

Міністерство освіти і науки України  
Західноукраїнський національний університет  
Факультет комп'ютерних інформаційних технологій  
Кафедра спеціалізованих комп'ютерних систем

**ЛЕНЬ Юрій Любомирович**

**КОМП'ЮТЕРНО-ІНТЕГРОВАНА СИСТЕМА КОНТРОЛЮ ТА  
УПРАВЛІННЯ ДОСТУПОМ ЖИТЕЛІВ ЖИТЛОВОГО КОМПЛЕКСУ./  
COMPUTER-INTEGRATED ACCESS CONTROL AND MANAGEMENT  
SYSTEM FOR RESIDENTS OF THE RESIDENTIAL COMPLEX**

спеціальність: 174 – Автоматизація, комп'ютерно-інтегровані технології та  
робототехніка  
освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані  
технології

Випускна кваліфікаційна робота  
здобувача першого (бакалаврського) рівня освіти

Виконав: студент групи АКІТ–42/1  
Ю. Л. Лень

---

Науковий керівник:  
к.е.н., доцент А.М. Шевчук

---

Випускну кваліфікаційну роботу  
допущено до захисту:  
" \_\_\_\_ " \_\_\_\_\_ 2026 р.

Завідувач кафедри СКС  
\_\_\_\_\_ А. І. Сегін

Тернопіль 2026

Факультет комп'ютерних інформаційних технологій  
Кафедра спеціалізованих комп'ютерних систем  
Освітній ступінь "бакалавр"  
спеціальність: 174 – Автоматизація, комп'ютерно-інтегровані технології та  
робототехніка  
освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані  
технології

**ЗАТВЕРДЖУЮ:**

зав. кафедри СКС

А. І. Сегін

"\_01\_" . \_грудня\_ 2025р.

**ЗАВДАННЯ**  
**НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Леню Юрію Любомировичу

(прізвище, ім'я по-батькові)

**1. Тема кваліфікаційної роботи**

Комп'ютерно-інтегрована система контролю та управління доступом жителів житлового комплексу./ Computer-integrated access control and management system for residents of the residential complex.

керівник роботи к.е.н., доцент Шевчук А.М.

затверджено наказом по університету від « 1 » грудня 2025 р. № 894

**2. Строк подання студентом закінченої кваліфікаційної роботи**

25 травня 2026р.

**3. Вихідні дані до кваліфікаційної роботи:**

1. Функціональні можливості СКУД.

2. Вимоги до інформаційної безпеки, кібербезпеки та захисту конфіденційності.

3. Системи тривожної та електронної безпеки. Системи електронного контролю доступу.

**4. Основні питання, які потрібно розробити**

1. Розробити архітектуру комп'ютерно-інтегрованої системи контролю та управління доступом із використанням RFID/NFC-ідентифікації.

2. Обґрунтувати вибір технічних засобів системи та визначити їх основні характеристики.

3. Розробити структуру програмного забезпечення серверної частини системи на базі HikCentral Professional Access Control.

4. Дослідити інформаційну взаємодію між RFID/NFC-зчитувачами, контролерами доступу та сервером системи.

5. Розробити алгоритм функціонування контролера доступу Hikvision DS-K2604.

## 5. Перелік графічного матеріалу у роботі

1. Структура системи контролю та управління доступом житлового комплексу.

2. Комп'ютерно-інтегрована система контролю та управління доступом житлового комплексу, що дозволяє здійснювати централізований моніторинг і керування доступними сервісами.

3. Алгоритм роботи системи контролю доступу користувача до сервісів.

4. Структурна схема централізованої системи контролю та управління доступом для житлового комплексу.

## 6. Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата   |                  |
|--------|-------------------------------------------|----------------|------------------|
|        |                                           | Завдання видав | Завдання прийняв |
| 1      | Шевчук А.М.                               |                |                  |
| 2      | Шевчук А.М.                               |                |                  |
| 3      | Шевчук А.М.                               |                |                  |
|        |                                           |                |                  |

## 7. Дата видачі завдання 01 грудня 2025р.

### КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назви етапів кваліфікаційної роботи                                                                                                                                | Строк виконання етапів роботи | Примітка |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------|
| 1     | Аналіз комп'ютерно-інтегрованих систем контролю та управління доступом жителів житлового комплексу та способів їх побудови                                         | 01.12.2025 р. – 15.01.2026 р. | виконано |
| 2     | Розробка структури та обґрунтування обрання технічних засобів централізованої комп'ютерно-інтегрованої системи контролю та управління доступом житлового комплексу | 16.01. 2026 р.– 15.03.2026р.  | виконано |
| 3     | Структура програмного забезпечення серверної частини СКУД та її взаємодія з мобільним застосунком NIK-CONNECT                                                      | 16.03.2026 р. – 30.04.2026 р. | виконано |
| 4     | Остаточне оформлення та подача кваліфікаційної роботи на перевірку щодо плагіату                                                                                   | 1.05.2026 р. – 25.05.2026 р.  | виконано |

Студент

\_\_\_\_\_  
(підпис)      Лень Ю. Л.

Керівник роботи

\_\_\_\_\_  
(підпис)      к.т.н. доц. Шевчук А.М.

## АНОТАЦІЯ

Лень Ю. Л. Комп'ютерно-інтегрована система контролю та управління доступом жителів житлового комплексу. – Рукопис.

Дослідження на здобуття першого (бакалаврського ) рівня освіти за спеціальністю 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка, освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані технології – Західноукраїнський національний університет, Тернопіль, 2026 р.

У кваліфікаційній роботі розроблено комп'ютерно-інтегровану систему контролю та управління доступом мешканців житлового комплексу на основі RFID/NFC-ідентифікації, контролера Hikvision DS-K2604, програмного комплексу HikCentral Professional та мобільного застосунку Hik-Connect. Запропоновано архітектуру системи, обґрунтовано вибір технічних і програмних засобів та розроблено алгоритм функціонування системи для підвищення рівня безпеки й комфорту мешканців.

## ANNOTATION

Len Y. L. Computer-integrated access control and management system for residents of the residential complex. – Manuscript.

Research for the first (bachelor's) level of education in the specialty 174 – Automation, computer-integrated technologies and robotics, educational and professional program – Automation and computer-integrated technologies – West Ukrainian National University, Ternopil, 2026.

The qualification work presents a computer-integrated access control and management system for residents of a residential complex, based on RFID/NFC identification, a Hikvision DS-K2604 controller, HikCentral Professional software suite, and the Hik-Connect mobile application. The system architecture is proposed, the selection of hardware and software components is justified, and a system operation algorithm is developed to enhance the security and comfort of residents.

## 3MIST

|                                                                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП.....                                                                                                                                                                         | 7  |
| 1. АНАЛІЗ КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ СИСТЕМ<br>КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ЖИТЕЛІВ<br>ЖИТЛОВОГО КОМПЛЕКСУ ТА СПОСОБІВ ЇХ ПОБУДОВИ....                                            | 11 |
| 1.1 Призначення та структура системи контролю та управління<br>доступом житлового комплексу.....                                                                                   | 11 |
| 1.2 Аналіз способів побудови комп'ютерно-інтегрованих систем<br>контролю та управління доступом жителів житлового комплексу.....                                                   | 14 |
| 2. РОЗРОБКА СТРУКТУРИ ТА ОБҐРУНТУВАННЯ ОБРАННЯ<br>ТЕХНІЧНИХ ЗАСОБІВ ЦЕНТРАЛІЗОВАНОЇ<br>КОМП'ЮТЕРНО-ІНТЕГРОВАНА СИСТЕМИ КОНТРОЛЮ ТА<br>УПРАВЛІННЯ ДОСТУПОМ ЖИТЛОВОГО КОМПЛЕКСУ..... | 21 |
| 2.1 Структурна схема контролю та управління доступом для<br>житлового комплексу.....                                                                                               | 21 |
| 2.2 Обґрунтування обраного обладнання та його технічні<br>характеристики.....                                                                                                      | 24 |
| 2.3 Алгоритм роботи контролера доступу Hikvision DS-K2604 у<br>централізованій комп'ютерно-інтегрованій системі контролю та<br>управління доступом.....                            | 29 |
| 2.4. Протоколи взаємодії RFID/NFC-зчитувачів із контролером DS-<br>K2604.....                                                                                                      | 32 |
| 3. СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ<br>СЕРВЕРНОЇ ЧАСТИНИ СКУД ТА ЇЇ ВЗАЄМОДІЯ З<br>МОБІЛЬНИМ ЗАСТОСУНКОМ НІК-CONNECT.....                                                        | 36 |

|           |      |                |        |      |                                                                                                      |                     |      |         |  |
|-----------|------|----------------|--------|------|------------------------------------------------------------------------------------------------------|---------------------|------|---------|--|
|           |      |                |        |      | ДП.АКІТ.11560261.00.00.000.ПЗ                                                                        |                     |      |         |  |
| Змн.      | Арк. | № докум.       | Підпис | Дата |                                                                                                      |                     |      |         |  |
| Розроб.   |      | Лень Ю. Л.     |        |      | Комп'ютерно-інтегрована<br>система контролю та<br>управління доступом жителів<br>житлового комплексу | Літ.                | Арк. | Акрушів |  |
| Перевір.  |      | Шевчук А.М.    |        |      |                                                                                                      |                     | 6    | 62      |  |
| Консульт. |      | Шевчук А.М.    |        |      |                                                                                                      | ЗУНУ.ФКІТ.АКІТ-42/1 |      |         |  |
| Н. Контр. |      | Заставний О.М. |        |      |                                                                                                      |                     |      |         |  |
| Затверд.  |      | Сегін А. І.    |        |      |                                                                                                      |                     |      |         |  |

|                                                                                                                    |    |
|--------------------------------------------------------------------------------------------------------------------|----|
| 3.1 Програмне забезпечення серверної частини комп'ютерно-інтегрованої системи контролю та управління доступом..... | 36 |
| 3.2 Обґрунтування вибору мобільного застосунку Hik-Connect.....                                                    | 42 |
| ВИСНОВКИ.....                                                                                                      | 46 |
| ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....                                                                                   | 48 |
| ДОДАТОК А. АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ.....                                                                       | 52 |

|     |      |          |       |      |                               |      |
|-----|------|----------|-------|------|-------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.11560261.00.00.000.ПЗ | Арк. |
|     |      |          |       |      |                               | 7    |
| Зм. | Арк. | № докум. | Підп. | Дата |                               |      |

## ВСТУП

**Актуальність теми.** Сучасний розвиток житлової інфраструктури характеризується активним впровадженням інформаційних технологій та концепції Smart Building, що передбачає інтеграцію різноманітних систем безпеки в єдине інформаційне середовище. Одним із ключових елементів таких систем є комп'ютерно-інтегровані системи контролю та управління доступом, які забезпечують захист мешканців, контроль доступу до об'єктів житлового комплексу та підвищення рівня комфорту користувачів [1].

Традиційні системи доступу, що базуються лише на механічних ключах або автономних електронних замках, не забезпечують необхідного рівня контролю, централізованого адміністрування та інтеграції з іншими підсистемами безпеки. Тому актуальним завданням є розроблення сучасних комп'ютерно-інтегрованих систем, які поєднують RFID/NFC-ідентифікацію [2], відеоспостереження, серверні технології та мобільні сервіси керування доступом.

**Метою кваліфікаційної роботи** є розроблення комп'ютерно-інтегрованої системи контролю та управління доступом мешканців житлового комплексу на основі RFID/NFC-технологій, централізованого серверного управління та мобільного доступу з інтеграцією підсистеми відеоспостереження.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- провести аналіз сучасних систем контролю та управління доступом і визначити вимоги до їх побудови для житлових комплексів;
- розробити архітектуру комп'ютерно-інтегрованої системи контролю та управління доступом із використанням RFID/NFC-ідентифікації;
- обґрунтувати вибір технічних засобів системи та визначити їх основні характеристики;

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 8    |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

- розробити структуру програмного забезпечення серверної частини системи на базі HikCentral Professional Access Control;
- дослідити інформаційну взаємодію між RFID/NFC-зчитувачами, контролерами доступу та сервером системи;
- розробити алгоритм функціонування контролера доступу Hikvision DS-K2604;
- проаналізувати можливості інтеграції мобільного застосунку Hik-Connect у структуру системи;
- оцінити практичну придатність запропонованих технічних рішень для використання в житлових комплексах.

**Об'єктом дослідження** є процеси контролю та управління доступом у житлових комплексах із використанням сучасних інформаційних та телекомунікаційних технологій.

**Предметом дослідження** є методи та засоби побудови комп'ютерно-інтегрованих систем контролю та управління доступом на основі RFID/NFC-ідентифікації, серверного програмного забезпечення та мобільних технологій.

**Методи дослідження.** У роботі використано методи системного аналізу для дослідження структури та функціонування систем контролю доступу, методи структурного проєктування для розроблення архітектури системи, методи моделювання інформаційних потоків для аналізу взаємодії її компонентів, а також методи порівняльного аналізу для обґрунтування вибору технічних і програмних засобів.

**Практичне значення одержаних результатів** полягає у розробленні архітектури комп'ютерно-інтегрованої системи контролю та управління доступом житлового комплексу, яка може бути використана під час проєктування та модернізації систем безпеки багатоквартирних будинків. Запропоновані технічні та програмні рішення забезпечують централізоване управління доступом, інтеграцію із системою відеоспостереження та

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 9    |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

можливість використання мобільних технологій для підвищення рівня безпеки та комфорту мешканців.

**Апробація результатів роботи**

А. Сегін, Ю. Лень. Система контролю та управління доступом жителів житлового комплексу. // Збірник матеріалів всеукраїнської науково-практичної конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ–2026)/ Тернопіль, 2026. С. 204–209.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 10   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

# 1. АНАЛІЗ КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ЖИТЕЛІВ ЖИТЛОВОГО КОМПЛЕКСУ ТА СПОСОБІВ ЇХ ПОБУДОВИ

## 1.1 Призначення та структура системи контролю та управління доступом житлового комплексу

Система контролю та управління доступом житлового комплексу являє собою багаторівневу інтегровану інформаційно-технічну структуру, призначену для забезпечення безпеки мешканців, контролю переміщення осіб та транспортних засобів, а також централізованого управління інженерними й сервісними підсистемами об'єкта [1]. Основною функцією такої системи є організація регламентованого доступу до території житлового комплексу та окремих його зон відповідно до прав користувачів, визначених адміністрацією або автоматизованими політиками безпеки.

Структурно система складається з декількох взаємопов'язаних рівнів, серед яких ключове місце займає ядро системи, користувачі, точки доступу та інтегровані підсистеми [3-5]. Взаємодія між усіма елементами забезпечується локальною або глобальною мережею передачі даних [6], що дозволяє організувати безперервний обмін інформацією між обладнанням, серверними модулями та програмним забезпеченням (рисунок 1.1).

До категорій користувачів системи належать мешканці житлового комплексу, відвідувачі, охоронний персонал, адміністратори та технічні працівники. Для кожної групи користувачів встановлюється окремий рівень доступу до приміщень, сервісів та функцій системи. Мешканці отримують можливість доступу до житлових секцій, ліфтів, паркінгів та допоміжних приміщень за допомогою персональних ідентифікаторів, мобільного додатка або біометричних засобів автентифікації. Гості можуть отримувати тимчасові пропуски або одноразові дозволи на вхід після підтвердження з боку

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 11   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

мешканця чи адміністратора. Охорона здійснює моніторинг подій, реагування на нештатні ситуації та контроль функціонування обладнання, тоді як обслуговуючий персонал має доступ лише до технічних зон відповідно до встановленого графіка роботи [7-8].

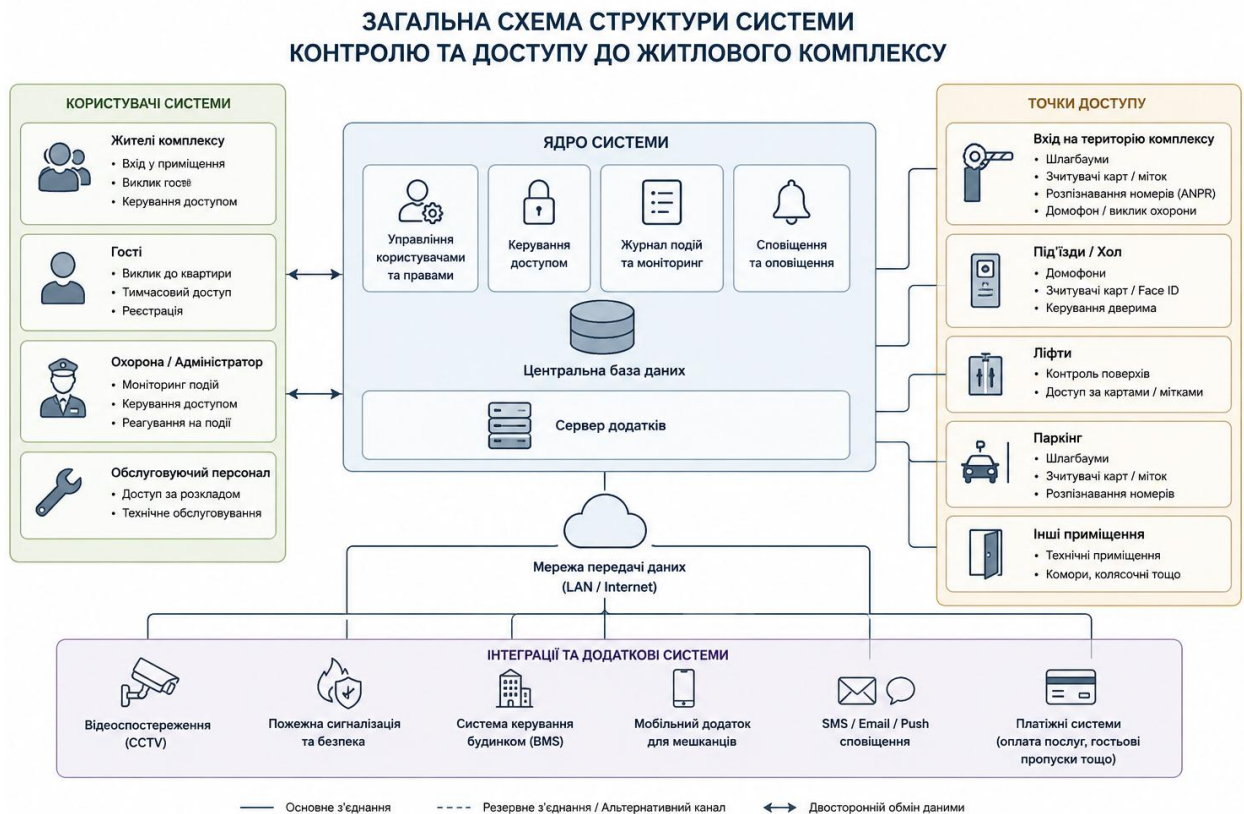


Рисунок 1.1 – Структура системи контролю та управління доступом житлового комплексу

Центральним елементом структури є ядро системи, яке включає сервер додатків, базу даних та програмні модулі управління. Сервер додатків забезпечує виконання логічних операцій, обробку запитів та взаємодію між усіма компонентами системи. База даних використовується для збереження інформації про користувачів, права доступу, журнали подій, відеоархіви, історію відвідувань та інші службові дані. Програмні модулі ядра реалізують функції керування користувачами, адміністрування прав доступу, ведення

|     |      |          |       |      |                               |      |
|-----|------|----------|-------|------|-------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.0000.ПЗ | Арк. |
|     |      |          |       |      |                               | 12   |
| Зм. | Арк. | № докум. | Підп. | Дата |                               |      |

журналів подій, генерації повідомлень та автоматичного реагування на порушення безпеки.

Система підтримує механізми постійного моніторингу подій, що дозволяє фіксувати кожну спробу входу або виходу, час перебування користувача в певній зоні та статус роботи обладнання. У випадку виникнення аварійної або несанкціонованої ситуації система формує сповіщення для охоронного персоналу або адміністратора через внутрішні канали зв'язку, мобільний додаток, електронну пошту чи SMS-повідомлення. Такий підхід забезпечує оперативне реагування на потенційні загрози та підвищує рівень загальної безпеки комплексу.

Точки доступу системи представлені фізичними елементами контролю, встановленими на входах до території комплексу, під'їздів, ліфтів, паркінгів та службових приміщень. На в'їздах до території використовуються автоматичні шлагбауми, системи розпізнавання державних номерних знаків транспортних засобів та RFID-зчитувачі [9-10]. Для доступу до житлових секцій застосовуються домофони, електронні замки, карткові або біометричні зчитувачі, що дозволяють ідентифікувати особу користувача та перевірити її права доступу. У ліфтових системах може реалізовуватись контроль доступу до окремих поверхів, що особливо актуально для багатофункціональних житлових комплексів із зонуванням території.

Важливою складовою системи є інтеграція із суміжними підсистемами безпеки та автоматизації будівлі. Зокрема, система контролю доступу взаємодіє з мережею відеоспостереження, що дозволяє синхронізувати події доступу із записами камер та здійснювати візуальну ідентифікацію осіб. Інтеграція з пожежною сигналізацією забезпечує автоматичне розблокування евакуаційних виходів у разі виникнення надзвичайної ситуації. Підключення до системи керування будинком дає можливість централізовано контролювати інженерні мережі, енергоспоживання та технічний стан обладнання. Окрім цього, сучасні системи можуть інтегруватися з

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 13   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

платіжними сервісами для автоматизації оплати паркінгу, комунальних послуг або формування гостьових перепусток.

Передача інформації між компонентами системи здійснюється через локальну мережу або захищені інтернет-канали. Для забезпечення надійності роботи використовуються резервні канали зв'язку та дублювання критичних вузлів системи. Така архітектура дозволяє підтримувати працездатність навіть у випадку часткових відмов обладнання або мережевої інфраструктури. Крім того, застосування сучасних методів шифрування та автентифікації забезпечує захист персональних даних користувачів і запобігає несанкціонованому втручанню в роботу системи.

Отже, система контролю та управління доступом житлового комплексу є складним програмно-апаратним комплексом, що поєднує функції безпеки, автоматизації та інформаційного управління. Її впровадження забезпечує підвищення рівня захищеності мешканців, оптимізацію роботи персоналу, автоматизацію процесів контролю доступу та ефективне управління інфраструктурою сучасного житлового комплексу.

## 1.2 Аналіз способів побудови комп'ютерно-інтегрованих систем контролю та управління доступом жителів житлового комплексу

Стрімкий розвиток інформаційних технологій та концепції «розумного будинку» сприяє активному впровадженню комп'ютерно-інтегрованих систем контролю та управління доступом у сучасних житлових комплексах. Такі системи призначені для забезпечення безпеки мешканців, контролю пересування осіб територією комплексу, автоматизації процесів ідентифікації користувачів та підвищення ефективності управління об'єктами житлової інфраструктури. На відміну від традиційних механічних засобів обмеження доступу, сучасні системи поєднують програмне забезпечення, мережеві

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 14   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

технології та спеціалізоване обладнання в єдине інформаційне середовище, що дозволяє здійснювати централізований моніторинг і керування всіма точками проходу (рисунок 1.2).

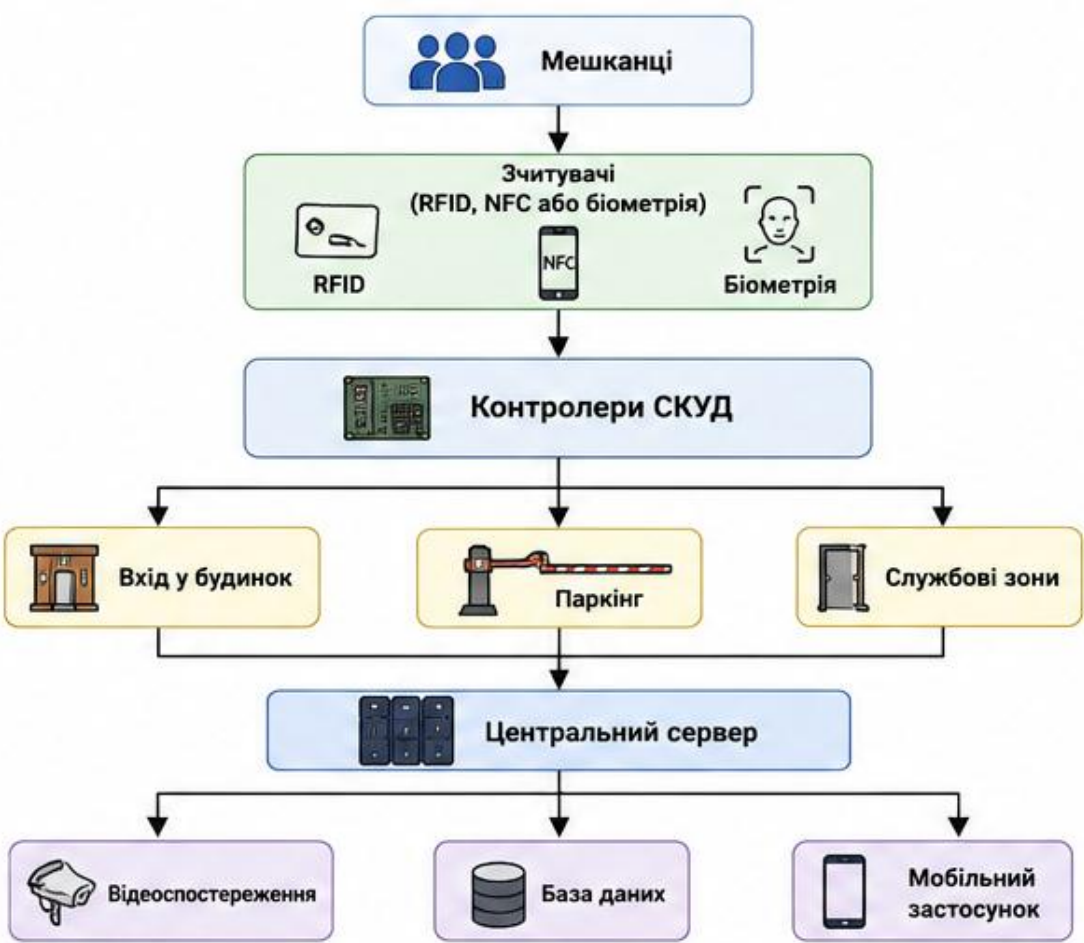


Рисунок 1.2 – Комп’ютерно-інтегрована система контролю та управління доступом житлового комплексу, що дозволяє здійснювати централізований моніторинг і керування доступними сервісами

Залежно від архітектури побудови можна виділити декілька основних підходів до реалізації систем контролю та управління доступом (рисунок 1.3).

Найпростішим рішенням є автономна система (рисунок 1.3, а), в якій кожна точка доступу функціонує незалежно від інших. У такій системі контролер, зчитувач і виконавчий механізм працюють локально без

постійного зв'язку із центральним сервером. Перевагами даного підходу є відносно низька вартість впровадження, простота монтажу та висока автономність роботи. Разом із тим відсутність централізованого управління значно обмежує можливості адміністрування, збору статистичних даних та оперативного реагування на позаштатні ситуації. Тому автономні системи доцільно використовувати переважно в невеликих житлових будинках або на окремих об'єктах із невеликою кількістю користувачів.



Рисунок 1.3 – Основні архітектури побудови систем контролю та управління доступом

Більш досконалим підходом є побудова централізованої комп’ютерно-інтегрованої системи контролю доступу (рисунок 1.3, б).

У цьому випадку всі контролери об’єднуються в єдину мережу та взаємодіють із центральним сервером, який здійснює обробку інформації, зберігання баз даних користувачів і ведення журналів подій. Централізована архітектура дозволяє оперативно змінювати права доступу мешканців, контролювати роботу обладнання в режимі реального часу та формувати різноманітні звіти щодо функціонування системи. Крім того, такий підхід значно спрощує масштабування системи при збільшенні кількості під’їздів,

паркінгів або інших контрольованих зон житлового комплексу. Незважаючи на вищу вартість реалізації та залежність від центрального сервера, централізовані системи сьогодні вважаються найбільш ефективним рішенням для багатоквартирних житлових комплексів.

Останніми роками все більшого поширення набувають хмарні системи контролю та управління доступом (рисунк 1.3, в). Їх особливістю є розміщення серверної частини в хмарній інфраструктурі, що дозволяє здійснювати адміністрування системи через мережу Інтернет без необхідності встановлення локального сервера. Такий підхід забезпечує високу гнучкість, можливість віддаленого керування та автоматичне резервування інформації. Адміністратори можуть отримувати доступ до системи з будь-якого пристрою, підключеного до мережі Інтернет, а оновлення програмного забезпечення виконуються централізовано постачальником послуг. Водночас ефективність функціонування таких систем значною мірою залежить від стабільності мережевого з'єднання та рівня захисту інформаційних ресурсів від кіберзагроз.

Важливою складовою будь-якої системи контролю доступу є підсистема ідентифікації користувачів (рисунк 1.4).

Найбільш поширеним методом залишається використання RFID-карток та безконтактних брелоків [11], які містять унікальний ідентифікатор і забезпечують швидке надання доступу до контрольованих зон. Завдяки невисокій вартості та простоті використання даний спосіб широко застосовується в житлових комплексах різного масштабу. Разом із тим сучасні тенденції свідчать про поступовий перехід до використання мобільних пристроїв як засобів ідентифікації. Технології NFC та Bluetooth Low Energy [12] дозволяють перетворити смартфон на цифровий ключ, що значно підвищує зручність користування системою та спрощує процедуру управління правами доступу.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 17   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

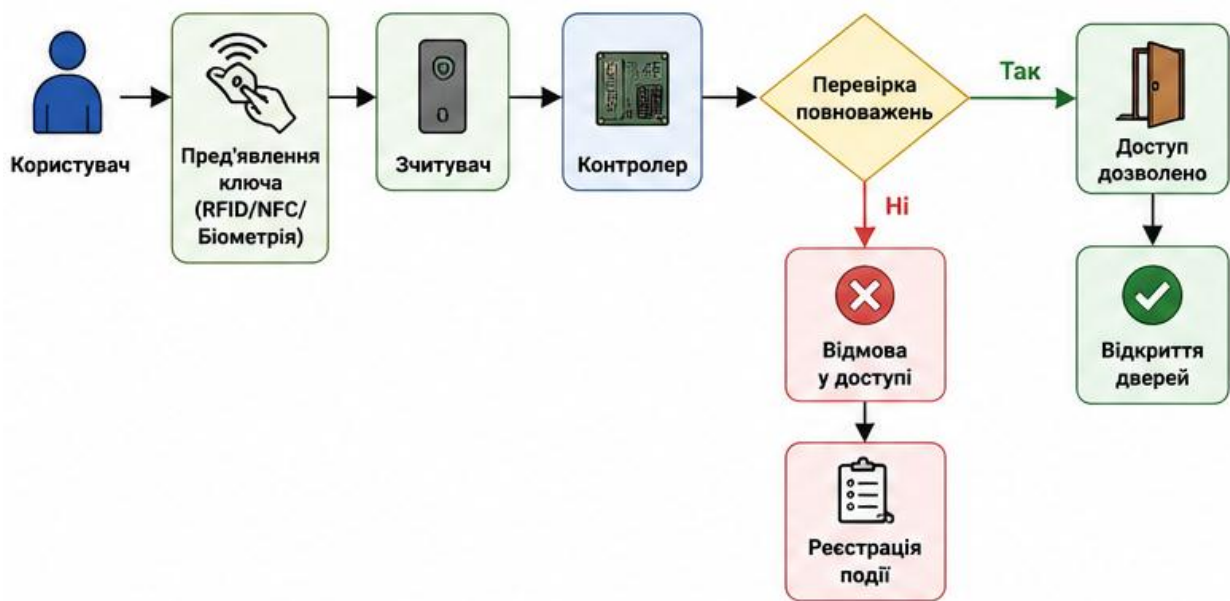


Рисунок 1.4 – Алгоритм роботи системи контролю доступу користувача до сервісів на прикладі відчинення дверей.

Перспективним напрямом розвитку є також використання біометричних методів ідентифікації, які базуються на розпізнаванні відбитків пальців, обличчя або райдужної оболонки ока. Основною перевагою таких рішень є високий рівень захищеності від несанкціонованого використання облікових даних. Однак впровадження біометричних технологій потребує значних фінансових витрат, а також додаткових заходів щодо захисту персональних даних користувачів відповідно до чинного законодавства [13].

Ефективність функціонування системи контролю доступу значною мірою залежить від обраних мережевих технологій. У великих житлових комплексах найчастіше використовуються провідні мережі на базі Ethernet або RS-485, які забезпечують високу надійність передачі даних та стійкість до електромагнітних завад. Водночас розвиток бездротових технологій відкриває нові можливості для побудови гнучких та масштабованих систем. Використання Wi-Fi, Bluetooth або ZigBee дозволяє зменшити витрати на прокладання кабельної інфраструктури та спростити модернізацію об'єкта.

Особливе значення для сучасних житлових комплексів має інтеграція системи контролю доступу з іншими підсистемами безпеки та автоматизації. Найчастіше СКУД об'єднується із системами відеоспостереження, домофонного зв'язку, охоронної та пожежної сигналізації, автоматизованими паркінгами та мобільними застосунками мешканців (рисунок 1.5). Така інтеграція забезпечує створення єдиного інформаційного простору, в межах якого всі підсистеми взаємодіють між собою та обмінюються даними. Наприклад, під час спроби несанкціонованого проникнення система може автоматично активувати запис відеокамер, надіслати повідомлення службі охорони та зафіксувати подію в журналі безпеки.



Рисунок 1.4 – Схема інтеграції системи контролю доступу з підсистемами безпеки та сервісами житлового комплексу

Аналіз існуючих способів побудови комп'ютерно-інтегрованих систем контролю та управління доступом показує, що найбільш перспективними для сучасних житлових комплексів є централізовані та хмарні архітектури (таблиця 1.1). Вони забезпечують високий рівень безпеки, можливість

масштабування, інтеграцію з іншими інженерними системами будівлі та підтримку сучасних методів ідентифікації користувачів. Використання таких рішень дозволяє не лише підвищити захищеність мешканців, але й створити основу для подальшого розвитку концепції інтелектуального житла та цифрової інфраструктури міського середовища.

Таблиця 1.1 – Порівняльний аналіз способів побудови

| Критерій                | Автономна | Централізована | Хмарна                 |
|-------------------------|-----------|----------------|------------------------|
| Вартість впровадження   | Низька    | Середня        | Середня                |
| Масштабованість         | Низька    | Висока         | Дуже висока            |
| Віддалене керування     | Ні        | Так            | Так                    |
| Надійність              | Висока    | Висока         | Залежить від Інтернету |
| Аналітика               | Обмежена  | Розвинена      | Розвинена              |
| Інтеграція з Smart Home | Низька    | Висока         | Дуже висока            |

## 2. РОЗРОБКА СТРУКТУРИ ТА ОБҐРУНТУВАННЯ ОБРАННЯ ТЕХНІЧНИХ ЗАСОБІВ ЦЕНТРАЛІЗОВАНОЇ КОМП'ЮТЕРНО- ІНТЕГРОВАНА СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ЖИТЛОВОГО КОМПЛЕКСУ

### 2.1 Структурна схема контролю та управління доступом для житлового комплексу.

Запропонована система побудована за централізованою архітектурою, в якій усі контролери доступу об'єднані локальною мережею Ethernet та підключені до центрального сервера. Сервер виконує функції зберігання бази даних користувачів, ведення журналів подій, синхронізації з мобільними застосунками та інтеграції із системою відеоспостереження.

Під час спроби проходу мешканець прикладає RFID-картку або використовує NFC-модуль смартфона. Зчитувач передає ідентифікатор на мережевий контролер. Контролер звертається до локальної бази дозволів або до центрального сервера та приймає рішення щодо відкриття дверей. Одночасно система формує запис у журналі подій та прив'язує його до відеофрагмента з найближчої камери спостереження.

На рисунку 2.1 наведено структурну схему централізованої комп'ютерно-інтегрованої системи контролю та управління доступом для житлового комплексу, що складається з 3–5 під'їздів та розрахований на проживання від 200 до 500 мешканців. Запропонована архітектура поєднує засоби RFID/NFC-ідентифікації, систему відеоспостереження, серверний комплекс обробки даних та мобільний застосунок мешканця в єдину інформаційно-комунікаційну систему.

Основу системи становить центральний серверний вузол, до складу якого входить сервер СКУД Dell PowerEdge T350, програмне забезпечення керування доступом HikCentral Access Control та мережевий відеореєстратор

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 21   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

Hikvision DS-7732NI-I4. Центральний сервер забезпечує обробку подій доступу, ведення бази даних користувачів, зберігання журналів подій та координацію роботи всіх підсистем комплексу. Завдяки використанню програмного забезпечення HikCentral Access Control реалізується централізоване адміністрування прав доступу, моніторинг стану обладнання в режимі реального часу та інтеграція з системою відеоспостереження.

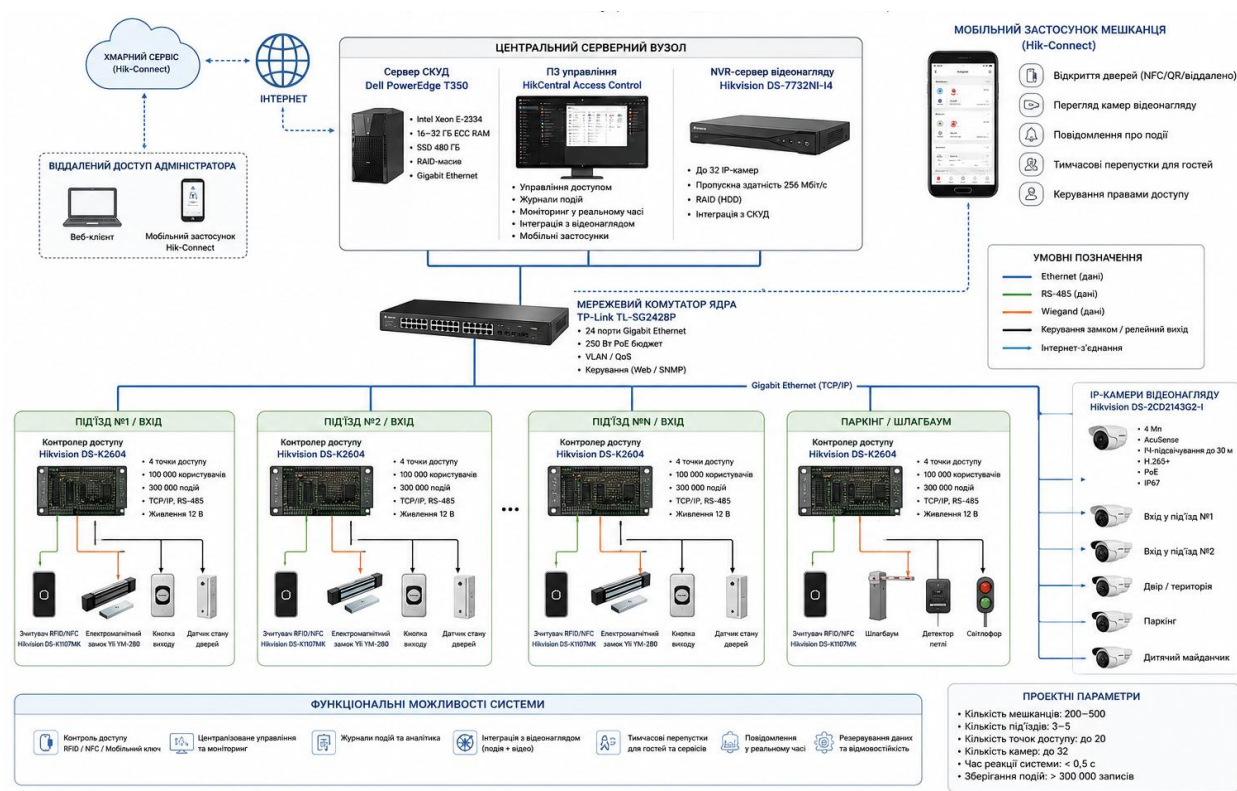


Рисунок 2.1 – Структурна схема централізованої системи контролю та управління доступом для житлового комплексу

Обмін інформацією між серверним вузлом та периферійними пристроями здійснюється через мережевий комутатор TP-Link TL-SG2428P, який виконує функції центрального комунікаційного вузла локальної мережі. Застосування гігабітної мережі Ethernet дозволяє забезпечити високу швидкість передачі даних між компонентами системи, а підтримка технології

PoE значно спрощує підключення IP-камер відеоспостереження та мережевого обладнання [14].

Для кожного під'їзду передбачено встановлення окремого мережевого контролера доступу Hikvision DS-K2604 [15]. Контролери підключаються до серверного вузла через мережу TCP/IP та забезпечують управління точками доступу незалежно від стану зв'язку із центральним сервером. До кожного контролера підключаються RFID/NFC-зчитувачі Hikvision DS-K1107MK [16], електромагнітні замки Yli YM-280, кнопки виходу та датчики контролю стану дверей. Така конфігурація дозволяє здійснювати ідентифікацію мешканців за допомогою безконтактних карток стандарту MIFARE або смартфонів із підтримкою NFC.

У момент пред'явлення ідентифікатора зчитувач передає отримані дані контролеру доступу, який виконує перевірку прав користувача та формує команду на відкриття електромагнітного замка. Одночасно інформація про подію передається на центральний сервер, де зберігається у базі даних та може бути використана для подальшого аналізу або формування звітності.

Окремим функціональним модулем системи є підсистема контролю доступу до паркінгу. Для її реалізації використовується контролер Hikvision DS-K2604, RFID/NFC-зчитувач, шлагбаум, індукційний детектор транспортних засобів та світлофорна сигналізація. Така конфігурація забезпечує автоматизований контроль в'їзду та виїзду автомобілів мешканців, а також ведення журналу транспортних подій.

Для забезпечення відеоконтролю території житлового комплексу використовуються IP-камери Hikvision DS-2CD2143G2-I [17], встановлені біля входів до під'їздів, на прибудинковій території, парковці та інших критично важливих ділянках. Відеопотоки від камер передаються на мережевий відеореєстратор DS-7732NI-I4 [18], де здійснюється запис та зберігання архіву. Інтеграція відеоспостереження із СКУД дозволяє автоматично прив'язувати відеозаписи до конкретних подій проходу

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 23   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

користувачів, що підвищує рівень безпеки та спрощує розслідування інцидентів.

Важливою складовою системи є хмарний сервіс Hik-Connect, який забезпечує віддалений доступ до функцій комплексу через мережу Інтернет. За допомогою мобільного застосунку мешканці можуть відкривати двері дистанційно, переглядати відео з камер, отримувати повідомлення про події та створювати тимчасові перепустки для гостей. Адміністратор системи, у свою чергу, отримує можливість здійснювати моніторинг та налаштування обладнання через вебінтерфейс або мобільний застосунок незалежно від свого місцезнаходження.

Запропонована структура забезпечує централізоване управління всіма точками доступу житлового комплексу, високу надійність функціонування та можливість подальшого масштабування. Використання мережевих контролерів, сучасних засобів ідентифікації, інтегрованого відеоспостереження та мобільних сервісів відповідає сучасним вимогам до побудови систем безпеки багатоквартирних житлових комплексів і створює основу для подальшого розвитку концепції «розумного будинку».

## 2.2 Обґрунтування обраного обладнання та його технічні характеристики

Пропонується використати контролер Hikvision DS-K2604 (рисунок 2.2). Він дозволяє обслуговувати кілька дверей одночасно та легко масштабується при збільшенні кількості під'їздів. Великий обсяг пам'яті забезпечує автономну роботу навіть при тимчасовій втраті зв'язку із сервером.

Основні характеристики [19]

– 4 точки доступу;

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 24   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

- підтримка до 100 000 користувачів;
- пам'ять на 300 000 подій;
- підтримка інтерфейсу RS-485 та Wiegand;
- інтеграція з відео спостереженням;
- 32-bit високошвидкісний процесор;
- кількість зчитувачів: 4 x Wiegand або 8 x RS-485
- входи: 4 тривожні, 4 датчики дверей, 4 кнопки виходу, 8 дод. входів, 1 тампер;
- виходи: 4 реле замку, 4 реле тривоги;
- живлення 12 В;



Рисунок 2.2 – Контролер Hikvision DS-K2604.

В якості RFID/NFC-зчитувача доцільно використати Hikvision DS-K1107МК (рисунок 2.3).



Рисунок 2.3 – RFID/NFC-зчитувач Hikvision DS-K1107МК

|     |      |          |       |      |                             |      |
|-----|------|----------|-------|------|-----------------------------|------|
|     |      |          |       |      | ДП.АКТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                             | 25   |
| Зм. | Арк. | № докум. | Підп. | Дата |                             |      |

Він підтримує як RFID-картки, так і смартфони через NFC, що дозволяє використовувати комбінований спосіб ідентифікації мешканців без додаткових витрат на модернізацію системи.

#### Характеристики Hikvision DS-K1107MK

- підтримка Mifare 13,56 МГц;
- підтримка NFC;
- дальність зчитування до 50 мм;
- ступінь захисту IP65;
- інтерфейс RS-485;
- робоча температура від -40 °С до +65 °С.

Електромагнітний замок Yli Electronic YM-280 (рисунок 2.4) забезпечує достатній рівень захисту для багатоквартирного житлового будинку та характеризується високою надійністю й тривалим терміном експлуатації [20].



Рисунок 2.4 – Електромагнітний замок Yli Electronic YM-280

#### Характеристики Yli Electronic YM-280:

- утримуюче зусилля 280 кг;
- живлення 12 В;
- споживання струму 500 мА;
- вбудований датчик стану дверей.

В якості сервера системи для житлового комплексу достатньо Dell Technologies PowerEdge T350 (рисунок 2.5) [29]:

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 26   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

- процесор Intel Xeon E-2334;
- 16–32 ГБ ECC RAM;
- RAID-масив;
- SSD 480 ГБ;
- Gigabit Ethernet.



Рисунок 2.5 – Сервер системи Dell Technologies PowerEdge T350

Сервер здатний одночасно обслуговувати базу даних СКУД, мобільний застосунок та систему відеоаналітики без перевантаження.

Для системи відео спостереження та інтеграції пропонується використати IP-камери Hikvision DS-2CD2143G2-I (рисунок 2.6) [21]:

- роздільна здатність 4 Мп;
- технологія AcuSense;
- інфрачервоне підсвічування до 30 м;
- H.265+;
- PoE живлення;
- захист IP67.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 27   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |



Рисунок 2.6 – IP-камера Hikvision DS-2CD2143G2-I

Камери дозволяють автоматично фіксувати всі події проходу та забезпечують високу якість відео навіть у нічний час.

Відеореєстратор обрано Hikvision DS-7732NI-I4 (рисунок 2.7) з технічними характеристиками [22]:

- підключення до 32 IP-камер;
- пропускна здатність 256 Мбіт/с;
- підтримка RAID;
- інтеграція з СКУД.



Рисунок 2.6 – Відеореєстратор Hikvision DS-7732NI-I4

Він забезпечує централізоване зберігання архіву відеоданих та синхронізацію із журналами доступу.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 28   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

### 2.3 Алгоритм роботи контролера доступу Hikvision DS-K2604 у централізованій комп'ютерно-інтегрованій системі контролю та управління доступом

Контролер доступу Hikvision DS-K2604 є центральним виконавчим елементом підсистеми контролю доступу та забезпечує взаємодію між засобами ідентифікації користувачів, виконавчими пристроями та центральним сервером СКУД. У запропонованій системі контролер здійснює приймання та обробку даних від RFID/NFC-зчитувачів, прийняття рішення щодо надання доступу, керування електромагнітними замками та передачу інформації про події до центрального серверного вузла (рисунок 2.7).

У початковому стані контролер перебуває в режимі очікування події доступу та постійно здійснює моніторинг стану підключених пристроїв. Одночасно контролюється справність зчитувачів, стан дверей, наявність мережевого з'єднання із сервером та працездатність виконавчих механізмів.

Після пред'явлення мешканцем RFID-картки або NFC-ідентифікатора зчитувач формує цифровий код користувача та передає його контролеру через інтерфейс зв'язку. Отримавши ідентифікатор, контролер виконує пошук відповідного запису у власній локальній базі даних або звертається до центрального сервера для актуалізації прав доступу.

На наступному етапі здійснюється перевірка повноважень користувача. Контролер аналізує наявність ідентифікатора у базі даних, відповідність часовим обмеженням, належність користувача до певної групи доступу та стан контрольованої точки проходу. Якщо всі умови виконані, формується команда на відкриття електромагнітного замка. У разі невідповідності хоча б одного параметра доступ блокується.

При позитивному результаті перевірки контролер активує релейний вихід, який забезпечує розблокування електромагнітного замка на заданий проміжок часу.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 29   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

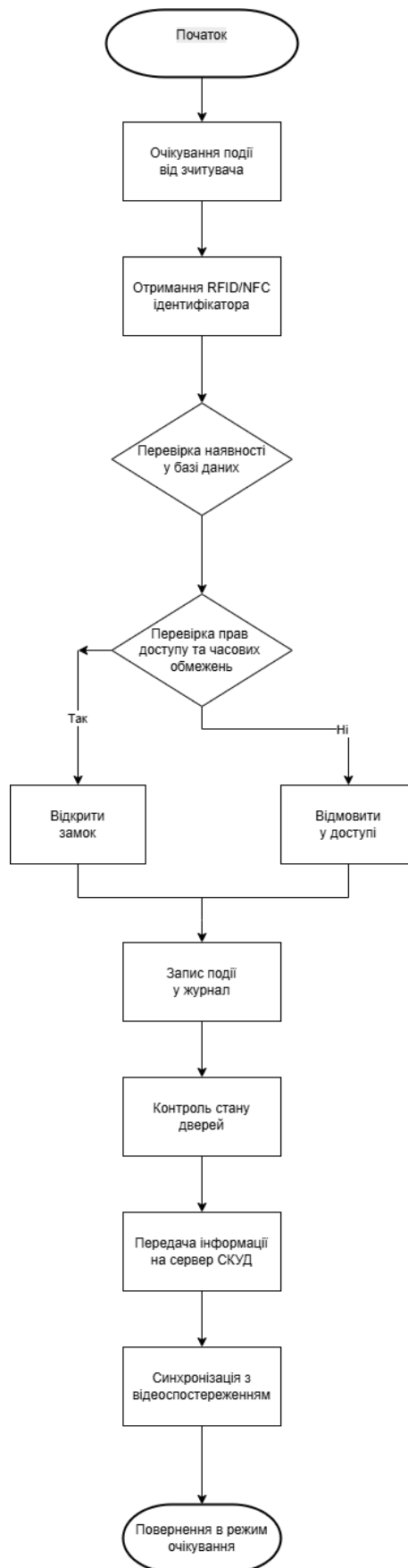


Рисунок 2.7 – Блок-схема алгоритму роботи контролера Hikvision DS-K2604

Після відкриття дверей контролер контролює сигнал від датчика стану дверей та фіксує факт проходження користувача через контрольовану точку доступу.

Паралельно з виконанням команди відкриття контролер формує службове повідомлення, яке містить дату та час події, ідентифікатор користувача, номер точки доступу та результат перевірки. Сформований запис передається до центрального сервера, де зберігається у журналі подій та використовується для подальшого аналізу. Одночасно система відеоспостереження може виконувати прив'язку відповідного відеофрагмента до зареєстрованої події доступу.

Після завершення проходження контролер перевіряє повернення дверей у закритий стан. Якщо двері залишаються відкритими довше встановленого часу або виявляється спроба несанкціонованого відкриття, формується тривожне повідомлення та передається на сервер для подальшої обробки оператором системи.

У разі втрати зв'язку із центральним сервером контролер продовжує автономну роботу, використовуючи локально збережену базу користувачів та журнал подій. Після відновлення мережевого з'єднання накопичена інформація автоматично синхронізується із сервером, що забезпечує безперервність функціонування всієї системи контролю та управління доступом.

Таким чином, контролер Hikvision DS-K2604 виконує функції локального центру прийняття рішень, забезпечуючи високу швидкодію, надійність та відмовостійкість комп'ютерно-інтегрованої системи контролю та управління доступом житлового комплексу.

Для розробленої системи на базі контролера Hikvision DS-K2604 взаємодія сервера з RFID/NFC-зчитувачами здійснюється не напряму, а через вказаний контролер доступу. Тобто сервер HikCentral Professional взаємодіє з

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 31   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

контролером DS-K2604 по мережі TCP/IP, а контролер вже обмінюється даними зі зчитувачами через спеціалізовані інтерфейси.

#### 2.4. Протоколи взаємодії RFID/NFC-зчитувачів із контролером DS-K2604

У запропонованій архітектурі доцільно використовувати зчитувачі серії Hikvision DS-K1107MK або аналогічні пристрої, які підтримують інтерфейс RS-485 та протокол Wiegand [30].

Основним інтерфейсом підключення є RS-485, який забезпечує двосторонній обмін даними між контролером та зчитувачем. Даний інтерфейс дозволяє не лише передавати ідентифікатор користувача, але й здійснювати конфігурування зчитувача, контроль його стану та діагностику несправностей.

##### Основні параметри RS-485:

- фізичний рівень — EIA-485;
- топологія — багатоточкова шина;
- швидкість обміну — від 9600 до 115200 біт/с;
- максимальна довжина лінії — до 1200 м;
- режим передачі — напівдуплексний.

Альтернативно може використовуватися протокол Wiegand-26 або Wiegand-34, який є де-факто стандартом для систем контролю доступу. Проте Wiegand забезпечує лише односторонню передачу коду картки від зчитувача до контролера та має нижчий рівень захисту порівняно з RS-485.

Протоколи RFID/NFC ідентифікації [31]. Для ідентифікації мешканців доцільно використовувати карти стандарту MIFARE Classic 1K або MIFARE DESFire EV2, які працюють відповідно до стандарту ISO/IEC 14443

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 32   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

Таблиця 2.1 –Робочі параметри NFC/RFID-підсистеми:

| Параметр                | Значення                       |
|-------------------------|--------------------------------|
| Частота                 | 13,56 МГц                      |
| Тип карт                | MIFARE Classic, MIFARE DESFire |
| Дальність зчитування    | 3–10 см                        |
| Швидкість обміну        | до 848 кбіт/с                  |
| Метод модуляції         | ASK                            |
| Антиколізійний алгоритм | ISO/IEC 14443A                 |

Після піднесення картки або смартфона з NFC зчитувач виконує процедуру антиколізії, вибирає активний ідентифікатор та передає UID до контролера DS-K2604.

Обмін між контролерами DS-K2604 та сервером HikCentral Professional здійснюється через Ethernet-мережу із використанням TCP/IP.

У самому RFID-зчитувачі використовуються службові реєстри, через які контролер отримує інформацію про стан пристрою та результати ідентифікації, наведені в таблиці 2.3.

Таблиця 2.3 – Реєстри обміну між зчитувачем та контролером

| Адреса | Назва реєстру        | Призначення                |
|--------|----------------------|----------------------------|
| 0x0001 | Device Status        | Стан зчитувача             |
| 0x0002 | Reader ID            | Ідентифікатор зчитувача    |
| 0x0003 | Card UID             | UID RFID/NFC картки        |
| 0x0004 | Access Result        | Результат перевірки        |
| 0x0005 | Alarm Status         | Стан тривоги               |
| 0x0006 | Tamper Status        | Контроль розкриття корпусу |
| 0x0007 | Firmware Version     | Версія прошивки            |
| 0x0008 | Communication Status | Стан каналу зв'язку        |

Алгоритм передачі даних представлений на рисунку 2.8.

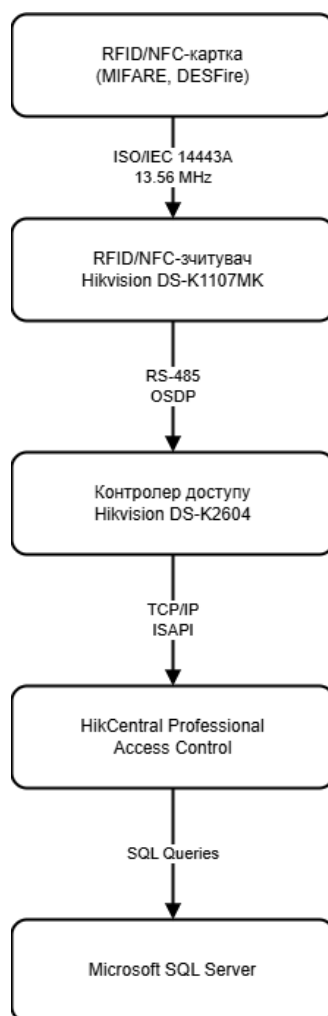


Рисунок 2.8 – Алгоритм передачі даних між контролерами DS-K2604 та сервером HikCentral Professional

Після зчитування картки контролер отримує пакет даних UID такого формату:

STX  
Reader\_ID  
Card\_UID  
Timestamp  
CRC16  
ETX

де:

- STX — початок кадру;
- Reader\_ID — адреса зчитувача;

- Card\_UID — унікальний номер RFID/NFC-носія;
- Timestamp — час події;
- CRC16 — контрольна сума;
- ETX — кінець кадру.

Після обробки контролером та сервером подія зберігається у Microsoft SQL Server за структурою представленою в таблиці 2.3.

Таблиця 2.3 – Структура запису події у базі даних

| Поле          | Тип         |
|---------------|-------------|
| Event_ID      | BIGINT      |
| User_ID       | INT         |
| Card_UID      | VARCHAR(32) |
| Reader_ID     | INT         |
| Controller_ID | INT         |
| Access_Point  | VARCHAR(50) |
| Event_Time    | DATETIME    |
| Event_Result  | VARCHAR(20) |
| Camera_ID     | INT         |

Саме така структура дозволяє реалізувати подальшу інтеграцію із системою відеоспостереження, модулем аналітики та мобільним застосунком Hik-Connect. Для дипломної роботи це вже буде повноцінний опис інформаційного обміну між RFID/NFC-зчитувачами, контролерами DS-K2604 та серверним програмним забезпеченням СКУД.

### 3. СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СЕРВЕРНОЇ ЧАСТИНИ СКУД ТА ЇЇ ВЗАЄМОДІЯ З МОБІЛЬНИМ ЗАСТОСУНКОМ NIK-CONNECT

#### 3.1 Програмне забезпечення серверної частини комп'ютерно-інтегрованої системи контролю та управління доступом

Серверна частина [23] розробленої комп'ютерно-інтегрованої системи контролю та управління доступом реалізується на базі програмного комплексу HikCentral Professional Access Control, який встановлюється на сервер Dell PowerEdge T350 та виконує функції централізованого керування всіма підсистемами комплексу. Дане програмне забезпечення є ядром інформаційної системи та забезпечує взаємодію між контролерами доступу, системою відеоспостереження, мобільними застосунками користувачів і базою даних мешканців житлового комплексу.

Архітектура серверного програмного забезпечення побудована за модульним принципом. Основними компонентами є сервер авторизації, сервер керування доступом, модуль інтеграції відеоспостереження, база даних користувачів, модуль формування подій та підсистема мобільного доступу. Усі модулі взаємодіють між собою через внутрішню сервісну шину обміну повідомленнями та забезпечують централізовану обробку інформації від усіх пристроїв системи.

Після запуску програмний комплекс автоматично встановлює з'єднання з контролерами Hikvision DS-K2604, отримує їх конфігурацію та здійснює постійний моніторинг технічного стану. У разі втрати зв'язку із будь-яким пристроєм система формує повідомлення для адміністратора та реєструє відповідну подію у журналі.

Однією з основних функцій серверного програмного забезпечення є централізоване управління базою користувачів [24]. Для кожного мешканця

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 36   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

можуть зберігатися персональні дані, RFID-ідентифікатори, NFC-ключі, права доступу до окремих зон комплексу, інформація про транспортні засоби та історія відвідувань. Усі зміни в правах доступу автоматично синхронізуються з контролерами DS-K2604, що дозволяє оперативно блокувати або надавати доступ без необхідності фізичного перепрограмування обладнання.

Важливою складовою системи є модуль обробки подій доступу. Під час кожної спроби проходу сервер отримує від контролера інформацію про ідентифікатор користувача, точку проходу, дату та час події, а також результат перевірки прав доступу. Отримані дані зберігаються у централізованій базі даних та можуть використовуватися для формування звітів, статистичного аналізу або проведення аудиту безпеки.

Програмне забезпечення підтримує інтеграцію з системою відеоспостереження. Кожна подія доступу автоматично прив'язується до відеозапису з найближчої IP-камери Hikvision DS-2CD2143G2-I. Це дозволяє оператору швидко переглянути відеофрагмент, який відповідає конкретному факту проходу або спробі несанкціонованого доступу. Такий підхід значно підвищує ефективність розслідування інцидентів та спрощує пошук необхідних відеоматеріалів.

Окремий модуль забезпечує роботу підсистеми контролю паркінгу. Сервер отримує інформацію про всі операції відкриття шлагбаума, веде журнал в'їздів та виїздів транспортних засобів, а також може реалізовувати додаткові механізми контролю, зокрема обмеження кількості паркомісць або часові правила доступу.

Для взаємодії із мешканцями використовується модуль мобільного доступу, який інтегрується з платформою Hik-Connect. Завдяки цьому користувачі можуть дистанційно відкривати двері та ворота, отримувати повідомлення про події системи, переглядати відеопотоки з камер спостереження та створювати тимчасові перепустки для гостей. Передача

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 37   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

інформації між мобільним застосунком та сервером здійснюється через захищені мережеві протоколи із використанням механізмів шифрування та автентифікації користувачів.

Передбачена також функція програмного комплексу – формування звітності. Адміністратор системи може отримувати звіти про проходи мешканців, історію подій доступу, тривожні повідомлення, роботу обладнання та статистику використання точок доступу. Звіти можуть формуватися за довільний проміжок часу та експортуватися у формати PDF, XLSX або CSV для подальшого аналізу.

Для забезпечення надійності функціонування системи використовується централізована база даних Microsoft SQL Server. База даних забезпечує зберігання інформації про користувачів, пристрої, права доступу, журнали подій та відеоіндекси. Використання реляційної СУБД дозволяє забезпечити швидкий пошук інформації, високу продуктивність та можливість резервного копіювання даних.

Таким чином, програмне забезпечення HikCentral Professional Access Control виконує функції центрального керуючого вузла комп'ютерно-інтегрованої системи контролю та управління доступом житлового комплексу. Воно забезпечує інтеграцію всіх апаратних компонентів, централізоване адміністрування, ведення журналів подій, відеоверифікацію проходів, мобільний доступ та формування аналітичної звітності, що дозволяє створити єдиний інформаційний простір безпеки житлового комплексу.

Представлена на рисунку 3.1 структура програмного забезпечення серверної частини СКУД реалізує трирівневу архітектуру, яка забезпечує централізоване управління всіма компонентами комп'ютерно-інтегрованої системи контролю та управління доступом житлового комплексу. Такий підхід дозволяє розділити функції взаємодії з користувачами, обробки

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 38   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

інформації та керування обладнанням, що підвищує надійність, масштабованість і зручність адміністрування системи.

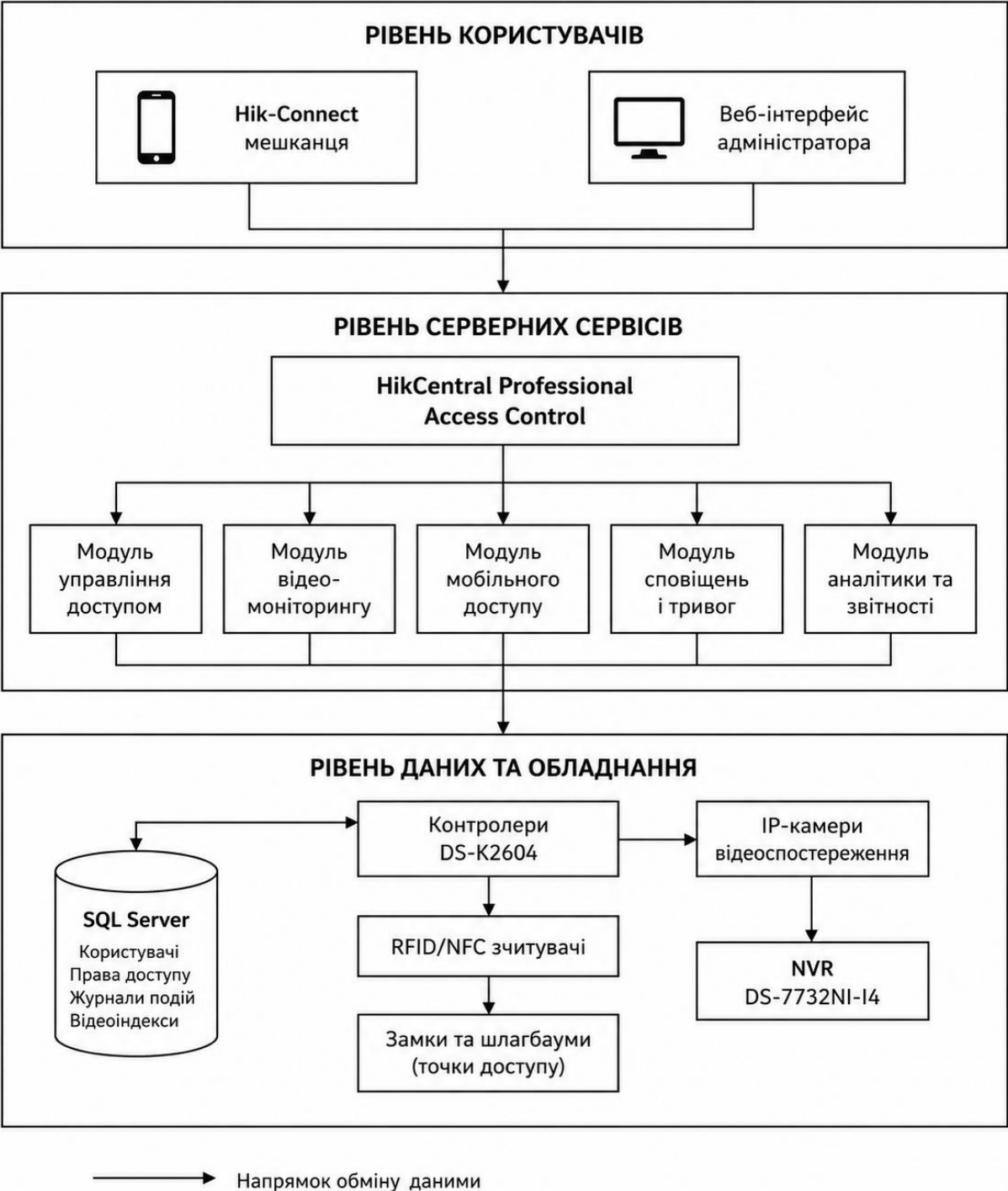


Рисунок 3.1 – Трирівнева структура програмного забезпечення серверної частини СКУД

На верхньому рівні архітектури розташовано рівень користувачів, який представлений мобільним застосунком Hik-Connect та веб-інтерфейсом адміністратора. Мобільний застосунок використовується мешканцями житлового комплексу для взаємодії із системою безпеки через смартфон. За його допомогою користувачі можуть відкривати двері під'їздів і ворота паркінгу, переглядати відео з камер спостереження, отримувати повідомлення про події та створювати тимчасові перепустки для гостей. Веб-інтерфейс адміністратора призначений для налаштування системи, керування правами доступу, моніторингу роботи обладнання та формування звітів. Обмін інформацією між клієнтськими пристроями та серверною частиною здійснюється через захищені мережеві протоколи, що забезпечують конфіденційність та цілісність даних.

Центральним елементом архітектури є рівень серверних сервісів, основу якого становить програмний комплекс HikCentral Professional Access Control. Саме цей компонент виконує функції централізованого керування всією системою, координує роботу контролерів доступу, забезпечує обробку подій та взаємодію між окремими програмними модулями. Усі запити від користувачів, а також повідомлення від апаратних пристроїв проходять через HikCentral, який виступає єдиним центром обробки інформації.

У складі серверного рівня функціонує модуль управління доступом. Його основним призначенням є зберігання та перевірка прав користувачів, керування режимами роботи точок доступу та обробка подій проходів. При отриманні запиту на доступ модуль перевіряє наявність відповідних дозволів у базі даних та формує команди для контролерів DS-K2604. Завдяки цьому забезпечується централізоване адміністрування всієї системи без необхідності окремого налаштування кожного контролера.

Модуль відеомоніторингу забезпечує інтеграцію системи контролю доступу із підсистемою відеоспостереження. Його завданням є отримання відеопотоків від IP-камер, керування записом відеоархіву та прив'язка

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 40   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

відеоданих до подій доступу. Наприклад, під час проходження мешканця через контрольовану точку система автоматично може сформувати посилання на відповідний відеофрагмент, що значно спрощує аналіз подій безпеки.

Модуль мобільного доступу [25] відповідає за взаємодію із застосунком Hik-Connect. Він обробляє команди користувачів, виконує перевірку їхніх повноважень та забезпечує передачу інформації між мобільними пристроями і сервером. Через цей модуль реалізуються функції цифрового ключа, віддаленого відкриття дверей та створення гостьових перепусток.

Важливу роль відіграє модуль сповіщень і тривоги. Він здійснює моніторинг подій системи та автоматично генерує повідомлення при виникненні нестандартних ситуацій. До таких подій можуть належати спроби несанкціонованого доступу, тривале перебування дверей у відкритому стані, відключення обладнання або втрата зв'язку з контролерами. Інформація передається адміністратору або безпосередньо мешканцям через мобільний застосунок.

Для підвищення ефективності управління системою використовується модуль аналітики та звітності. Він виконує обробку накопичених даних та формує статистичну інформацію щодо використання точок доступу, активності користувачів, кількості подій доступу та роботи обладнання. Результати аналізу можуть відображатися у вигляді таблиць, графіків або автоматично сформованих звітів.

Нижній рівень архітектури становлять база даних та апаратні засоби системи. Центральним елементом цього рівня є Microsoft SQL Server [26-28], у якому зберігаються персональні дані мешканців, права доступу, інформація про RFID/NFC-ідентифікатори, журнали подій та індекси відеоархіву. База даних є основним джерелом інформації для всіх програмних модулів серверної частини.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 41   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

Безпосереднє керування точками доступу здійснюють контролери Hikvision DS-K2604. Вони отримують команди від сервера та взаємодіють із RFID/NFC-зчитувачами, які забезпечують ідентифікацію користувачів. Після підтвердження права доступу контролер подає команду на відкриття електромагнітного замка або шлагбаума. Одночасно інформація про подію передається до серверної частини для подальшої обробки та зберігання.

Окремою складовою рівня обладнання є система відеоспостереження, представлена IP-камерами та мережевим відеореєстратором NVR DS-7732NI-I4. IP-камери здійснюють безперервний моніторинг території житлового комплексу, а відеореєстратор забезпечує централізоване зберігання архіву відеозаписів. Інтеграція відеоспостереження з підсистемою контролю доступу дозволяє підвищити рівень безпеки та забезпечити відеоверифікацію всіх подій проходку.

Таким чином, представлена архітектура забезпечує комплексну взаємодію користувачів, серверного програмного забезпечення та апаратних засобів СКУД. Централізована обробка інформації, інтеграція із системою відеоспостереження та підтримка мобільного доступу створюють єдиний інформаційний простір безпеки житлового комплексу, який відповідає сучасним вимогам до побудови інтелектуальних систем управління доступом.

### 3.2 Обґрунтування вибору мобільного застосунку Hik-Connect

У розробленій комп'ютерно-інтегрованій системі контролю та управління доступом житлового комплексу як мобільний клієнт обрано застосунок Hik-Connect. Даний програмний продукт розроблений компанією Hikvision та призначений для віддаленого управління пристроями безпеки,

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 42   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

системами відеоспостереження, домофонії та контролю доступу через мережу Інтернет.

Вибір Hik-Connect обумовлений тим, що всі основні компоненти запропонованої системи, зокрема контролери доступу Hikvision DS-K2604, IP-камери Hikvision DS-2CD2143G2-I та програмний комплекс HikCentral Access Control, належать до єдиної екосистеми Hikvision. Це забезпечує повну програмну та апаратну сумісність усіх елементів системи без необхідності використання додаткових програмних шлюзів або сторонніх сервісів інтеграції.

Використання Hik-Connect дозволяє реалізувати концепцію цифрового ключа, відповідно до якої смартфон мешканця виступає засобом ідентифікації та управління доступом. Завдяки цьому усувається необхідність постійного використання RFID-карток або брелоків, а права доступу можуть змінюватися дистанційно адміністратором системи.

Важливою перевагою застосунку є підтримка хмарної архітектури. Усі команди керування передаються через захищений хмарний сервіс Hik-Connect Cloud, що забезпечує можливість роботи користувача незалежно від його місцезнаходження. При цьому система підтримує шифрування даних та багаторівневу автентифікацію користувачів, що підвищує рівень кібербезпеки комплексу.

Функціональні можливості застосунку охоплюють дистанційне відкриття дверей та воріт, перегляд відеопотоків із камер спостереження, отримання повідомлень про події доступу, створення тимчасових перепусток для гостей та контроль історії відвідувань. Таким чином, мешканець отримує централізований інструмент керування всіма сервісами безпеки житлового комплексу.

Архітектура взаємодії Hik-Connect із системою контролю доступу здійснюється наступним чином. Архітектура функціонування мобільного застосунку побудована за клієнт-серверним принципом. Смартфон

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 43   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

користувача виконує роль клієнтського пристрою, через який здійснюється взаємодія із серверною частиною системи (рисунк 3.2).

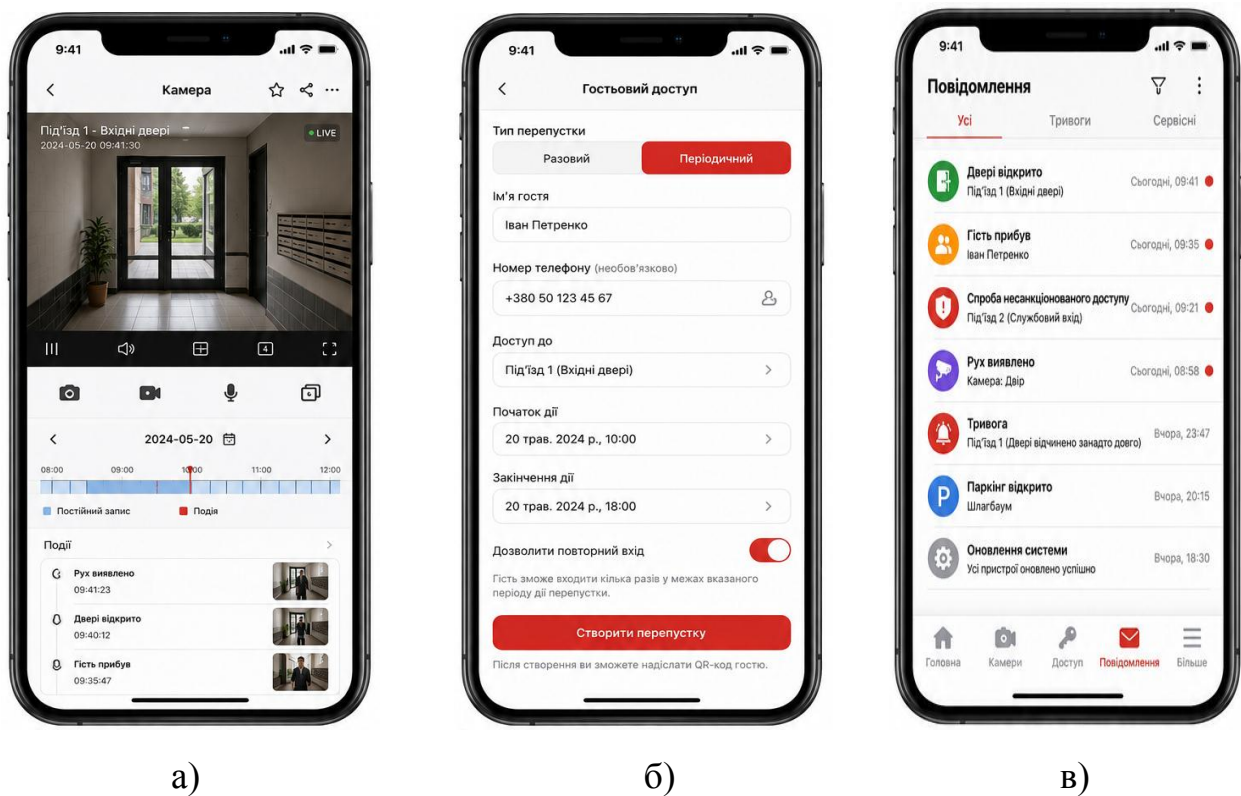


Рисунок 3.2 – Приклади екранів на смартфоні взаємодії із серверною частиною системи.

Після запуску застосунку користувач проходить процедуру автентифікації. Після підтвердження облікового запису мобільний застосунок встановлює захищене з'єднання з хмарним сервером Hik-Connect. Усі запити користувача передаються через хмарну платформу до серверного комплексу HikCentral Access Control, який взаємодіє з контролерами доступу та іншими пристроями системи.

У випадку дистанційного відкриття дверей користувач надсилає команду через інтерфейс застосунку. Команда передається на сервер HikCentral, після чого відповідний контролер DS-K2604 отримує команду на активацію релейного виходу та розблокування електромагнітного замка.

Одночасно інформація про подію записується до журналу системи та може бути прив'язана до відеозапису з найближчої камери спостереження.

Архітектура також забезпечує двосторонній обмін інформацією. Окрім надсилання команд користувачем, сервер може передавати повідомлення про виклики домофона, тривожні події, спроби несанкціонованого доступу та інші системні сповіщення (рисунок 3.2, в).

Як зазначалося в якості мобільного застосунку мешканця доцільно використовувати Hik-Connect, функції якого:

- відкриття дверей через смартфон;
- отримання повідомлень;
- перегляд камер;
- створення тимчасових перепусток;
- контроль відвідувачів.

Мешканець отримує можливість повноцінно керувати доступом без фізичних карток, що відповідає сучасним концепціям Smart Building.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 45   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

## ВИСНОВКИ

1. В результаті виконання кваліфікаційної роботи було проведено аналіз сучасних підходів до побудови комп'ютерно-інтегрованих систем контролю та управління доступом житлових комплексів та визначено основні вимоги до їх функціонування в умовах сучасної концепції Smart Building.

2. На основі проведеного аналізу запропоновано архітектуру централізованої комп'ютерно-інтегрованої системи контролю та управління доступом для житлового комплексу на 3–5 під'їздів із кількістю мешканців від 200 до 500 осіб. Розроблена структура системи поєднує RFID/NFC-ідентифікацію користувачів, систему відеоспостереження, серверне програмне забезпечення та мобільний застосунок мешканця в єдиному інформаційному середовищі.

3. Обґрунтовано вибір технічних засобів системи, зокрема контролера доступу Hikvision DS-K2604, RFID/NFC-зчитувачів, IP-камер відеоспостереження, мережевого відеореєстратора та серверного обладнання. Показано, що використання обладнання одного виробника забезпечує високий рівень сумісності компонентів та спрощує процес інтеграції системи.

4. Розроблено структурну схему програмного забезпечення серверної частини на базі комплексу HikCentral Professional Access Control, який забезпечує централізоване управління користувачами, правами доступу, подіями системи та інтеграцію із підсистемою відеоспостереження.

5. Досліджено особливості інформаційної взаємодії між RFID/NFC-зчитувачами, контролерами доступу та сервером системи. Розглянуто використовувані протоколи передачі даних, формати повідомлень та структуру зберігання інформації в базі даних Microsoft SQL Server.

6. Розроблено алгоритм функціонування контролера доступу Hikvision DS-K2604, який забезпечує перевірку прав користувачів, прийняття рішень

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 46   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

щодо надання доступу, керування виконавчими пристроями та реєстрацію подій у системі.

7. Використання мобільного застосунку Hik-Connect дозволяє реалізувати функції віддаленого відкриття дверей, моніторингу відеокамер, отримання сповіщень та створення тимчасових перепусток для відвідувачів, що підвищує зручність експлуатації системи та рівень безпеки житлового комплексу.

8. Отримані результати можуть бути використані під час проєктування та впровадження сучасних систем контролю та управління доступом у багатоквартирних житлових будинках, житлових комплексах та інших об'єктах цивільної інфраструктури.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 47   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Системи контролю та управління доступом : навчальний посібник / В. М. Дубовой, О. В. Матвійчук. – Вінниця : ВНТУ, 2020. – 165 с.
2. Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. – 3rd ed. – Wiley, 2010. – 462 p.
3. Комп'ютерно-інтегровані технології та системи управління : підручник / за ред. П. Г. Берника. – Львів : Новий Світ-2000, 2021. – 420 с.
4. Автоматизовані системи керування технологічними процесами та виробництвами / М. Г. Коваленко. – Київ : Ліра-К, 2019. – 352 с.
5. Буров Є. В. Інформаційні системи та технології : навчальний посібник. – Львів : Магнолія 2006, 2020. – 336 с.
6. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі. – Київ : Юніор, 2018. – 672 с.
7. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою.
8. ДСТУ EN 60839-11-1:2018. Системи тривожної та електронної безпеки. Системи електронного контролю доступу.
9. ISO/IEC 14443-1:2018. Identification cards – Contactless integrated circuit cards – Proximity cards.
10. ISO/IEC 14443-2:2020. Identification cards – Contactless integrated circuit cards – Proximity cards – Radio frequency power and signal interface.
11. Want R. An Introduction to RFID Technology // IEEE Pervasive Computing. – 2006. – Vol. 5, No. 1. – P. 25–33.
12. Coskun V., Ozdenizci B., Ok K. Professional NFC Application Development for Android. – Wiley, 2013. – 456 p.
13. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2020. – 784 p.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 48   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

14. Tanenbaum A., Wetherall D. Computer Networks. – 6th ed. – Pearson, 2021. – 960 p.

15. Hikvision. DS-K2604 Access Controller User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024. – 188 p.

16. Hikvision. DS-K1107 Series Card Reader User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024.

17. Hikvision. DS-2CD2143G2-I Network Camera User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024.

18. Hikvision. DS-7732NI-I4 Network Video Recorder User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024.

19. Компанія SmartEl розумна електроніка. Мережевий контролер Hikvision DS-K2604. Режим доступу: <https://smartel.ua/ua/product/setevoy-kontroller-hikvision-ds-k2604/?srsltid=AfmBOoooZPRL0niy27TbaAfAEtSfcSMfqaGuO0JbLEHHhIqrk2Am4Ug->

20. Компанія SmartEl розумна електроніка. Замок електромагнітний YM-280(BLED). Режим доступу: [https://smartel.ua/ua/product/zamok-elektromagnitnyy-ym-280-bled/?gad\\_source=1&gad\\_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdfuDnolv7uTYh&gclid=Cj0KCQjw2\\_TQBhCnARIsAF3-XhzsV3L3rtj2jbPyzqqO7qkG6ofzCAY6EmyejQ9CYuo0gEQQwsWI2MkaAvD2EALw\\_wcB](https://smartel.ua/ua/product/zamok-elektromagnitnyy-ym-280-bled/?gad_source=1&gad_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdfuDnolv7uTYh&gclid=Cj0KCQjw2_TQBhCnARIsAF3-XhzsV3L3rtj2jbPyzqqO7qkG6ofzCAY6EmyejQ9CYuo0gEQQwsWI2MkaAvD2EALw_wcB)

21. Компанія SmartEl розумна електроніка. IP відеокамера DS-2CD2143G2-I. Режим доступу: [https://smartel.ua/ua/product/ip-videokamera-ds-2cd2143g2-i/?gad\\_source=1&gad\\_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdfuDnolv7uTYh&gclid=Cj0KCQjw2\\_TQBhCnARIsAF3-XhyS0VweN20AeKfpzY45XANVga9cn0bJSXg2SdEIAGTVHyyXdlmJYxYaAuszEALw\\_wcB](https://smartel.ua/ua/product/ip-videokamera-ds-2cd2143g2-i/?gad_source=1&gad_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdfuDnolv7uTYh&gclid=Cj0KCQjw2_TQBhCnARIsAF3-XhyS0VweN20AeKfpzY45XANVga9cn0bJSXg2SdEIAGTVHyyXdlmJYxYaAuszEALw_wcB)

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 49   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

22. Компанія SmartEl розумна електроніка. IP відеореєстратор Hikvision DS-7732NI-I4/24P. Режим доступу: [https://smartel.ua/ua/product/ip-videoregistrator-hikvision-ds-7732ni-i4-24p/?gad\\_source=1&gad\\_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdFuDnulv7uTYh&gclid=Cj0KCQjw2\\_TQBhCnARIsAF3-Xhz6IAsTX3XPTkm3VHYGSTl-87rQXgaoQvQutVtLdOM6QaJBgV4aipgaAjWKEALw\\_wcB](https://smartel.ua/ua/product/ip-videoregistrator-hikvision-ds-7732ni-i4-24p/?gad_source=1&gad_campaignid=23772062092&gbraid=0AAAAADtn4WfzKTeAITvXdFuDnulv7uTYh&gclid=Cj0KCQjw2_TQBhCnARIsAF3-Xhz6IAsTX3XPTkm3VHYGSTl-87rQXgaoQvQutVtLdOM6QaJBgV4aipgaAjWKEALw_wcB)

23. Hikvision. HikCentral Professional Access Control Module User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024.

24. Silberschatz A., Korth H., Sudarshan S. Database System Concepts. – 7th ed. – McGraw-Hill, 2020. – 1376 p.

25. Hikvision. Hik-Connect Mobile Client User Manual. – Hangzhou : Hikvision Digital Technology Co., Ltd., 2024.

26. Elmasri R., Navathe S. Fundamentals of Database Systems. – 7th ed. – Pearson, 2017. – 1272 p.

27. Microsoft Corporation. SQL Server 2022 Documentation. – Redmond : Microsoft, 2024.

28. Microsoft Corporation. Windows Server 2022 Documentation. – Redmond: Microsoft, 2024.

29. Dell Technologies. PowerEdge T350 Technical Guide. – Dell Inc., 2024. Призначення: характеристики серверного обладнання.

30. OSDP Verified Compliance Specification. – Security Industry Association (SIA), 2023.

31. Bregman D. Smart Building Systems for Architects, Owners and Builders. – Elsevier, 2022. – 398 p.

32. Методичні рекомендації до виконання випускної кваліфікаційної роботи освітнього ступеня «Магістр». Галузь знань 15 – Автоматизація та приладобудування, спеціальність 151 – Автоматизація та комп'ютерно-інтегровані технології освітньо-професійна програма – Автоматизація та

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 50   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

комп'ютерно-інтегровані технології / А.І. Сегін, Н.Я. Возна, І.Р. Пітух / Під ред. Я.М. Николайчука – Тернопіль: ТНЕУ, 2020.– 40 с.

33. Загальні методичні рекомендації з підготовки, оформлення, захисту та оцінювання кваліфікаційних робіт здобувачів вищої освіти першого «бакалаврського» і другого «магістерського» рівнів. // Укладачі: В. М. Островерхов, Л. І. Біловус, К. З. Возьний, О. О. Луцишин, Г. Л. Монастирський, С. В. Питель, С. А. Надвиничний, С. К. Шандрук. Тернопіль: ЗУНУ, 2024. – 89 с.

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 51   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |

ДОДАТОК А.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ

|     |      |          |       |      |                              |      |
|-----|------|----------|-------|------|------------------------------|------|
|     |      |          |       |      | ДП.АКІТ.1156026100.00.000.ПЗ | Арк. |
|     |      |          |       |      |                              | 52   |
| Зм. | Арк. | № докум. | Підп. | Дата |                              |      |