матеріали обладнання. Концентрація шкідливих речовин повинна відповідати гранично допустимим нормам. У разі потреби необхідно використовувати системи очищення та фільтрації повітря, які не допускають застосування масляних фільтрів.

Освітлення приміщення має бути не менше 500 люкс, виміряного на висоті одного метра від підлоги. Електроживлення освітлення та телекомунікаційного обладнання повинно здійснюватися від різних розподільних електрощитів, а світильники розташовуватись на стелі. Вимикачі для керування освітленням слід

встановлювати поруч із дверима на висоті 1,5 метра, уникаючи використання пристроїв плавного регулювання освітленості (димерів). Серверна повинна бути оснащена достатньою кількістю розеток вздовж стін, на висоті не нижче 15 см від підлоги. Електричні розетки мають витримувати змінний струм до 16А і живитися від різних кабелів. Електроживлення подається через виділений силовий кабель, бажано безпосередньо від головного розподільного щита. Для обладнання потужністю до 100 кВА допускається установка джерел безперебійного живлення (ДБЖ) у серверному приміщенні, а для потужності понад 100 кВА – в окремих кімнатах. Приміщення має бути обладнане магістральною телекомунікаційною заземлювальною шиною для підключення заземлюючих провідників від конструктивів, обладнання та металевих кабелепроводів.

Для організації кабельних потоків необхідно використовувати надійно закріплені кабелепроводи, які захищають кабелі та забезпечують мінімально допустимий радіус їх вигину, вони повинні бути відкритими та доступними для обслуговування, а після прокладання кабелів усі вводи мають бути герметично закриті вогнетривкими матеріалами. Стелі, стіни та перегородки серверного приміщення повинні бути виготовлені з негорючих матеріалів, що забезпечують вогнестійкість не менше 45 хвилин. Двері також мають відповідати вимогам вогнестійкості (не менше 36 хвилин), бути виготовленими з важкозаймистих матеріалів або оббитими сталлю. Приміщення повинно мати витяжні шахти площею не менше 0,2% від загальної площі, розташовані на відстані не більше 20 метрів від будь-якої точки кімнати. Фальшпідлоги, їх опори та стояки повинні бути виконані з вогнетривких матеріалів із межею вогнестійкості не менше 30 хвилин, хоча верхнє покриття може бути згоряємим.

3.2.2 Розробка системи відеонагляду

Наступним кроком є встановлення камер відеоспостереження як на території підприємства, так і всередині робочих приміщень. Усього планується встановити 34 камери, з яких 9 розташовуватимуться на вулиці, а 25 – у приміщеннях. Дві з

вуличних камер будуть слугувати виключно для сканування номерних знаків автотранспорту для автоматичного відкриття воріт без участі охоронця.

На рисунку 3.5 детально показане місце встановлення кожної камери разом із напрямками їхнього огляду.



Рисунок 3.5 План-схема розміщення камер відеонагляду

В табл. 3.2 розписані призначення камер, що присутні на плані, спосіб їх встановлення та висота, а також орієнтовний метраж кабеля. Це допоможе розрахувати попередні витрати а також обсяг робіт, дана процедура зручна для обох сторін, для замовника – це орієнтовний прорахунок, щоб знати, на яку суму розраховувати і на яку продовжуваність монтажних робіт, а для інсталяторів – розуміння, коли можна домовлятись про монтаж на нових об’єктах.

Таблиця 3.2

Призначення кожної камери в порядку нумерації

№ камери	Призначення	Спосіб встановлення	Висота встановлення (м)	Довжина кабеля (м)
1*	Розпізнавання номерних знаків транспортних засобів (на в'їзд)	Паркан, власний комутаційний бокс	3	60
2*	Розпізнавання номерних знаків транспортних засобів (на виїзд)	Паркан, власний комутаційний бокс	1,5	60
1	Оглядова камера поза межами паркану території (зустрічна до 2-ї)	Металева труба, комутаційний бокс з монтажною стрічкою	4	70
2	Оглядова камера поза межами паркану території (зустрічна до 3-ї)	Металева труба, комутаційний бокс з монтажною стрічкою	4	40
3	Оглядова камера території (зустрічна до 4-ї)	Металева труба, комутаційний бокс з монтажною стрічкою	4	70
4	Оглядова камера території (зустрічна до 3-ї)	Фасад будівлі, комутаційний бокс	3	26
5	Оглядова камера території	Металева труба, комутаційний бокс з монтажною стрічкою	4	40
6	Оглядова камера території	Фасад будівлі, комутаційний бокс	4	30
7	Оглядова камера входу в будівлю	Фасад будівлі, комутаційний бокс	3	30

Продовження таблиці 3.2

№ камери	Призначення	Спосіб встановлення	Висота встановлення (м)	Довжина кабеля (м)
8	Внутрішній огляд вхідного коридору	Стеля Армстронг	3	28
9	Внутрішній огляд коридору	Стеля Армстронг	3	26
10	Внутрішній огляд коридору	Стеля Армстронг	3	12
11	Внутрішній огляд коридору	Стеля Армстронг	3	13
12	Внутрішній огляд коридору	Стеля Армстронг	3	17
13	Внутрішній огляд коридору	Стеля Армстронг	3	10
14	Внутрішній огляд коридору	Стеля Армстронг	3	17
15	Внутрішній огляд кімнати охорони	Стеля Армстронг	3	17
16	Внутрішній огляд кабінету №1	Стеля Армстронг	3	11
17	Внутрішній огляд кабінету №2	Стеля Армстронг	3	26
18	Внутрішній огляд кухні	Стеля Армстронг	3	7
19	Внутрішній огляд кабінету №3	Стеля Армстронг	3	22
20	Внутрішній огляд кабінету №4	Стеля Армстронг	3	18

Продовження таблиці 3.2

№ камери	Призначення	Спосіб встановлення	Висота встановлення (м)	Довжина кабеля (м)
21	Внутрішній огляд кабінету №5	Стеля Армстронг	3	21
22	Внутрішній огляд кабінету №6	Стеля Армстронг	3	25
23	Внутрішній огляд серверної кімнати	Стеля Армстронг	3	3
24	Внутрішній огляд кабінету №7	Стеля Армстронг	3	7
25	Внутрішній огляд кабінету №8	Стеля Армстронг	3	5
26	Внутрішній огляд кабінету №9	Стеля Армстронг	3	25
27	Внутрішній огляд кабінету №9	Стеля Армстронг	3	13
28	Внутрішній огляд складського приміщення №1	Стеля Армстронг	3	15
29	Внутрішній огляд кабінету №11	Стеля Армстронг	3	17
30	Внутрішній огляд кабінету №12	Стеля Армстронг	3	20
31	Внутрішній огляд складського приміщення №2	Стеля Армстронг	3	18
32	Внутрішній огляд гаражу	Стеля приміщення	3	40

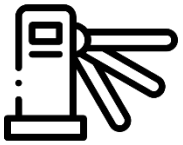
Камери були встановлені в кожному приміщенні (окрім вбиральні) без сліпих зон. Все розміщення камер є відносним і приблизним. Під час монтажу проявляться всі нюанси, що не зазначені на плані і розташування камер може трохи змінитись, але не критично. На плані та в таблиці камери «1*» та «2*» не входять до загальної нумерації, тому що вони не будуть підключатися до реєстратору для фіксації відеоархіву, а будуть встановленні лише для автоматичного відкриття та закриття воріт.

3.2.3 Розробка системи контролю доступом

Далі представлене розміщення основних та допоміжних охоронних датчиків та засобів, включно з: турнікетом, воротами (вже були встановлені на території), дверними дотягувачами та магнітними замками, датчиками руху, розбиття скла, затоплення, сповіщувальною сиреною, тощо. В табл. 3.3 наведені умовні позначення кожного з них.

Таблиця 3.3

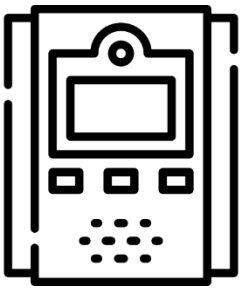
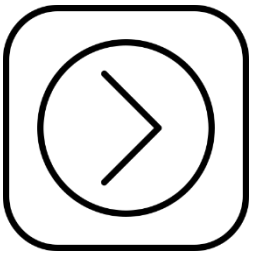
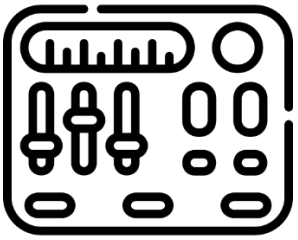
Умовні позначення складових охоронної системи

Тип складової	Умовне позначення
Турнікет	
Ворота	
Датчик руху	

Продовження таблиці 3.3

Тип складової	Умовне позначення
Охоронна централь	
Датчик розбиття скла	
Сирена	
Тривожна кнопка	
Датчик затоплення	
Зчитувач	
Електромагнітний замок з дотягувачем	

Продовження таблиці 3.3

Тип складової	Умовне позначення
Відеодомофон зі зчитувачем	
Кнопка виходу	
Контролер доступу	

Загалом потрібно змонтувати 12 датчиків руху по коловим кімнатам і коридорам, 13 датчиків розбиття на всі вікна, 2 датчики затоплення у вбиральнях , 1 охоронна централь та декілька контролерів доступу прямо в серверній, 1 сирену та тривожну кнопку біля охоронця і 1 кнопку в кабінеті директора, 1 турнікет на вході для зчитування облич. В деякі приміщення потрібен доступ лише уповноваженим особам, тому при вході в них було встановлено зчитувачі, дотягувачі з електромагнітними замками та кнопками виходу. На вході в територію потрібен домофон із зчитувачем для проходу відвідувачів (в яких немає електронного ключа і охоронець зможе їм відчиняти двері дистанційно) та працівників. До воріт будуть підключені 2 камери зчитування номерних знаків, але на екстренні випадки охоронець також зможе дистанційно їх відчинити. Не

дивлячись на те, що охоронець буде чергувати цілодобово, був встановлений базовий мінімум датчиків, що потрібні для повноцінного функціонування охоронної системи та упередженню пограбувань, актів вандалізму, тощо. На рис. 3.6 зображено точне розміщення складових повноцінної охоронної системи.

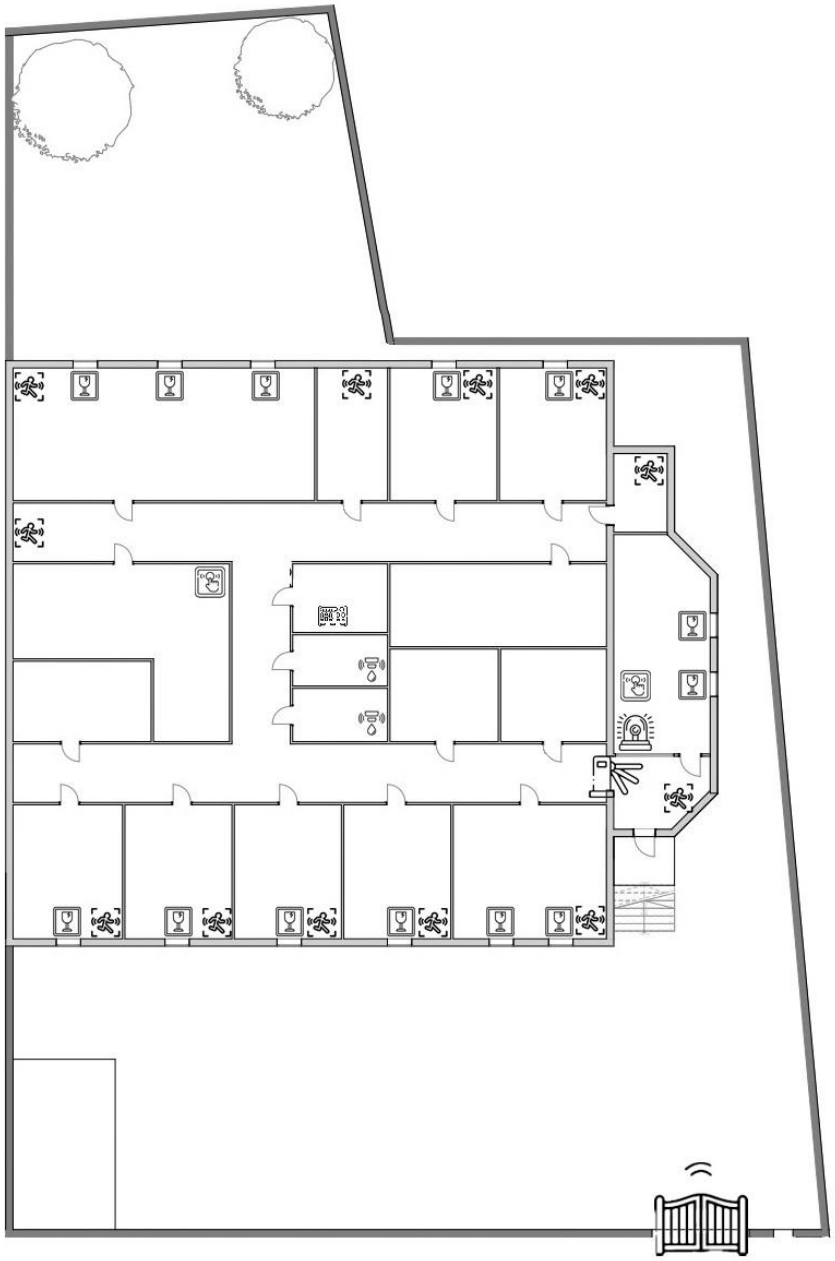


Рисунок 3.6 План-схема охоронної системи

А також на рис. 3.7 зображено точне розміщення системи контролю і управління доступом.

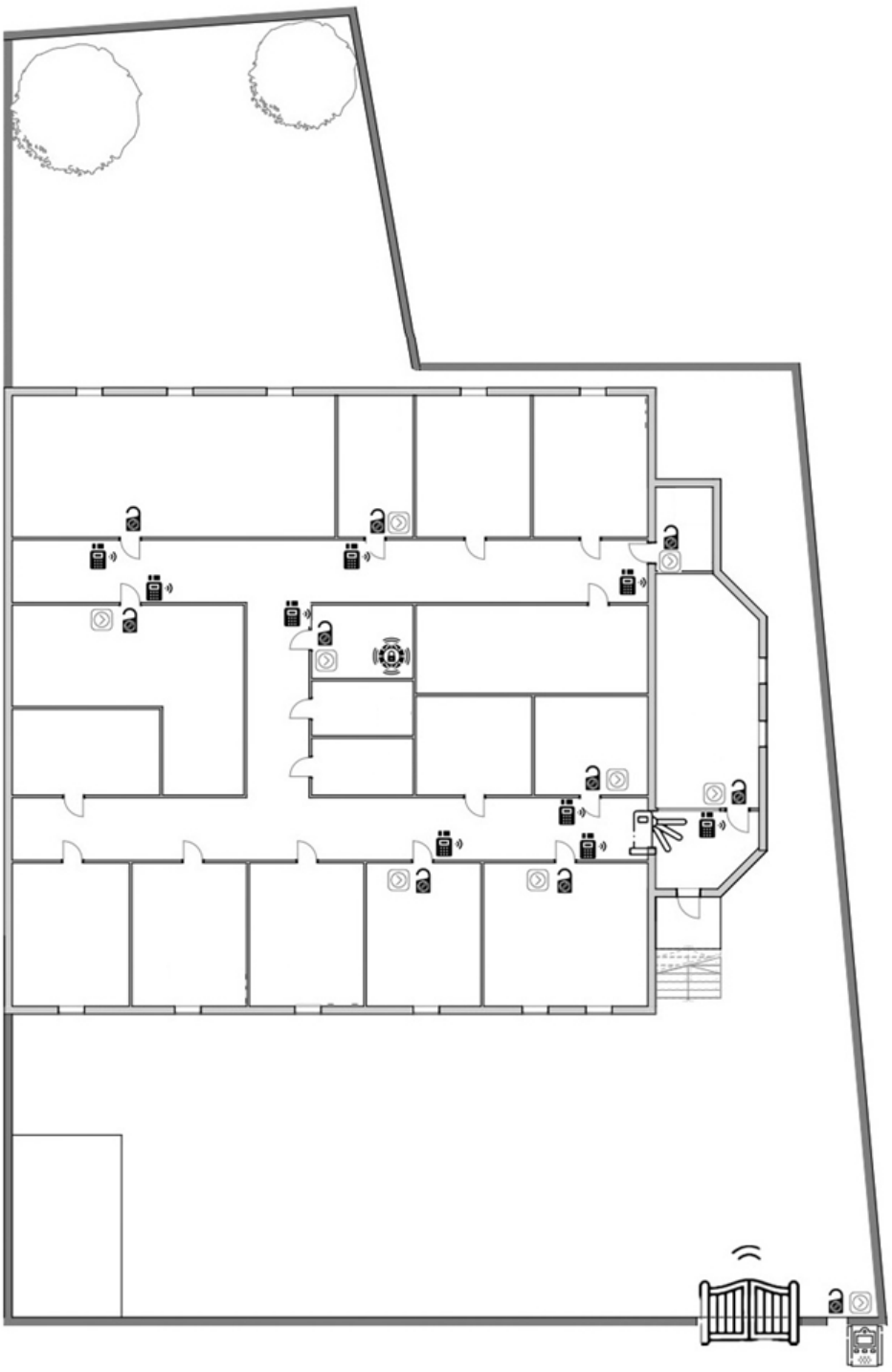


Рисунок 3.7 План-схема СКУД

3.3 Налаштування та монтаж обладнання з відеонагляду

Після завершення проєктування наступним етапом є монтаж системи, а власне сам монтаж починається з протягування кабельних мереж. Для монтажу

системи відеонагляду та камер всередині приміщень буде використано внутрішній F/UTP CAT5e кабель, він є оптимальним рішенням як і фінансово так і задач, які ставить перед собою інсталяція відеоспостереження, для монтажу вуличних камер буде використано зовнішній F/UTP CAT5e кабель. Внутрішній і зовнішній кабель категорії 5e відрізняються конструкцією та призначенням, внутрішній кабель має ПВХ-ізоляцію, яка не захищає від ультрафіолетового випромінювання та вологи, тоді як зовнішній покритий спеціальним матеріалом (зазвичай поліетиленом), стійким до впливу сонячного світла, дощу та механічних пошкоджень. Внутрішній кабель м'якший і гнучкіший, оскільки не потребує посиленого захисту, тоді як зовнішній жорсткіший через укріплену конструкцію. На рис. 3.8 зображена візуальна різниця між різними категоріями кабеля.

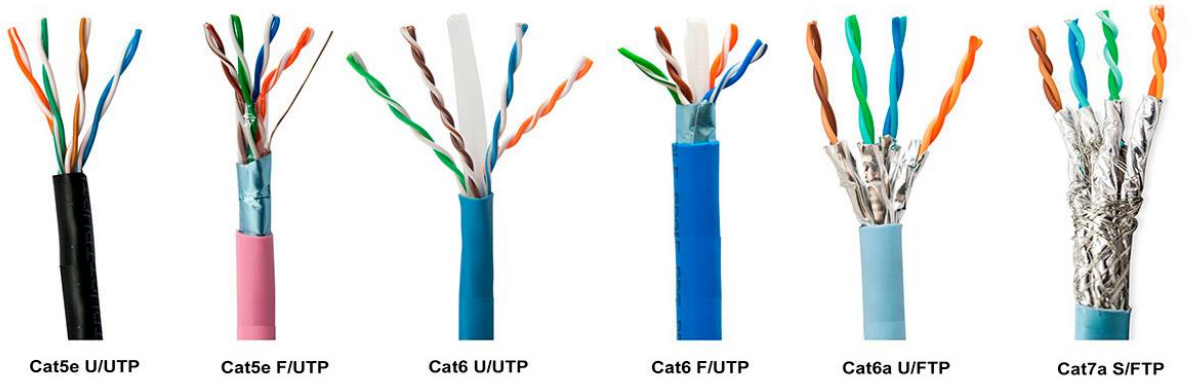


Рисунок 3.8 Візуальна різниця між різними категоріями кабеля

На рис. 3.9 схематично зображено траси прокладання кабелю різними кольорами, в якій червоним – вуличний кабель, зеленим – внутрішній.



Рисунок 3.9 План прокладання кабелів для відеонагляду

Коли всі кабелі заведені до серверної кімнати, можна приступати до встановлення та збору комутаційної шафи. Попередньо при прокладці кабелю потрібно залишати невеличкий запас від одного до трьох метрів з обох кінців на передбачувані випадки.

Далі потрібно підрахувати приблизну кількість обладнання яка буде в комутаційній шафі. Підрахувавши приходимо до висновку, що ідеальним варіантом буде настінна шафа на 9U. Юніт (U) – це одиниця вимірювання, яка використовується для опису висоти сервера, мережевого комутатора або іншого аналогічного пристрою, встановленого в стійці. Один юніт дорівнює 44,45 мм (1,75 дюйма). Обираємо перфоровану серверну шафу на 9U з розмірами 600 см на 450 см, її якраз вистачить на випадок розширення системи. На мою думку перфоровані дверцята краще справляються з вентиляцією ніж зашиті акриловим склом.

На рис. 3.10 представлена схема розміщення всього обладнання, яке буде встановлено в шафі, з урахуванням його габаритів. Шафа монтуватиметься на висоті 2,4 м від її нижньої частини, забезпечуючи доступ до неї лише за допомогою драбини.

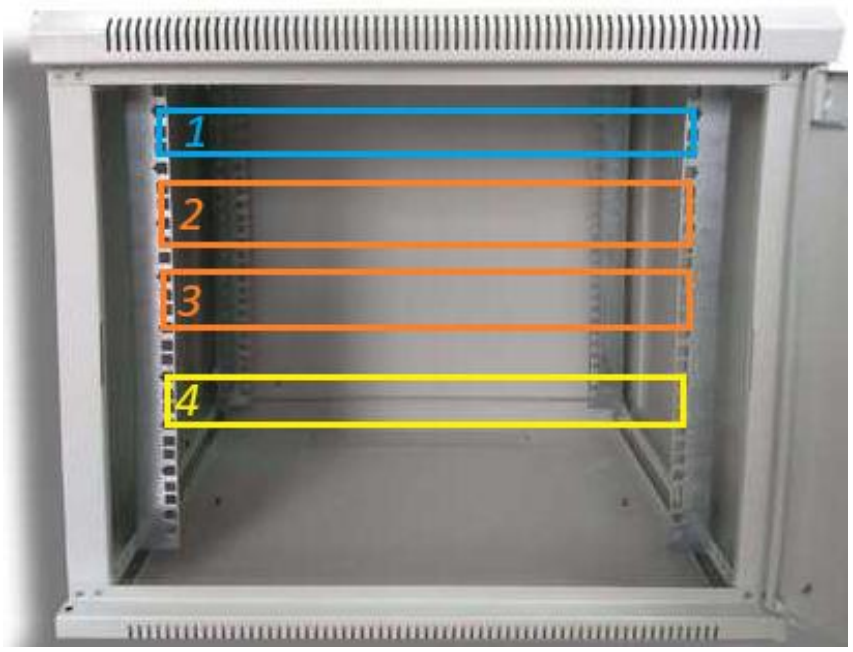


Рисунок 3.10 Схематичне зображення комутаційної шафи в зборі

На рис. 3.10 подовжувач схематично зображений в комірці «1».

Подовжувачі стійкового формату, такі як Ritar 1U-M6-K-GER, що зображений на рис. 3.11, зручні в використанні, бо закріплюються безпосередньо в стійку, а також дає змогу легко відслідкувати кількість приладів ввімкнених в

нього.

Загалом для підключення всіх пристроїв потрібно 3 розетки, але 6 було обрано про запас для майбутніх можливих розширень. Також важливим фактором є відсутність фізичного вимикача блоку, який захований за пластиковою накладкою, щоб уникнути випадкових вимкнень усієї системи.



Рисунок 3.11 Подовжувач мережі Ritar 1U-M6-K-GER 1,8 м, 6 розеток

Для підключення камер відеонагляду було обрано два 24-портових некерованих PoE комутатори Hikvision DS-3E0326P-E(C). Всього в даній схемі відеонагляду 34 камери та 1 реєстратор, тому було обрано 2 комутатори з загальною кількістю портів – 24, На рис. 3.10 комутатори схематично зображені в комірках «2» та «3». PoE комутатор дозволяє уникнути необхідності забезпечувати кожну камеру окремим блоком живлення, оскільки живлення та передача даних здійснюються через єдиний кабель витої пари. Важливою функцією цих комутаторів є «Watchdog», у пристроях Hikvision це вбудована функція, яка автоматично відстежує та підтримує стабільну роботу системи, забезпечуючи її безперебійність, якщо вона виявить якийсь збій в програмному забезпеченні або апаратній частині пристрою, вона автоматично повідомить про це та буде намагатись автоматично його відновити (наприклад перезавантажить порт).

На рис. 3.12 показано правильне підключення камер відеонагляду та інших пристроїв до комутаторів за портами та між собою.

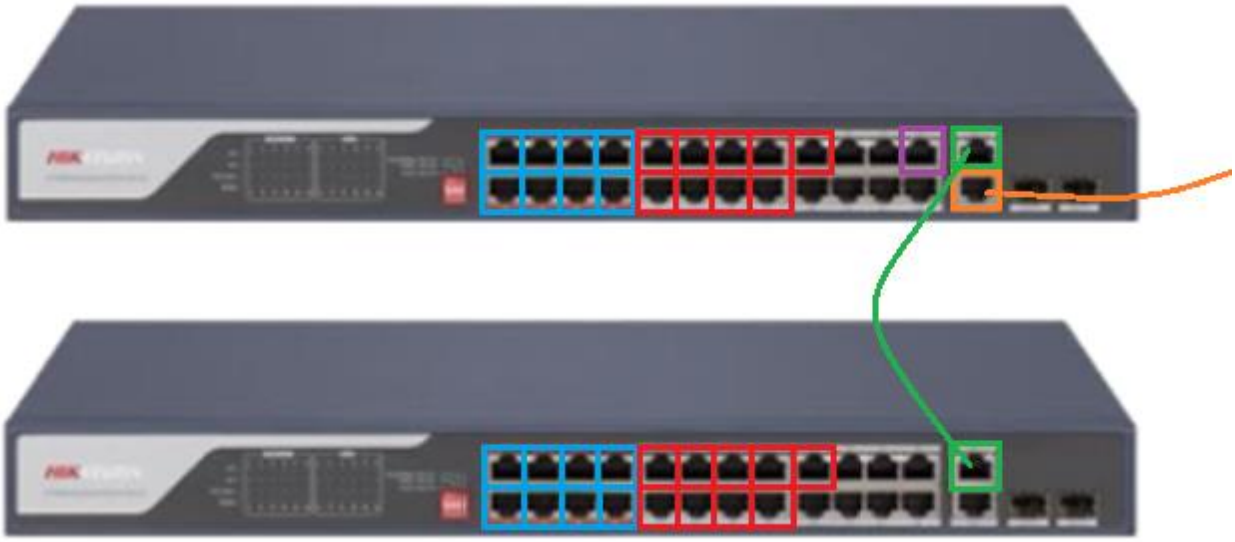


Рисунок 3.12 Схема підключення пристроїв до комутаторів між собою

Синім кольором позначені порти з функцією PoE+, що відрізняються від портів, що позначені червоним кольором з функцією PoE, більшою потужністю, тому камери, що мають більшу відстань від комутатора повинні підключатись в ці порти задля достатньої подачі живлення. Також важливим моментом є те, що камери підключені до портів у відповідності до свого розташування за планом, тобто камера №1 в перший порт, камера №2 в другий, камера №18 – 1-й порт другого комутатора і так далі. Фіолетовим кольором позначено реєстратор, який зазвичай підключиться в 23-24 порт першого комутатора, для того, щоб візуально відділити його від камер. 25-ті порти в обох комутаторах є перемичкою, для зв'язку між собою. 26-й порт першого комутатора з’єднує їх з основним комутатором або напряму роутером в мережі, який знаходиться в окремому місці.

Для забезпечення роботи камер відеоспостереження та збереження записів необхідний відеореєстратор, його вибір залежить від конкретних вимог. У даному випадку система включає 32 камери, тому реєстратор має підтримувати не менше 32 каналів. Існують моделі відеореєстраторів із різною кількістю каналів, зокрема на 4, 8, 16, 32 і більше.

64-канальний реєстратор Hikvision 8K ANPR POS RAID DS-9664NI-M8, що зображений на рис. 3.13, підтримує 64 канали з роздільною здатністю 2МП, але для

замовника важливо було мати чіткіше зображення в окремих зонах, а камери з роздільною здатністю 4МП забирають більше каналів. Реєстраторає місце для підключення 4-х жорстких дисків та підтримує кодек H.265+, на якому будуть працювати камери для економії місця та покращення якості зображення.



Рисунок 3.13 64-канальний Hikvision 8K ANPR POS RAID DS-9664NI-M8

Для збереження архіву на реєстраторі потрібні жорсткі диски спецільних серій, для фірми Western Digital це лінійка Purple, спроєктована для цілодобового запису з мережевих і цифрових відеореєстраторів. Ліміт робочого навантаження диска втричі вищий, ніж у звичайних дисків для настільних ПК. Виходячи з кількості камер та поставленої кількості днів архіву – 2 місяці за зробленими прорахунками всиановимо 4 жорстких диски Western Digital Purple Pro 18 TB 7200 rpm 512 MB WD181PURP 3.5 SATA III.

Перед встановленням реєстратора в шафу, схематично який зображений в комірці «4» на рис. 3.10, потрібно встановити та підключити жорсткі диски кабелями живлення та SATA з’єднати їх з материнською платою. Для попереднього налаштування реєстратора треба підключити його до мережі 220 В блоком живлення, який надається в комплекті та кабелем RJ-45 до мережі.

Для налаштування всіх пристроїв від компанії Hikvision потрібно попередньо одні й ті самі кроки, тому це буде продемонстровано 1 раз. Потрібно завантажити їхнє ПЗ під назвою SADP, за посиланням https://hikvision.org.ua/uk/zavantazhyty-

hikvision-sadp/. При запуску програми відразу відображаються всі пристрої, що знаходяться в одній мережі з пристроєм з якого відбувається налаштування, як показано на рис. 3.14.

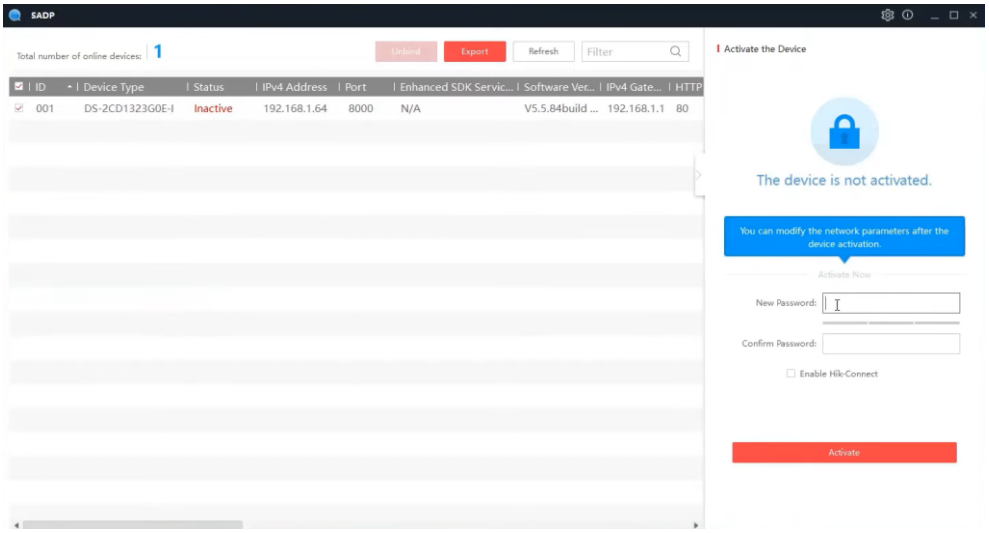


Рисунок 3.14 Меню активації пристроїв

Далі потрібно ввести та підтвердити пароль, ввести відповіді на контрольні питання або ввести резервну електронну адресу, які дають змогу відновити втрачений пароль. А також натиснути пташку «Enable Hik-Connect» для можливості зручного перегляду відео з мобільного телефону а також адміністрування пристроїв через веб-сайт. Після того, як реєстратор активовано, потрібно додати камери на реєстратор, для цього вони всі повинні бути підключені до комутатора. Також потрібно під’єднати мишку, що надається в комплекті до реєстратора і монітор або телевізор HDMI або VGA кабелем. Далі зайти в режим повного екрану реєстратора і натиснути на вкладку «Configuration», як показано на рис. 3.15.

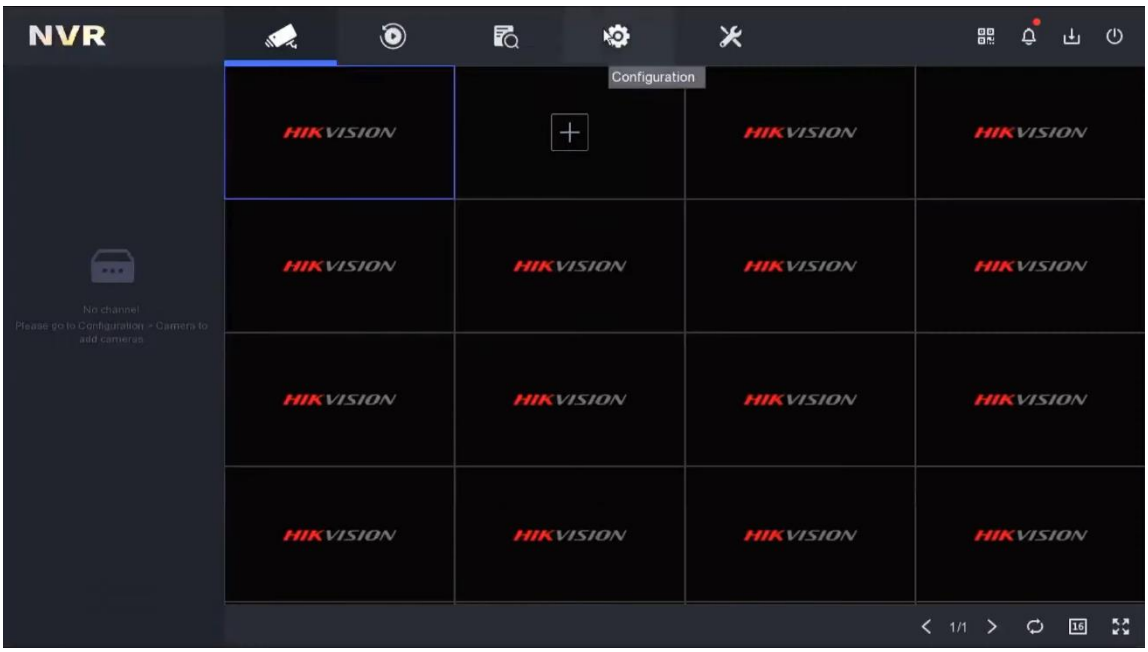


Рисунок 3.15 Головне меню повного екрану

Після цього знайти пункт «Camera», «IP Camera» та натиснути «Activate All» і ввести пароль, який задавали раніше на реєстраторі, потім всі камери покажуть свій статус і вони будуть готові до додавання, як показано на рис. 3.16.

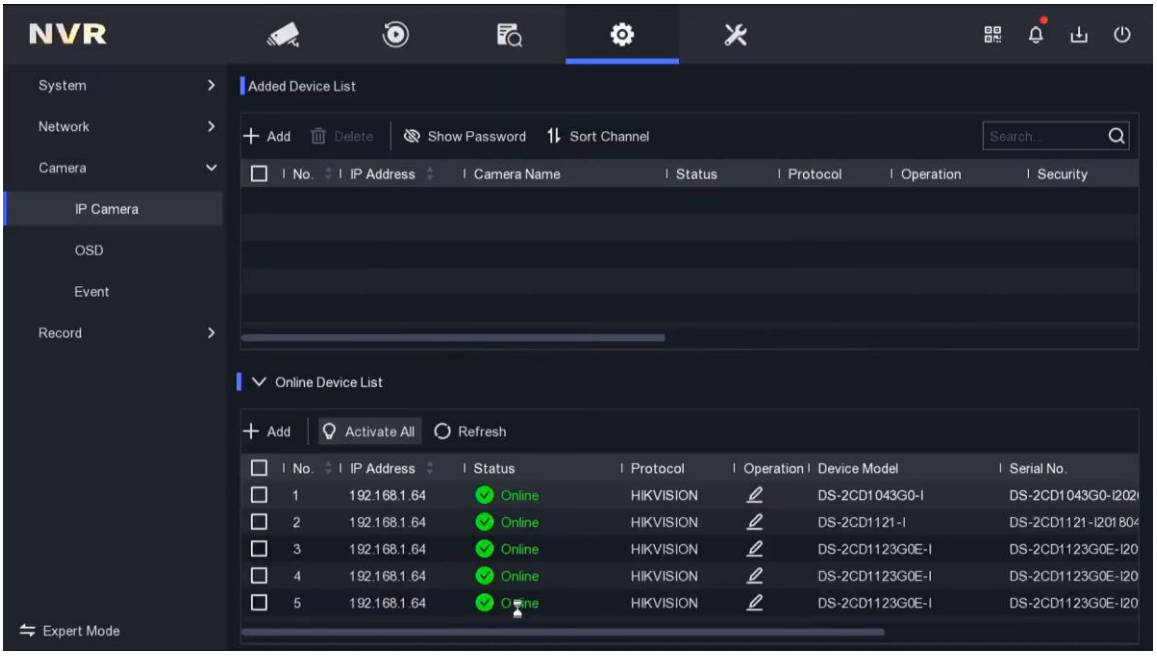


Рисунок 3.16 Статус камер

Далі через SADP буде видно IP-адресу кожної камери, потрібно в кожній камері прибрати пташку навпроти пункту «DHCP», щоб камери зафіксували свою адресу, а після цього на реєстраторі виділити їх всі і натиснути «Add». Щоб змінити порядок камер, потрібно натиснути на кнопку з зображенням олівця і змінити IP-адреси камер між собою.

В меню «System» можна змінити назву реєстратора (за бажанням) а також задати час відображення вручну, або за допомогою NTP сервера.

Для камер всередині приміщення, де потрібна проста відеофіксація буде використано камери Hikvision IP DS-2CD1321G0-I (2.8мм), яка зображена на рис. 3.17.



Рисунок 3.17 Камера Hikvision IP DS-2CD1321G0-I

Вона має відносно невелику ціну, компактний розмір і найголовніше кодек H.265+.

Для камер всередині приміщення, де вже потрібна покращена деталізація буде використано схожі камери Hikvision IP DS-2CD1341G0-I (2.8мм). Вони мають аналогічні характеристики та вигляд з попередньою камерою, окрім роздільною здатності в 4МП з покращеною матрицею.

В складських приміщеннях буде встановлена камера 2 МП AcuSense з мікрофоном DS-2CD2523G2-IS(D) (2.8мм), яка зображена на рис. 3.18.



Рисунок 3.18 Камера Hikvision DS-2CD2523G2-IS(D)

До її особливостей можна віднести наявність мікрофону, можливість підраховувати кількість осіб в заданій зоні, кодек H.265+. За проханням замовника в складах повинно перебувати одночасно не більше 1-ї людини, якщо ця умова не виконується камера викликає спрацювання тривоги.

Для якісного відеонагляду в нічний час на вулиці буде використовуватись камера 4 МП ColorVu Smart Hybrid Light DS-2CD1047G2H-LIUF (2.8мм), яка зображена на рис. 3.19.



Рисунок 3.19 Камера Hikvision DS-2CD1047G2H-LIUF

ColorVu Smart Hybrid Light – це сучасна технологія від компанії Hikvision, яка поєднує кольорове нічне бачення та гібридне підсвічування для забезпечення якісного відеоспостереження в умовах низької освітленості.

Камери з цією технологією використовують високочутливу матрицю та передову оптику, що дозволяє отримувати чітке кольорове зображення навіть у темряві. Вбудоване гібридне підсвічування автоматично перемикається між інфрачервоним і теплим LED-світлом залежно від ситуації. Інфрачервоне підсвічування використовується, коли потрібен ненав’язливий режим, щоб уникнути засвічення території, а тепле LED-світло активується, якщо необхідно отримати детальне кольорове зображення. Також в ній є вбудований ШІ, який здатний сигналізувати в разі виявлення потенційного саботажу.

Для автоматичного відкриття воріт будуть встановлені камери з функцією розпізнавання номерних знаків (ANPR), камера Hikvision 4 МП ANPR ІЧ варіофокальна iDS-2CD7A46G0/P-IZHS (C) (2.8-12мм) зображена на рис. 3.20.



Рисунок 3.20 Камера Hikvision iDS-2CD7A46G0/P-IZHS (C)

Всі вуличні камери мають металевий корпус, а з'єднання з витою парою буде заховане в комутаційний бокс, на який і безпосередньо будуть вішатись камери. Всі камери матимуть фокусну відстань 2.8 мм, її можна назвати еталонною, вона ідеально підходить для відеофіксації як в приміщенні так і на вулиці, лише ANPR-камери можуть змінювати її, тому що вони мають варіофокальний об’єктив, що допоможе краще налаштувати кут огляду камери при монтажі.

Після встановлення камер потрібно зайти знову на реєстратор в пункт «Congifuration», «Record», «Parameter» і виставити там обов’язково максимально допустиму роздільну здатність, кількість кадрів на секунду а також увімкнути кодек H.265+, як показано на рис. 3.21.

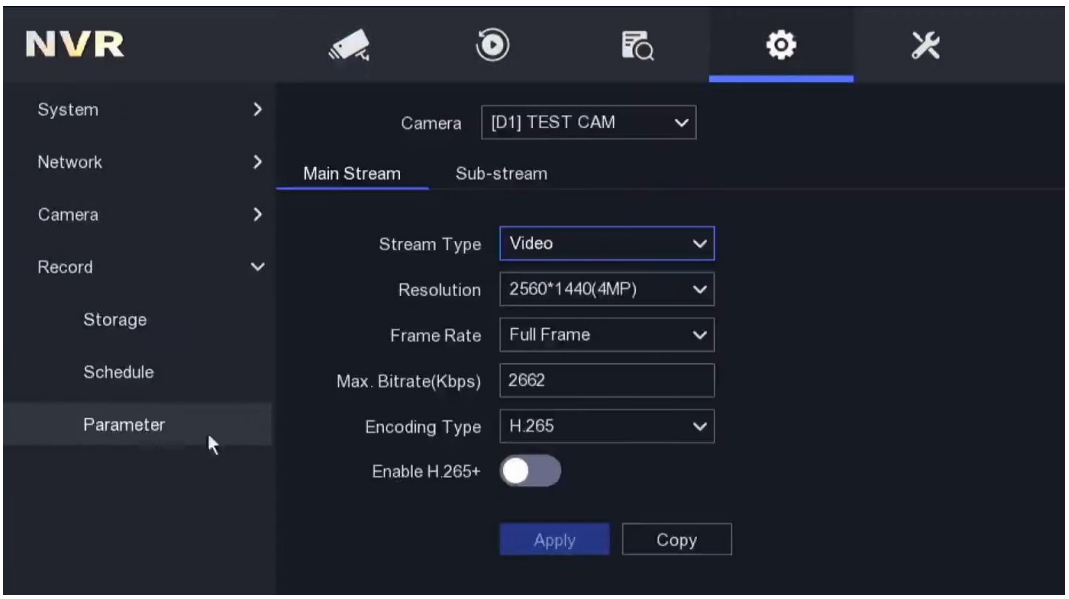


Рисунок 3.21 Налаштування параметрів камер

А також зайти знову «Schedule» і виставити там постійний запис всіх каналів. Після цього зайти в вкладку «Storage» та підготувати жорсткі диски до запису повністю почистивши та ініціалізувавши їх.

Для підключення камер кожний кінець кабеля обтискається разом з конекторами RJ-45 спеціальним інструментом, що має назву кримпер. Для цього потрібно зняти ізоляцію, і розставити кожну жилу за порядком, як вказано на рис. 3.22.

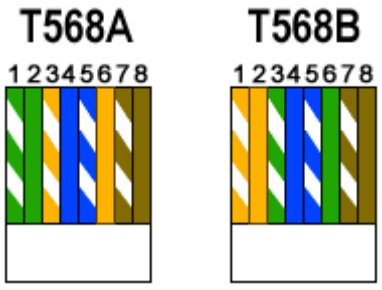


Рисунок 3.22 Типи обтискання кабеля

Існує 2 прийнятих стандарти обтискання: «А» і «В», в Україні популярніший тип «В», сильної різниці немає, але якщо якась обслуговуюча компанія чи

спеціаліст буде виправляти несправність, більшість з них будуть розраховувати на тип «B», але головне, щоб 2 кінці конектору були обтиснуті однаково.

Для того, щоб підключити ANPR-камери до автоматичних воріт, потрібно підключити з боку камери роз'єми «Alarm output 1A» та «Alarm output 1B» і з боку блоку керуванням воротами в роз'єми «Open control +» та «Open control -», як показано на рис. 3.23.

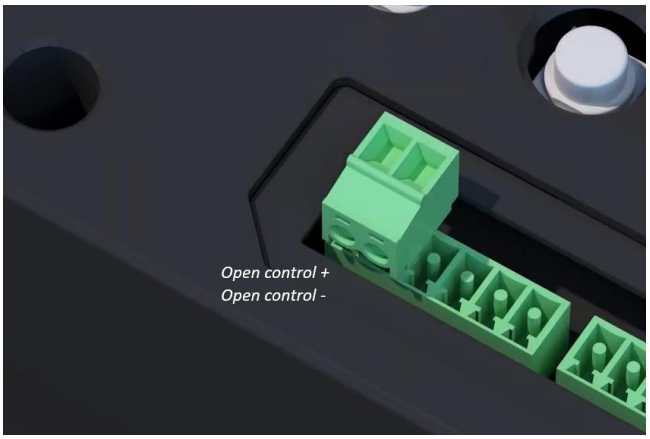


Рисунок 3.23 Схема підключення ANPR-камери

Після цього потрібно прив'язати ці входи до дії відкривання воріт, в пункті «Event», «Basic Event», «Alarm Input» а також «Alarm Output», як показано на рис. 3.24.

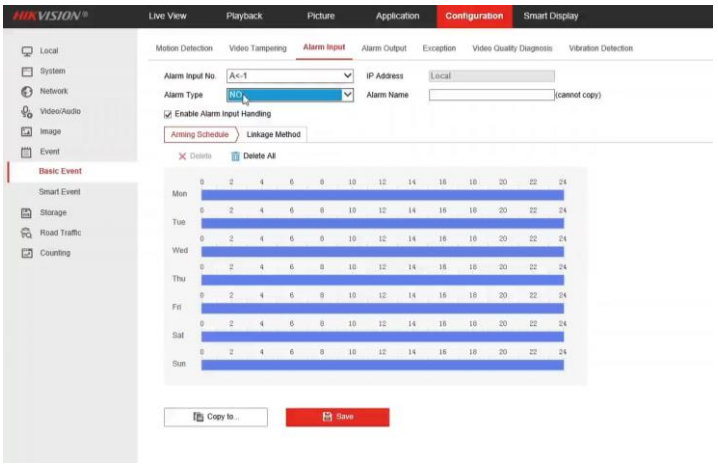


Рисунок 3.24 Прив'язування воріт до камери

Для того, щоб налаштувати список автомобілів, які можуть заїжджати на територію, потрібно в меню налаштувань ANPR-камери, яка буде направлена на в'їзд на територію, зайти в пункт «Road Traffic» і включити детекцію натиснувши на прапорець «Enable», а також вибрати зону, в якій буде зчитуватись номерний знак, після чого в пункті регіону обрати «CIS Region» для коректної роботи з українськими номерними знаками, а також в режимі «Blacklist and Whitelist» ввести номера потрібних авто, як показано на рис. 3.25. В камері, що буде направлена на виїзд з території потрібно просто ввімкнути детекцію і вона автоматично буде випускати всі автомобілі.

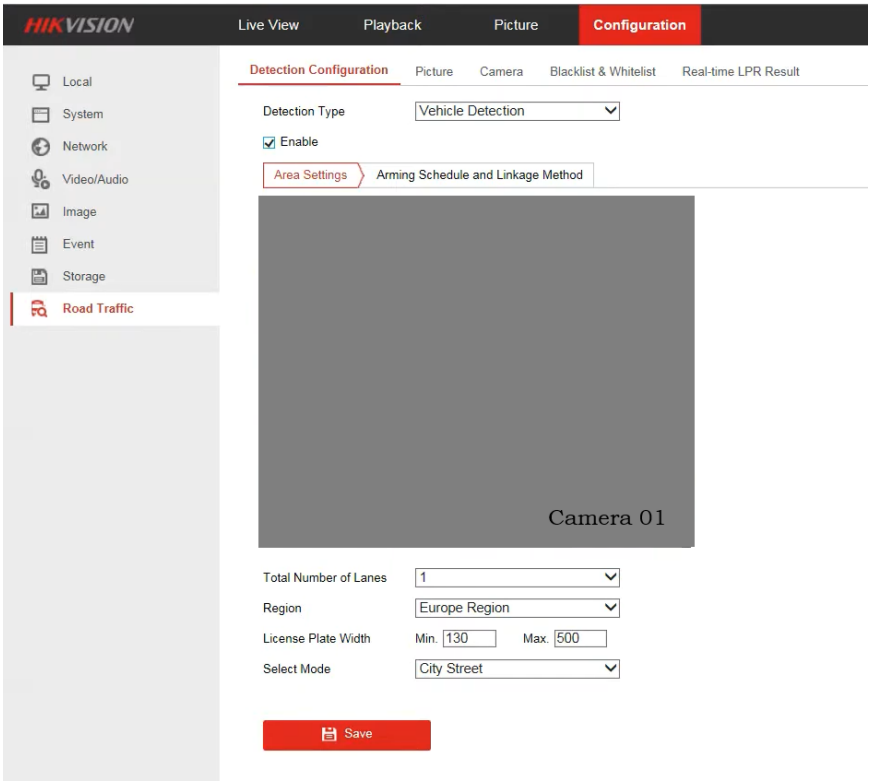


Рисунок 3.25 Меню налаштування ANPR-камери

Перегляд камер для охорони буде відбуватись наступним чином: в кімнаті охорони буде встановлено ПК з двома моніторами. На персональний комп'ютер буде встановлено ПЗ IVMS-4200. Далі після завантаження буде створений профіль з певними правами доступу, після чого додані всі камери в потрібній та зручній послідовності.

Мінімальні системні вимоги ПК для підтримки програми IVMS-4200:

- операційна система: Microsoft Windows 7 / Windows 8.1 / Windows 10 (32-біта або 64-біта), Microsoft Windows XP SP3 (32-біта), Microsoft Windows 2008 R2 / Windows Server 2012 (64-біта);
- ЦПП: Intel Pentium IV 3.0 ГГц або вище;
- пам'ять: 2 Гб або вище ;
- відеокарта: RADEON X700 Series або вище;
- графічний процесор: 256 МБ або вище.

3.4 Налаштування та монтаж обладнання охоронної системи

На вході планується встановлення двопрохідного розсувного турнікета Hikvision DS-K3B801BX, що зображений на рис. 3.26, який забезпечує зручний і одночасний рух в обох напрямках. Турнікет також дозволяє спрощувати контроль проходів для охорони та забезпечує автоматичне розпізнавання облич за допомогою камери зі штучним інтелектом, що дозволяє системі контролю доступу (СКУД) працювати без втручання сторонніх осіб.



Рисунок 3.26 Турнікет Hikvision DS-K3B801BX

Він ідеально підходить за розмірами, легко встановлюється, такоє нього є вбудований зчитувач пропусків та QR-кодів, завдяки цьому можна створити через додаток QR-код та надіслати відвідувачу, відредагувавши його дозволи та час роботи перепустки і найголовнішим його плюсом є те, що до нього можна прикріпити різні модулі, які будуть між собою співпрацювати та допомагати отримати кращий досвід використання турнікету. Один із таких буде встановлено на даному підприємстві, він має назву Hikvision DS-K5671-ZU, що зображений на рис. 3.27.



Рисунок 3.27 Модуль розпізнавання обличчя DS-K5671-ZU

Він має 7-дюймовий РК-сенсорний екран, 2-мегапіксельну камеру з роздільною здатністю 1080P. За допомогою штучного інтелекту має можливість автоматично фокусуватись та самоадаптуватись до людей різної статури, має пам’ять на 20 000 облич, а також 50 000 подій, використовуючи алгоритм глибокого навчання. Відстань розпізнавання обличчя: 0,3 м ~ 3 м.

Як і у випадку з камерами та реєстратором, турнікет потрібно спочатку активувати за допомогою програми SADP, можна змінити IP-адресу вручну, або дозволити йому взяти її автоматично. Перейшовши за цього IP-адресою через веб-переглядач можна швидко змінити його назву, задати час, та вручну відкрити чи

закрити одну з секцій, потім ввести дані про адміністратора.

Для початку роботи модуля розпізнавання обличчя потрібно кожного користувача додати до бази, потім в разі чого система дозволяє гнучко адмініструвати дозволи та відомості про кожного співробітника і головне фіксувати час його роботи та швидко розпізнавати надаючи доступ до примішення.

Щоб додати користувача, потрібно зайти в вкладу «Person Management» та натиснути «Add». Після цього в вікні, яке зображене на рис. 3.28, можна починати запонювати профіль користувача, ввести його ПІП, стать (якщо потрібно), тип прав дозволів, прив’язати відразу фізичнку картку та просканувати обличчя.

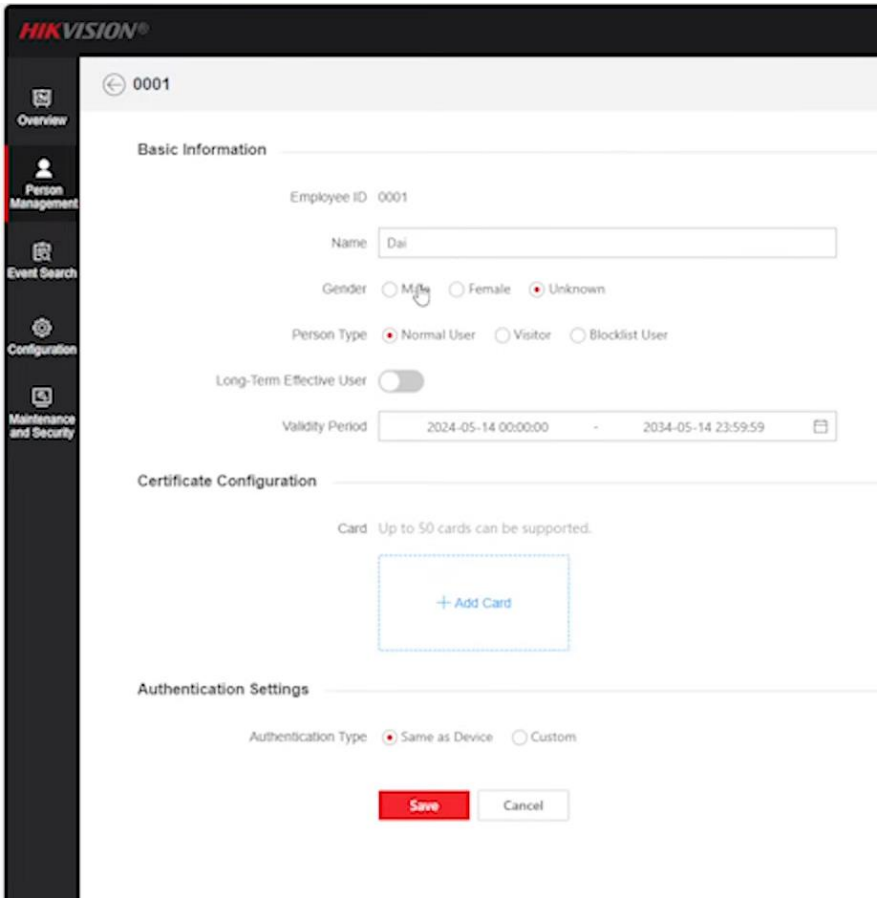


Рисунок 3.28 Меню додавання користувача

Далі при входах в деякі кабінети будуть змонтовані зчитувачі та електромагнітні замки з кнопками виходу та доводчиками автоматичного для контролю доступу.

Зчитувач моделі Hikvision DS-K1802M, що зображений на рис. 3.29, потребує додаткового встановлення контролера, тому що він може лише зчитувати та передавати інформацію, для решти функцій потрібні потужності контролеру.



Рисунок 3.29 Зчитувач Hikvision DS-K1802M

В якості контролера буде використано Hikvision DS-K2604T, це контролер для 4-х дверей, всього на об’єкті 9 дверей, тому потрібно встановити 3шт. На рис. 3.30 зображена схема роз’ємів, куди потрібно буде виконувати підключення.

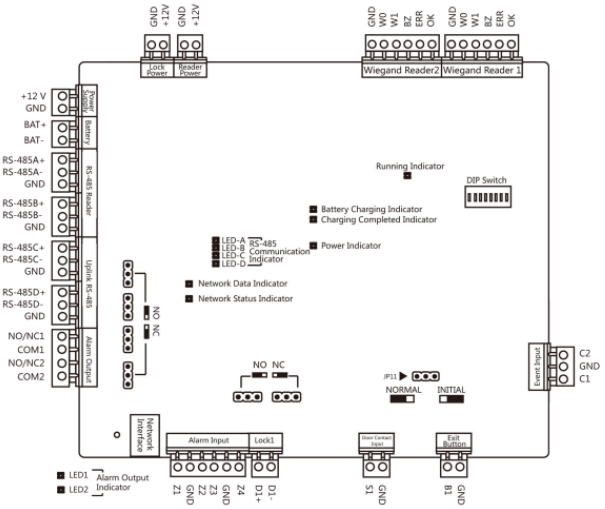


Рисунок 3.30 Схема роз’ємів Hikvision DS-K2604T

В роз’ємний клемник «Power Supply» потрібно подати живлення 12В з силою струму не менше 9А, в клемник «Wiegant Reader 1 та 2» підключаємо зчитувачі відповідно до маркування, в клемник «Exit Button» кнопку виходу, в «Alarm Output» електромагнітний замок.

Для реалізації кнопок виходу потрібно використати, SEVEN K-7497ND, вона сенсорна, що полегшує відкриття, а також має гарний дизайн.

В якості реалізації електромагнітного замку було використано YM-180N(LED), він має світловий індикатор, що полегшує орієнтування, щодо стану дверей (відкриті чи закриті), має сили втримання 180кг, що з запасом вистачає для офісних дверей, а також живиться від 12В, що дає змогу підключити його напряму в наш контролер.

Базовою охоронною системою, що буде спрацьовувати в разі певних тривог було обрано рішення від фірми Ajax. Всіма датчиками керує головна централь Ajax HUB, яка зображена на рис. 3.31, її буде змонтовано в серверній кімнаті і вже до неї будуть підключатись всі датчики та сирени, на хаб можна додати до 100 пристроїв Ajax, які захищають об’єкт від вторгнення, пожежі, затоплення, а також дають змогу керувати електроприладами автоматично за сценаріями або вручну через застосунки Ajax.



Рисунок 3.31 Охоронна централь Ajax HUB

Щоб додати пристрій до Ajax Hub, потрібно відкрити мобільний застосунок Ajax, авторизуватись або зареєструватись, перейти до розділу "Пристрої", натиснути "Додати пристрій". Ввести назву пристрою (може слугувати підказкою, де він знаходиться), відсканувати QR-код, що знаходиться на кожному пристрої або ввести серійний номер вручну і вибрати кімнату, далі увімкнути пристрій і дочекатися його підключення до хабу. В якості датчиків затоплення було обрано Ajax LeaksProtect, які будуть встановленні у вбиральнях, датчиків розбиття скла –

Ajax GlassProtect, датчиків руху – Ajax MotionProtect. А в разі екстрених випадків 2 кнопки Ajax Button та сирена Ajax HomeSiren.

3.5 Розрахунок загальної вартості системи

Розрахунок загальної вартості СКУД та системи відеонагляду, що описаний в табл. 3.4, є орієнтовним, тому що більшість комплектуючих замовляються з інших країн, відповідно ціни на них формуються в залежності від курсу гривні до інших валют.

Також орієнтовною є вартість робіт, все залежить від рахунків, які можуть виставити різні інсталятори, або обслуговуючі компанії.

Таблиця 3.4

Загальна вартість комплектуючих та матеріалів

№	Опис	Ціна (грн)	Кількість	Сума (грн)
Система відеонагляду				
1	Відеокамера Hikvision iDS-2CD7A46G0/P-IZHS (C)	34 440	2	68 800
2	Відеокамера Hikvision DS-2CD1047G2H-LIUF	3935	7	27 545
3	Відеокамера Hikvision IP DS-2CD1321G0-I	2537	24	60 888
4	Відеокамера Hikvision DS-2CD2523G2-IS(D)	5590	1	5590
5	Кабель мережевий OK-Net FTP cat.5e, 305м	4800	3	14 400
6	Конектор RJ45 cat.5e UTP 8P8C * 100 Cablexpert	249	1	249
7	Серверна шафа 9U 600x350x503, перфорована, сіра	4300	1	4300
8	Подовжувач мережі Ritar 1U-M6-K-GER 1,8 м, 6 розеток	819	1	819

Продовження таблиці 3.4

№	Опис	Ціна (грн)	Кількість	Сума (грн)
Система відеонагляду				
8	Комутатор Hikvision DS-3E0326P-E(C)	15 287	2	30 574
9	64-канальний відеореєстратор Hikvision 8K ANPR POS RAID DS-9664NI-M8	8 0696	1	80 696
10	Жорсткий диск Western Digital Purple Pro 18 TB 7200 rpm 512 MB WD181PURP 3.5 SATA III	19 228	4	76 912
Загальна сума по відеонагляду:				*370 773 грн*
СКУД				
1	Турнікет Hikvision DS-K3B801BX	372 256	1	372 256
2	Модуль розпізнавання обличчя Hikvision DS-K5671-ZU	70 473	1	70 473
3	Зчитувач Hikvision DS-K1802M	1058	9	9522
4	Контролер доступу Hikvision DS-K2604T	14 100	3	42 300
5	Кнопка SEVEN K-7497ND	635	10	6350
6	Електромагнітний замок Yli Electronic YM-180N(LED)	1421	9	12 789
7	Панель виклику Hikvision DS-KV6113-WPE1(C)	6411	1	6411
8	Кабель сигнальний Одескабель W 8x0.22 CU, екранований 100 м (YT35243)	1830	3	5490
Загальна сума по СКУД:				*525 591 грн*
Охоронна система				
1	Охоронна централь Ajax Hub White	6699	1	6699
2	Датчик руху Ajax MotionProtect white	1719	12	20 628
3	Датчик розбиття Ajax GlassProtect white	2009	13	26 117

Продовження таблиці 3.4

№	Опис	Ціна (грн)	Кількість	Сума (грн)
4	Датчик затоплення Ajax LeaksProtect white	1609	2	3218
5	Бездротова тривожна кнопка Ajax Button white	999	2	1998
6	Бездротова кімнатна сирена Ajax HomeSiren white	2009	1	2009
Загальна сума по охоронній системіі:				*60 669 грн*
Загальна сума:				*957 033 грн*

Загальний та орієнтовний прорахунок вартості робіт, описаний в таблиці 3.5.

Таблиця 3.5

Загальна вартість монтажних робіт

№	Опис	Ціна (грн)	Кількість	Сума (грн)
Система відеонагляду				
1	Монтаж камери всередині приміщення	600	25	15 000
2	Монтаж камери на вулиці	900	9	8100
3	Монтаж комутаційного боксу	150	9	1350
4	Прокладання кабеля	20	886	17 720
5	Обтискання конекторів	68	10	680
6	Встановлення серверної шафи	500	1	500
7	Монтаж елементів всередині шафи	100	4	400
8	Налаштування реєстратора	500	1	500
9	Налаштування обладнання	10 000	1	10 000
Загальна сума по монтажу відеонагляду:				*54 250 грн*

Продовження таблиці 3.5

№	Опис	Ціна (грн)	Кількість	Сума (грн)
СКУД				
1	Встановлення турнікету	2500	1	2500
2	Встановлення зчитувача	200	9	1800
3	Встановлення кнопки	130	10	1300
4	Встановлення доводчика	300	9	2700
5	Встановлення електромагнітного замка	280	9	2520
6	Встановлення та підключення контролеру доступу	2000	3	6000
7	Встановлення панелі виклику	1000	1	1000
8	Прокладання кабеля	20	276	5520
9	Налаштування обладнання	1	5000	5000
Загальна сума по монтажу СКУД:				*28 240 грн*
Охоронна система				
1	Встановлення та підключення охоронної централі	1000	1	1000
2	Встановлення та підключення датчиків	200	27	5400
3	Встановлення сирент	300	1	300
Загальна сума по монтажу охоронної системи:				*6700 грн*
Загальна сума по всім монтажним роботам:				*89 460 грн*

ВИСНОВКИ

У процесі написання кваліфікаційної роботи проведено детальний аналіз існуючих рішень у сфері біометричних систем контролю та управління доступом, що базуються на штучному інтелекті. Досліджено сучасні системи, їхній вплив на суспільство, а також динаміку розвитку технологій у цій галузі.

У першому розділі було проведено всебічний аналіз основних аспектів штучного інтелекту. Розглянуто його історичний розвиток, що включає ключові етапи становлення та формування технології, яка сьогодні активно впроваджується в різні сфери. Проаналізовано провідні галузі застосування ШІ, серед яких виокремлено сферу безпеки, де використання штучного інтелекту демонструє високий потенціал для автоматизації процесів і підвищення ефективності. Також було приділено увагу вразливостям і недосконалостям ШІ, які можуть впливати на його надійність та створювати ризики, особливо у випадках впровадження в критично важливі системи. Отримані результати стали основою для подальшого дослідження інтеграції ШІ в системи управління доступом.

У другому розділі поглиблено було досліджено СКУД на базі штучного інтелекту. Розглянуто основні завдання цих систем, зокрема забезпечення безпеки об’єктів шляхом автоматизації процесів доступу. Проаналізовано технологічні особливості сучасних СКУД, включаючи їхні структурні компоненти, які формують основу функціонування таких систем. Окрему увагу приділено використанню аксесуарів, які покращують функціональність і зручність систем. Висвітлено особливості монтажу СКУД, які є критичними для забезпечення коректної роботи системи. Завершує розділ аналіз інтеграції штучного інтелекту в автоматизовані системи управління доступом, що дозволяє значно підвищити їхню ефективність і адаптивність до потреб користувачів.

Результатом роботи в третьому розділі стала інтегрована система на базі обладнання від фірми Hikvsion, яка забезпечує не лише контроль доступу, але й відстеження кількості присутності осіб (за допомогою камери Hikvision DS-

2CD2523G2-IS(D)) та транспортних засобів із використанням алгоритмів штучного інтелекту (за допомогою камери Hikvision iDS-2CD7A46G0/P-IZHS (C)) . Розроблені план-схеми відеонагляду, СКУД та охоронної системи, що дозволяють оптимально розмістити обладнання при мінімізованих витратах, забезпечуючи 100% використання потенціалу системи при взаємодії елементів. Також було проведено розрахунок вартості кожної з систем, загалом вона становить 957 033 гривень, а також було проведено розрахунок орієнтовної вартості монтажних робіт, вони обійшлись в 89 460 гривень. Загальна вартість цього комплексу під ключ виходить близько 1 046 493 гривень, що є чималою сумою, але якщо розуміти її потенціал і те, скільки вона зможе зекономити в перспективі дає розуміння, що це вигідна інвестиція.

Практичний потенціал впровадження цієї системи має велике значення через свою універсальність в застосуванні, тому вона може бути адаптована для різних сфер. У майбутньому можливе розширення функціональності системи через інтеграцію додаткових біометричних методів, такі як: відбитки пальців, райдужна оболонка ока, тощо. Також можлива заміна камер базових моделей на більш просунуті аналоги з покращеною аналітикою та роздільною здатністю.

Загалом ця кваліфікаційна робота стала внеском у розвиток інтелектуальних систем безпеки, які здатні адаптуватися до сучасних викликів і забезпечувати високий рівень надійності та зручності у використанні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Романенко К. Еволюція штучного інтелекту (ШІ): Визначні моменти в історії та застосування. *CASES*. URL: https://cases.media/en/article/evolyuciya-shtuchnogo-intelektu-shi-viznachni-momenti-v-istoriyi-ta-zastosuvannya
2. Generative AI could raise global GDP by 7%. *Home | Goldman Sachs*. URL: https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent.html
3. Ключові переваги ШІ-прокторингу для онлайн-навчання | Constructor Technology. *Constructor Technology*. URL: https://constructor.tech/ua/node/294
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
5. Переваги та недоліки штучного інтелекту. *Ardenis agency - We Provide Unique Effective Solutions*. URL: https://ardenis.com.ua/blog/shtuchnyj-intelekt-shi-perevagy-ta-nedoliky-chastyna-1/
6. Про переваги та недоліки штучного інтелекту у навчальному процесі. *behindthenews.ua*. URL: https://behindthenews.ua/spetsproiekti/po-toy-bik-novin-kids/pro-perevagi-ta-nedoliki-shtuchnogo-intelektu-u-navchalnomu-protsesi-720/
7. Introducing OpenAI. *OpenAI*. URL: https://openai.com/index/introducing-openai/
8. Contributors to Wikimedia projects. Stable Diffusion - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Stable_Diffusion
9. Астраханцев А., Ляшенко Г. Дослідження ефективності методів біометричної автентифікації. *ResearchGate*. URL: https://www.researchgate.net/publication/323728995_Doslidzenna_efektivnosti_metodiv_biometricnoi_avtentifikacii

10. Порівняння смарт-карток Em-Marine, Mifare, Fudan | Новини RFID. *idcard.com.ua*. URL: https://idcard.com.ua/ua/blog/sravnenie-smart-kart-em-marine-mifare-fudan/
11. Все про RFID-зчитувачі. idcard.com.ua. URL: https://idcard.com.ua/ua/blog/vse-rfid-schityvatelyah-opisanie-raznovidnosti-harakteristiki/?srsltid=afmboop_fkarq5ag2z3fmzd2ifhqtpkpxgwyagajx3_eds86ixl3tzcc.
12. Система контролю доступу нового покоління U-Prox | ERC Ukraine. ERC Ukraine. URL: https://erc.ua/erc-reviews/21105/sistema-kontroliu-dostupu-novogo-pokolinnia-u-prox.
13. Fingerprint Vendor Technology Evaluation (FpVTE). NIST. URL: https://www.nist.gov/programs-projects/fingerprint-vendor-technology-evaluation-fpvte.
14. Solution. https://www.centermclient.com/. URL: https://www.centermclient.com/centerm-solution-for-education/.
15. Difference Between Latching and Momentary Button Switches: Exploring Switch Actions and Contact Types - FAQs | Marine Toggle Switch Panels, Fuses, Circuit Breakers Manufacturer | YIS Marine. *Yih Sean Enterprise Co., Ltd.* URL: https://www.yismarine.com/en/faq/faq_14_PB.html.
16. Вибір електромагнітних замків, кронштейнів їх встановлення та експлуатація | Блог на Bezpeka-shop.com. www.bezpeka-shop.com. URL: https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/vybor-elektromagnitnykh-zamkov-kronshteynov-ikh-ustanovka-i-ekspluatatsiya/?srsltid=AfmBOooIuBhDtR0C3cyfwe6bjf0GyZyLU0S6ZACF3ZvCroXXvCYnVsjm.
17. Виклични панелі. Security-shop. URL: https://security-shop.com.ua/ua/videosposterezhennya/domofoni/viklichni-paneli.
18. Dojo – новий суперкомп'ютер від Tesla: настільки потужний, що може знеструмити міста. ITC.ua. URL: https://itc.ua/ua/novini/dojo-novij-superkomp-yuter-vid-tesla-nastilki-potuzhnij-shho-mozhe-znestrumiti-mista/.

ДЕМОНСТРАТИВНІ МАТЕРІАЛИ

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дмитро Зеленський

Назва: Система контролю і управлінням доступом з використанням відеонагляду та штучного інтелекту

Координатор: Лариса Дакова

Підрозділ: ННІТ

Коефіцієнт подібності 1:16.9

Коефіцієнт подібності 2:14

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*