Західноукраїнський національний університет
Факультет комп’ютерних інформаційних технологій
Кафедра спеціалізованих комп’ютерних систем

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

освітнього ступеня "магістр"
на тему:

Комп’ютерно-інтегрована система захисту від несанкціонованого проникнення на об’єкт закритого типу /
Computer-integrated system for protection against unauthorized entry into a closed facility

Виконав студент групи АКІТм-21
Гарліцький Руслан Васильович

Керівник роботи: к.т.н., доцент Албанський І.Б.

Тернопіль2025

Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем
Освітній ступінь "магістр"
Спеціальність – 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані технології

ЗАТВЕРДЖУЮ
Завідувач кафедри СКС
_____ А.І.Сегін
04 грудня 2024 р.

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТА

Гарліцький Руслан Васильович
(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Комп'ютерно-інтегрована система захисту від несанкціонованого проникнення на об'єкт закритого типу / Computer-integrated system for protection against unauthorized entry into a closed facility.
Керівник роботи: к.т.н., доцент Албанський І.Б.

Затверджені наказом по університету від 28 листопада 2024 р. № 938.

2. Строк подання студентом закінченої кваліфікаційної роботи
1 грудня 2025р.

3. Вихідні дані до кваліфікаційної роботи:
1. Аналіз та дослідження систем контролю управління доступом.
2. Структура та функціональні схеми комп'ютерно-інтегрованої системи.
3. Процеси збору й обробки інформації в автоматизованих системах.
4. Метод асоціативного навчання нейронної мережі для функціонування можливостей інтегрованих систем безпеки.

4. Основні питання, які потрібно розробити
1. Дослідження систем контролю управління доступом.
2. Обґрунтування вибору основних засобів автоматизації та розробка комп'ютерно-інтегрованої системи.
3. Коригування ієрархічних структур, об'єктів систем безпеки методами нейронних мереж.

5. Перелік графічного матеріалу у роботі

1. Структура та блок-схема алгоритму роботи комп'ютерно-інтегрованої системи захисту об'єкта закритого типу.

Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Албанський І.Б., к.т.н., доцент кафедри СКС		
2	Албанський І.Б., к.т.н., доцент кафедри СКС		
3	Албанський І.Б., к.т.н., доцент кафедри СКС		

7. Дата видачі завдання 2 грудня 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз систем контролю управління доступом	12.2024р. – 02.2025р.	виконано
2	Обґрунтування вибору основних засобів автоматизації та розробка комп'ютерно-інтегрованої системи	03.2025р. – 06.2025р.	виконано
3	Розробка методу асоціативного навчання нейронної мережі для функціонування можливостей інтегрованих систем безпеки	07.2025р. – 11.2025р.	виконано
4	Остаточне оформлення та подача кваліфікаційної роботи на перевірку щодо плагіату та виправлення недоліків	11.2025р. – 12.2025р.	виконано

Студент _____ Гарліцький Р.В.
(підпис)

Керівник роботи _____ к.т.н., доцент Албанський І.Б.
(підпис)

АНОТАЦІЯ

Гарліцький Р.В. Комп’ютерно-інтегрована система захисту від несанкціонованого проникнення на об’єкт закритого типу. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю – 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка», освітньо-професійна програма – «Автоматизація та комп’ютерно-інтегровані технології» - Західноукраїнський національний університет. Тернопіль, 2025.

У роботі: досліджені систем контролю управління доступом; визначені етапи проектування універсальних СКУД для багатофункціональних задач сьогодення; розроблено структуру та алгоритм роботи комп’ютерно-інтегрованої системи захисту об’єкта закритого типу; обґрунтовано вибір засобів автоматизації запропонованої структури СКУД; проведено коригування ієрархічних структур, об'єктів систем безпеки методами нейронних мереж; запропоновано спосіб формування вихідних даних щодо пріоритетності функцій ІСБ.

ANNOTATION

Garlitsky R.V. Computer-integrated system of protection against unauthorized penetration into a closed facility. – Manuscript.

Research for obtaining a master's degree in the specialty - 174 "Automation, computer-integrated technologies and robotics", educational and professional program - "Automation and computer-integrated technologies" - Western Ukrainian National University. Ternopil, 2025.

The work: studies access control systems; identifies the stages of designing universal ACS for multifunctional tasks of today; develops the structure and algorithm of the computer-integrated system for the protection of a closed-type facility; justifies the choice of automation tools for the proposed ACS structure; adjusts hierarchical structures and security system objects using neural network methods; proposes a method for generating output data regarding the priority of ACS functions.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСК - автоматизованих систем керування;

СКУД - система контролю та управління доступом;

ПЗ – програмне забезпечення;

КПР - контрольно-пропускного режиму;

АСУ - автоматизована система управління;

АСУ ТП - автоматизована система управління технологічним процесом;

АЦП - аналого-цифровий перетворювач;

ЦАП - цифро-аналоговий перетворювач;

ОК - об’єкт керування;

КПП – контрольно-пропускний пункт;

ПІД - пропорційно-інтегрально-диференціальний;

ОМС - оператор-моніторингова система;

ПЛК - програмовано-логічний контролер;

АРМ - автоматизоване робоче місце;

ІЧ - інфрачервоний;

БД – база даних;

ПК - персональний комп'ютер;

ОЗТ - об'єкти закритого типу;

МАІ - метод аналізу ієрархій;

ІСБ - інтегрована система безпеки;

ІУ - індекс узгодженості;

ССТС - структурно-складних технічних систем.

ВСТУП

Актуальність теми. У сучасних умовах зростання кіберзлочинності та ускладнення методів несанкціонованого проникнення, забезпечення безпеки об'єктів закритого типу стає пріоритетним завданням національної безпеки.

Актуальність створення комп’ютерно-інтегрованої системи захисту від несанкціонованого проникнення (КІСЗ) на об’єкті закритого типу (наприклад, підприємство, склад, дата-центр, державний об’єкт) є дуже високою з огляду на сучасні загрози, технологічний розвиток і нормативні вимоги. З огляду на це можна навести основні ключові аргументи, чому така система — не просто доцільна, а необхідна.

Зростання і ускладнення загроз безпеці, а саме синтез кібер- і фізичних загроз, тобто сучасні зловмисники дедалі частіше комбінують фізичні проникнення з кібернападами — доступ до внутрішньої мережі може дати змогу піти далі в атаці. КІСЗ дозволяє поєднувати контролюючі системи (відеоспостереження, датчики руху) з системами кіберзахисту.

Інсайдерські загрози, тобто співробітники можуть ненавмисно або навмисно порушити фізичну безпеку. Інтегрована система дозволяє відстежувати аномальну активність, комбінуючи доступні дані (відео, RFID-браслети, контроль доступу).

До основних перспектив розвитку можна віднести перспективи розвитку використання штучного інтелекту (AI) для аналізу відеопотоків, виявлення незвичної поведінки або аномалій. Інтеграція з блокчейн-технологіями для захисту логів доступу та подій — підвищення цілісності записів. Використання біометрії (відбитки пальців, розпізнавання обличчя) у поєднанні з класичними системами контролю доступу для багаторівневого захисту.

Комп’ютерно-інтегрована система захисту від несанкціонованого проникнення — це не «розкіш», а необхідний елемент безпеки сучасного закритого об’єкта. Вона забезпечує:

- багаторівневий і глибокий захист (фізичний + кібер);
- швидку реакцію на загрози;
- економію ресурсів;
- відповідність регуляторним вимогам;
- підвищену репутацію й довіру.

У світі, де загрози стають розумнішими, об’єкти — все більш автоматизованими, а нормативи — жорсткішими, впровадження такої системи є стратегічним кроком на користь безпеки, стабільності і розвитку.

Мета і завдання дослідження. Метою роботи є дослідження і проектування комп’ютерно-інтегрованої системи захисту від несанкціонованого проникнення на об’єкт закритого типу та розробка методу асоціативного навчання нейронної мережі для функціонування можливостей інтегрованих систем безпеки.

Для досягнення поставленої мети роботи необхідно:

- проаналізувати відомі методи та алгоритми навчання нейронних мереж для роботи з інтегрованими системами безпеки;
- дослідити відомі системи контролю управління доступом;
- проаналізувати засоби автоматизації та структури систем контролю і управління доступом, апаратне та програмне забезпечення відповідно;
- розробити структурну (функціональну) комп’ютерно-інтегрованої системи захисту від несанкціонованого проникнення на об’єкт закритого типу;
- обґрунтувати вибір засобів автоматизації запропонованої системи контролю і управління доступом;
- скорегувати ієрархічні структури об’єктів систем безпеки методами нейронних мереж;
- дослідити способи формування вихідних даних щодо пріоритетності функцій інтегрованих систем безпеки.

Об’єкт дослідження: процеси автоматизації та контролю керування доступом інтегрованих систем безпеки на об’єктах з підвищеним рівнем безпеки.

Предметом дослідження є автоматизована система контролю і управління доступом на об’єкт закритого типу.

Наукова новизна одержаних результатів: розроблено метод асоціативного навчання нейронної мережі для функціонування можливостей інтегрованих систем безпеки та проведено коригування ієрархічних структур об’єктів, систем безпеки запропонованої комп’ютерно-інтегрованої системи шляхом застосування способів формування вихідних даних щодо пріоритетності функцій інтегрованих систем безпеки, що забезпечує високоефективну роботу такої системи.

Практичне значення отриманих результатів: універсальність, гнучкість, простота та можливість масштабування інтегрованих систем безпеки запропонованої комп’ютерно-інтегрованої системи захисту від несанкціонованого проникнення, що дозволяє ефективніше виявляти несанкціоновані або злочині проникнення на об’єкти закритого типу.

Апробація. На основі досліджень підготовлено та опубліковано 2 тези доповідей на наукових конференціях (додаток А).

1. АНАЛІЗ СИСТЕМ КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

1.1 Дослідження систем контролю управління доступом

Контроль управління доступом (Access Control) в контексті автоматизованих систем керування (АСК) — це комплекс технічних, програмних та організаційних заходів, спрямованих на регламентацію прав доступу користувачів, систем та компонентів до ресурсів АСК відповідно до визначених політик безпеки.

Автоматизована система контролю та управління доступом (СКУД) — це комплекс програмних та технічних засобів для автоматизації пропускного режиму: обмеження доступу людей та транспорту на територію та приміщення, а також для обліку робочого часу (рисунок 1.1). Основні завдання СКУД включають запобігання несанкціонованому проникненню, ідентифікацію користувачів, розмежування зон доступу та ведення журналів подій. Як ідентифікатори використовуються карти, брилки, біометричні дані (відбиток пальця, обличчя) або PIN-коди.

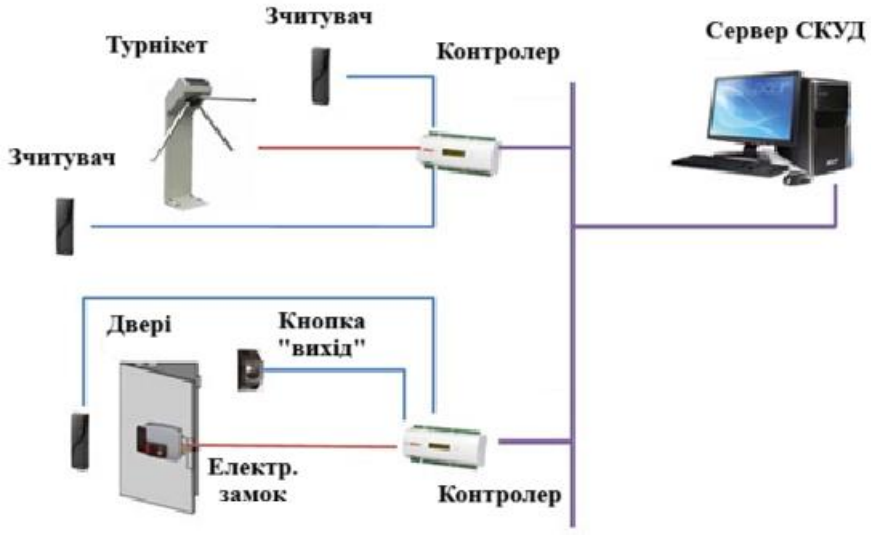


Рисунок 1.1 – Загальна структура СКУД

До основних ключових компонентів системи контролю доступу можна віднести:

- ідентифікацію — процес розпізнавання суб'єкта доступу (користувача, системи, процесу);

- аутентифікація — підтвердження автентичності ідентифікатора;

- авторизація — надання визначених прав доступу до певних ресурсів;

- аудиторський контроль — фіксація та аналіз подій доступу.

Основними функціями СКУД є:

- обмеження доступу - запобігання небажаному проникненню на об'єкт або в певні зони;

- ідентифікація - перевірка особи користувача за допомогою електронних ключів або біометричних даних;

- облік робочого часу - автоматична реєстрація часу приходу та догляду співробітників;

- розмежування доступу - налаштування прав доступу для різних категорій користувачів залежно від їхньої посади або завдань;

- ведення журналів - реєстрація всіх подій доступу та переміщень для подальшого аналізу;

- інтеграція - можливість інтеграції з іншими системами безпеки, такими як відеоспостереження та сигналізація.

Основними компонентами системи є [1]:

- контролери - "мозок" системи, що приймає рішення про доступ на основі даних;

- зчитувачі - пристрої, які зчитують інформацію з ідентифікаторів (наприклад, карт або біометричних даних);

- ідентифікатори - електронні ключі (карти, брелоки) або біометричні дані, які використовує користувач для проходу;

- виконавчі пристрої (механізми) - устаткування, яке безпосередньо блокує або відкриває прохід (електромагнітні/електромеханічні замки, турнікети, шлагбауми);

- програмне забезпечення дозволяє настроювати систему, керувати користувачами та переглядати звіти.

Загалом розрізняють основні типи СКУД систем, а саме: автономні, мережеві, універсальні. Автономні системи працюють незалежно від центрального сервера і зазвичай керують одним або декількома проходами (рисунок 1.2). Підходять для невеликих об'єктів із простими завданнями. Мережеві СКУД підключені до комп'ютера для централізованого керування, моніторингу та збору даних (рисунок 1.3). Забезпечують більш високий рівень безпеки та контролю. Універсальні СКУД можуть працювати як в мережевому, так і в автономному режимі, автоматично перемикаючись у разі екстреної ситуації (рисунок 1.4).

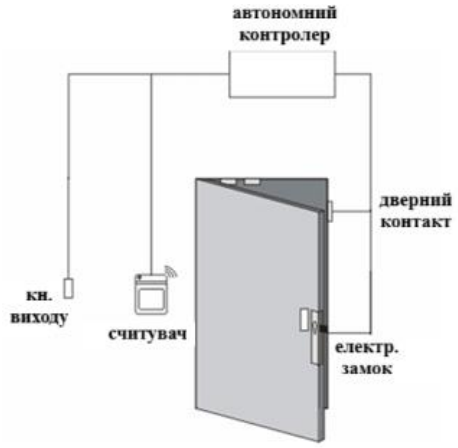


Рисунок 1.2 – Загальний вигляд автономних СКУД

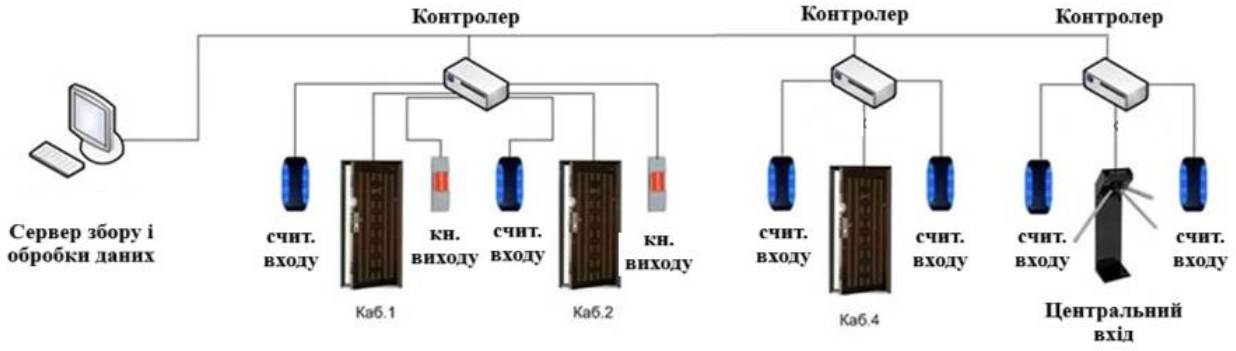


Рисунок 1.3 – Загальний вигляд мережевих СКУД

Універсальна СКУД є складним багаторівневим комплексом, що забезпечує ефективний контроль та управління доступом. Сучасні системи характеризуються: високою надійністю за рахунок архітектури з розподіленими контролерами, масштабованістю для адаптації до змінних

потреб об'єкта, гнучкістю у налаштуванні правил та політик безпеки, інтегрованістю з іншими системами безпеки та корпоративними платформами.

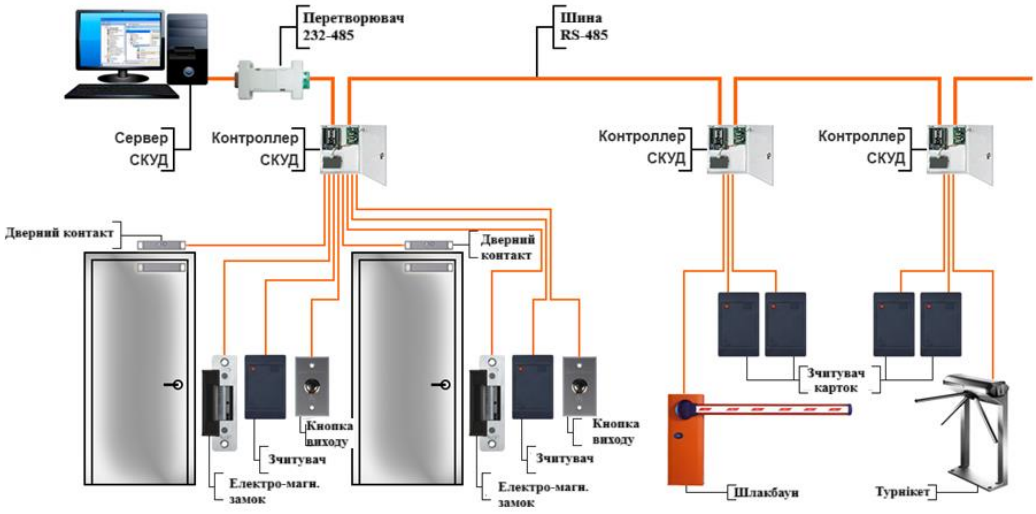


Рисунок 1.4 – Загальний вигляд універсальної СКУД

Алгоритм роботи системи забезпечує комплексну обробку запитів на доступ - від ідентифікації користувача до прийняття рішення та фіксації події. Розвиток технологій спрямований на підвищення зручності, безпеки та інтелектуальності систем, що робить їх невід'ємним елементом сучасної інфраструктури безпеки.

Елементи СКУД не працюють роз'єднано, вони функціонують лише у єдиній системі. Робота її має два напрями - ведення бази всіх осіб, які мають доступ на об'єкт, а також контроль відмикання турнікетів та інших пристроїв, що захищають. Людина практично не впливає на роботу СКУД. Вона працює у повністю автоматичному режимі. Особа отримує доступ до будівлі або на об'єкт декількома способами – за допомогою біометрії обличчя, через пароль, магнітними мітками чи спеціальними картками.

Додатково СКУД веде журнал подій. У ньому видно, коли саме людина контактувала із системою. У разі непередбачених ситуацій, наприклад несанкціонованого проникнення сторонніх осіб, можна з точністю до секунди визначити час. Окрім захисту об'єкта СКУД дозволяє враховувати

відпрацьований співробітниками час. Такі системи знайшли застосування не тільки в офісах та на виробництвах компаній, а й у платних парковках, розважальних та ділових центрах. З їхньою допомогою регулюють потік людей, розмежовують права доступу співробітникам підприємства та організують ефективний захист об'єкта.

На технологічному ринку на сьогодні існують такі класи СКУД [2]:

- 1 клас (Багатофункціональні системи невеликої ємності, що працюють автономно. Найчастіше використовуються в офісах та на невеликих підприємствах. Використовуються для контролю часу виходу і входу у приміщення, реєстрації проходів співробітників. Включають у своєму складі контролер та зчитувач з виконавчим елементом (електронні ключі та магнітні картки, рідко – безконтактні));

- 2 клас (Працюють в мережному режимі. Мають у своєму складі додаткові функції – контроль переміщення персоналу і майна всередині об'єкта, табельний облік, складання баз даних);

- 3 клас (Мережеві СКУД, де контролери об'єднуються в локальну мережу та працюють у режимі реального часу. Найчастіше використовуються на великих підприємствах. Тут можуть впроваджуватися складні ідентифікатори, зокрема біометричний контроль особи);

- 4 клас (СКУД 4 класу – найпотужніші, із сучасним ПЗ, багатим функціоналом та можливістю інтеграції з іншими системами безпеки чи охорони).

Система певного класу вибирається залежно від таких факторів як:

- розміру об'єкта;
- кількості осіб із доступом;
- необхідністю в інтеграції з іншими системами.

Системи контролю та управління доступом обслуговують різну кількість осіб – від 60 до 2800 осіб.

Послуги контролю доступу надаються різними постачальниками, тому їх функції можуть відрізнятися. Тим не менш, кожна система безпеки має базовий набір ключових елементів:

- персональні ідентифікатори для працівників компанії, це можуть бути магнітні картки або жетони, що працюють за безконтактним принципом;

- зчитувачі призначені для зчитування персональних ідентифікаторів;

- пристрої узгодження;

- пристрої контролю управління системи;

- блокатори;

- програмне забезпечення.

Завдяки роботі персональних ідентифікаторів здійснюється контроль доступу персоналу до різних приміщень, а також використання тих чи інших даних. Устаткування зчитує спеціальний код, закладений у брелку або карті, а потім виконує дію, на яку воно запрограмоване, наприклад, відчиняє двері. Якщо код виявляється неправильним, у допуску працівникові буде відмовлено.

СКУД на малих чи великих підприємствах може виконувати ряд функцій:

- управління дозволами та допусками;

- аналіз статистичних даних;

- відстеження роботи працівників організації;

- врахування часу роботи, запізнень, інших порушень робочого розпорядку;

- інтеграція з іншими заходами безпеки та охоронними комплексами.

Установка СКУД дозволяє не лише створити додатковий захист для об'єкта, а й автоматизувати деякі трудові процеси, наприклад, облік робочого часу персоналу.

Автоматизована система контролю доступу має відповідати певним параметрам [3]:

- наявність кабельної лінії, де встановлено всі необхідні сенсори;

- відкрита програмна платформа;

- легкість під час експлуатації, а також під час проведення ремонтних робіт;

- конкурентоспроможність серед заходів безпеки.

Автоматизований контроль доступу має модульний принцип роботи. Це значно спрощує процес впровадження, і навіть технічного супроводу, особливо за умови відкритості платформи.

При необхідності ремонтних робіт або впровадження додаткових функцій достатньо встановити ще один або кілька модулів та узгодити їх роботу між собою. Крім того, контроль доступу, організований за модульним принципом, складніше вивести з ладу. Така СКУД захищена від різних атак, поломок. За порушення роботи одного модуля, інші продовжують функціонувати.

1.2 Етапи проектування універсальних СКУД для багатофункціональних задач сьогодення

Під поняттям СКУД слід розуміти апаратно-програмний комплекс, пристрої якого мають перешкоджати несанкціонованому доступу на територію підприємства чи об’єкта, що охороняється (турнікетами, пропускними пристроями), фіксувати (камерами, сенсорами руху) та повідомляти (різними сигнальними системами), програмними засобами для роботи перерахованих пристроїв (драйверами) і взаємодії з користувачем (інтерфейсом, базою даних).

Основні функції систем контролю та управління доступом: санкціонування, ідентифікація, авторизація, автентифікація, дозвіл або відмова у доступі, реєстрація та реагування.

Важливим компонентом у роботі СКУД є можливість організації контрольно-пропускного режиму підприємства (КПР), в основі роботи якого лежить механізм «заборон» та «обмежень» по відношенню до осіб, які

потрапляють на територію організації [4]. Особливий контрольно-пропускний режим можна встановити як для всієї організації, так і для її окремих компонентів (приміщень). Це дозволяє призначити різним об'єктам (приміщенням) у межах одного підприємства різні рівні допуску.

Існування диференціації приміщень за рівнем закритості для відвідувачів різних категорій (рівнів допуску) є важливим аспектом при проектуванні СКУД в цілому та політики рівнів безпеки для різних користувачів (відвідувачів) зокрема. Незалежно від специфіки реалізації системи контролю та управління доступом на конкретному підприємстві, будь-яка СКУД складатиметься з наведених нижче компонентів (рисунок 1.5) [4, 5].

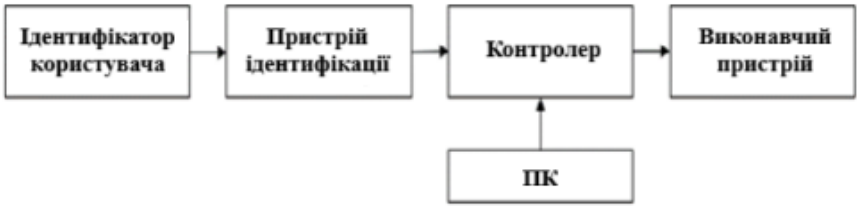


Рисунок 1.5 – Загальна схема СКУД

Ідентифікатор користувача – це пристрій або ознака, за якою можна провести однозначну ідентифікацію відвідувача. Ідентифікатори можна розділити на атрибутні та біометричні. Прикладами атрибутивних ідентифікаторів є електронні пропуски, токени, прикладами біометричних – обличчя, голос та інші біологічні атрибути користувача системи. Пристрій ідентифікації особи (зчитувач) – пристрій, який здійснює зчитування ідентифікатора користувача та передає отримані дані на контролер. Прикладами зчитувачів є кнопкова клавіатура для введення коду доступу, зчитувач карт, біометричний зчитувач.

Контролер обробляє інформацію від зчитувача ідентифікаторів та на основі отриманих даних керує виконавчим пристроєм (дозвіл або заборона на прохід через КПП). Виконавчий пристрій є механізм, який фізично обмежує доступ на територію об'єкту: турнікет, замок, автоматичні ворота. Відкриття

виконавчого пристрою здійснює контролер при отриманні коректного ідентифікатора особи користувача.

До описаної вище структури насамперед звертатися на початкових етапах проектування СКУД - на етапах визначення апаратної бази та вибору технологій проектування та розробки програмно-інформаційної підсистеми

Система, що розробляється, планується як біометрична СКУД, тому основними елементами виступлять такі компоненти [5]:

- ідентифікатор користувача – біометричні дані (особа відвідувача);

- пристрій ідентифікації – камера відеоспостереження, розміщена у приміщенні, або спеціальний біометричний сенсор на КПП;

- контролер - залежить від реалізованої в організації пропускної системи;

- виконавчий пристрій - турнікет на вході в офіс або цифровий замок на дверях приміщення.

Додатково у разі реалізації тільки підсистеми відеоспостереження з функцією ідентифікації відвідувачів на місці контролера та виконавчого пристрою перебуватиме клієнтська програма, що здійснює отримання даних з відеокамер, виконання ідентифікації та передачу інформації на інтерфейс користувача.

Система контролю віддаленого доступу із електромеханічними замками стала необхідною частиною будь-якої великої установи. Чим більше приміщень, тим більше ключів, які доводиться носити із собою або брати їх на вахті, що також витрачає додатковий час працівників. Сучасним варіантом вирішення проблеми є відкриття дверей за допомогою електронного ключа чи телефону.

На сьогоднішній день існують різні способи аутентифікації користувача в системах СКУД, а саме [6]:

- аутентифікація за парою логін/пароль – найпростіша аутентифікація для її реалізації треба лише перевірити пару логін/пароль на наявність у базі

даних користувачів, недоліком цього методу є необхідність знати пару логін та пароль;

- аутентифікація за технологією NFC (RFID) – перевагою даного способу аутентифікації є те, що користувачу не потрібно вводити будь-які дані, сам NFC-чіп містить всю необхідну інформацію для аутентифікації користувача, недоліком NFC буде необхідність наявності фізичного пристрою (NFC-чіпа) у користувача;

- автентифікація за ключами iButton – має всі ті ж переваги та недоліки, як і NFC, однак iButton має одну перевагу перед NFC - це більш проста і дешева реалізація як фізичного устрою, і протоколу передачі.

Згідно з викладеними вище способами аутентифікації та вимогами до системи, проектована система має реалізовувати такі функції:

- авторизація користувача через Wi-Fi-мережу;

- надання доступу до приміщення через NFC-ключ;

- надання доступу до приміщення через QR-код;

- реєстрація подій відкриття дверей приміщення за допомогою звичайного ключа;

- ведення журналу доступу користувачів до приміщення.

Згідно з функціональними вимогами, система повинна вміти автоматично авторизувати користувача в системі в тих випадках, коли він підключений до Wi-Fi-мережі організації, а також підтримувати відкриття дверей за NFC-міткою та QR-кодом з веденням журналу доступу.

Як приклад для найпростішого завдання - відкриття дверей за QR-кодом. Для його вирішення потрібно взяти до уваги, що є деяка система, яка вміє авторизувати користувача за логіном та паролем і надає веб-інтерфейс, в якому можна за натисканням кнопки відчинити двері. Тоді найпростішим рішенням цієї задачі буде зробити QR-коди зі посилання на кнопку відкриття дверей. Відразу ж варто відзначити, що якщо користувач не авторизований і не має прав, система повинна перенаправити на сторінку входу або повідомити про відсутність прав.

Наступним кроком стане створення концепції автоматичного входу користувача в систему у разі, якщо він зайшов у формі входу з Wi-Fi-мережі організації. Так як в організації використовується єдина точка входу для всіх клієнтів Wi-Fi-мережі та тип авторизації EAP, пропонується підключитися до шлюзу авторизації та при виявленні нового користувача в системі спробувати отримати інформацію про нього зі шлюзу авторизації Wi-Fi-мережі.

Як варіант можна розглянути спосіб відкриття дверей за допомогою сайту. Тут відразу ж варто відзначити, що сайт є єдиною точкою управління всіма дверима, до якого у невеликі інтервали часу буде звертатися велика кількість людей, і система має дати відповідь кожному користувачеві у прийнятний час. З іншого боку, необхідно керувати замком кожних дверей окремо, а на відкриття замка дверей йде деякий час. З цього випливає, що не можна керувати замком дверей безпосередньо із сайту.

Для вирішення цієї проблеми систему можна поділити на дві частини:

- веб-сайт, що відповідає за авторизацію, контроль доступу та ініціювання команд керування дверима;

- модуль управління замком дверей, що відповідає за виконання команди та виявлення подій відкриття дверей.

З цієї архітектури випливає, що необхідно зробити інтерфейс взаємодії двох частин системи. Оскільки запити на веб-сайт йдуть за протоколом HTTP, то краще і простіше всього реалізувати взаємодії між частинами системи через REST.

Наступним кроком буде вирішення задачі про відкриття дверей NFC-карткою. Оскільки пристрій для зчитування NFC-карти перебуватиме поруч із дверима, то логічніше взаємодіяти з ним через модуль керування замком. Другою проблемою NFC буде автентифікація картки в системі – за цю частину відповідає веб-сайт. З цього випливає, що необхідно врахувати можливість підтвердження картки через вебсайт.

Для взаємодії між системами варто використати REST. Тепер потрібно визначитися із системою команд та форматом обміну даними, для цього

потрібно визначити, якими даними необхідно обмінюватися двом частинам системи (у разі сервер – це вебсайт, а клієнт – модуль управління замком) [7]:

- команда на відкриття/закриття замка (від сервера до клієнта);
- команда на підтвердження доступу по карті (від клієнта до сервера);
- додавання видалення ключів;
- подія відкриття/закриття дверей (від клієнта до сервера);
- подія відкриття/закриття замку (від клієнта до сервера).

Таким чином, важливим етапом проектування будь-якої системи контролю та управління доступом є правильний вибір обладнання відповідно задачам та архітектурі системи. Для представленої автоматизованої системи основними апаратними компонентами будуть виступати камери відеоспостереження. Звідки виникає необхідність більш детального аналізу доступних на ринку камер та їх ключових характеристик. За способом передачі та обробки сигналу всі камери можна розділити на аналогові та цифрові. У аналогових камер зображення з камер передається в вигляді аналогового сигналу, який відцифровується для обробки, але для передачі знову перетворюється на вихідний аналоговий сигнал. У цифрових камерах передача та обробка сигналу відбувається повністю у цифровому форматі. При цьому сигнал може передаватися як у вихідному вигляді HDI-SD камери, так і стискатися і кодуватися для збільшення швидкості передачі даних (наприклад, IP-камери).

Важливою вимогою до камер, задіяних у системах відеоспостереження з реалізованою функцією розпізнавання осіб, є висока якість одержуваного зображення. Рекомендована якість відео в таких системах має бути не нижче 720 px. Основним недоліком аналогових камер та аналогової передачі сигналу є низька якість одержуваного зображення (особливо для старих моделей), тому в системах з розпізнаванням осіб найчастіше використовуються сучасні цифрові камери з високою якістю зображення.

Крім типу сигналу, що передається (аналоговий або цифровий) важливою характеристикою при виборі камер для систем

відеоспостереження з розпізнаванням осіб є кут огляду. Він визначається розміром матриці та фокусною відстанню.

Говорячи про фокусну відстань камери, в першу чергу мається на увазі задня фокусна відстань (f') – у першому наближенні його можна визначити, як відстань від поверхні останньої лінзи об'єктива камери до точки заднього фокусу. Від фокусної відстані обернено пропорційно залежить кут огляду камери, який розраховується за наступною формулою [8]:

$$\alpha = 2\text{arctg}(d/2f),$$

де α - кут огляду камери, d – розмір світлочутливості сенсора, f' – фокусна відстань.

За вище наведеною формулою, виходячи з характеристик конкретної камери та дистанцій виявлення і розпізнавання об'єкта для конкретного приміщення, можна підібрати потрібну камеру. На рисунку 1.6 представлена приблизна залежність кута огляду від фокусної відстані камери.

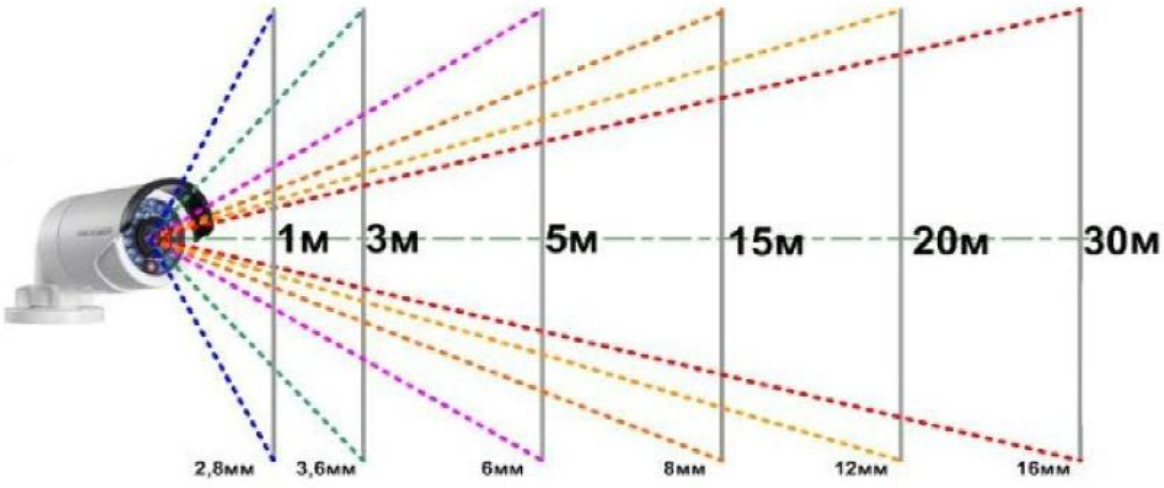


Рисунок 1.6 – Залежність кута огляду від фокусної відстані

Таким чином, вибір камер для проектованої системи буде залежати від їхнього розташування в приміщеннях. Для офісних приміщень буде достатньо камер з фокусною відстанню від 3,6 мм та кутом огляду 72 °. У разі розміщення камери на вулиці фокусне відстань буде відповідно більшою. Окремого дослідження в рамках розробки та оптимізації

алгоритму розпізнавання вимагатиме розмір зони розпізнавання для конкретних камер відеоспостереження.

В якості апаратно-програмного рішення розглядається розробка автоматизованої СКУД на основі системи відеоспостереження із вбудованою системою розпізнавання осіб.

Система, що розробляється як комплексне рішення повинна виконувати такі функції [9, 10]:

- детектування та розпізнавання співробітників та відвідувачів організації;

- швидке виявлення несанкціонованого доступу у приміщеннях організації;

- оповіщення про несанкціонований доступ;

- забезпечення можливості організації пропускного режим на основі біометрії;

- можливість створення системи допусків різного рівня таємності.

Відповідно до виділених функцій всю систему можна поділити на блоки (підсистеми). У майбутньому це дозволить найзручнішим способом описати роботу апаратно-програмного комплексу та алгоритму, що використовуються в ньому:

- підсистема відеоспостереження;

- підсистема зберігання даних;

- підсистема формування звітності;

- підсистема ідентифікації.

Конструктивно автоматизована система повинна складатися з підсистем відеоспостереження, зберігання даних, формування звітності та підсистеми ідентифікації. Таке розбиття на функціональні блоки допоможе на етапі проектування найбільш точно описати технічні та функціональні вимоги у вигляді технічного завдання.

Серед основних функцій, які виконуватиме система, можна виділити детектування та розпізнавання співробітників та відвідувачів організації,

швидке виявлення несанкціонованого доступу до приміщень та оповіщення про нього, забезпечення можливості організації пропускного режиму на основі біометрії та створення системи допусків різного рівня таємності.

1.3 Способи забезпечення інформаційної безпеки за допомогою комбінованих систем контролю і управління доступом

Проблема забезпечення інформаційної безпеки продовжує займати ключові місця в секторі інформаційних технологій на сьогоднішній день. Переважно цей фактор є наслідком повсюдної цифровізації сучасного суспільства, а також побутових та професійних сфер життєдіяльності людини. Саме недостатній рівень забезпечення інформаційної безпеки здатний призвести до колосальних втрат матеріального та економічного характеру.

Іншою причиною необхідності розвитку систем інформаційної безпеки та, зокрема, систем контролю та управління доступом є вдосконалення алгоритмів та махінацій кіберзлочинців.

Повсюдна цифровізація суспільства породжує різні кібератаки. Виходячи з цього, з метою забезпечення належного рівня роботи інформаційних систем на підприємствах потрібен повсюдний розвиток та підвищення рівня забезпечення інформаційної безпеки в спеціалізованих системах. Тому рішення проблеми необхідності розробки інтеграції інноваційних комбінованих СКУД є дуже актуальною задачею.

Системи контролю та управління доступом являють собою сукупність сумісних між собою засобів апаратного та програмного рівня. Кожен із цих інструментів спрямований з метою обмеження доступу людей, транспорту та інших об'єктів до тих чи інших приміщень або території. Саме за допомогою СКУД відбувається попередження несанкціонованого доступу до засекреченої, корпоративної чи іншої інформації на об'єкті.

Системи контролю та управління доступом мають достатньо примітивний вигляд, включаючи зчитувач, приймач, сервер та інше. На рисунку 1.7 представлена загально прийнята структура СКУД на підприємстві, яка основана на перепустках та турнікетах [10].

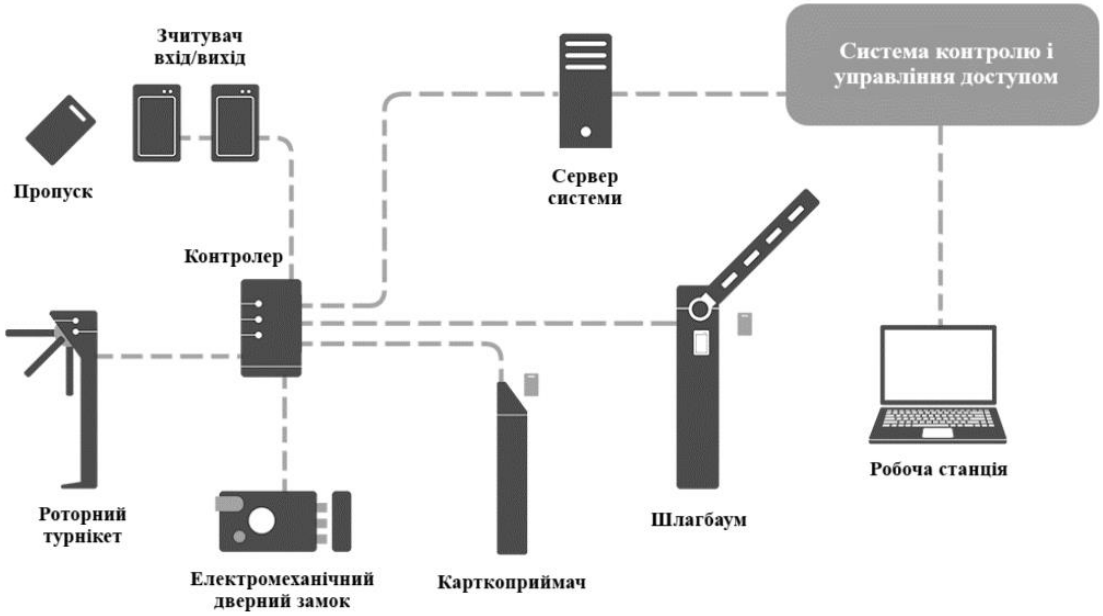


Рисунок 1.7 – Загальноприйнята структура СКУД

Сучасні СКУД старіють через інтенсивне поширення і покращення алгоритмів роботи хакерських атак на інформаційні системи підприємства. Таким чином, сучасні системи контролю та управління доступу необхідно негайно розвивати та вдосконалювати, інтегруючи інноваційні алгоритми та технології. Одним з найбільш актуальних та ефективних напрямків інноваційного розвитку СКУД є інтеграція інтелектуальних технологій, зокрема, засобів відеоспостереження з метою автоматичного виявлення несанкціонованого доступу. Це стало можливим завдяки розвитку фотокамер та перехід на цифрові апарати, що мають високу чіткість. Перспективні засоби відеоспостереження здатні в автоматичному режимі детектувати рух у зазначених областях кадру, а також виконувати багатокамерний супровід об'єкта, вимірюючи статистичні та біометричні ознаки людини.

Іншим перспективним рішенням для систем контролю та управління доступом є нанесення на документи RFID-ідентифікаторів. Активний

радіочастотний ідентифікатор, що є наклейкою, дозволить відстежувати місцезнаходження предметів та документів у реальному часі. Також є перспективним використання активних RFID-перепусток для безконтактної ідентифікації. Особлива перевага такої технології виявляється у аварійних ситуаціях в умовах вільного проходу. Коли зберігається можливість зареєструвати всіх осіб, покинули зону, що охороняється.

Необхідно підкреслити, що найперспективнішим варіантом розвитку СКУД є розробка комбінованих систем, що включають у собі безліч спеціалізованих програм та функцій і має найбільшу ефективність відмови від несанкціонованого доступу (рисунок 1.8).

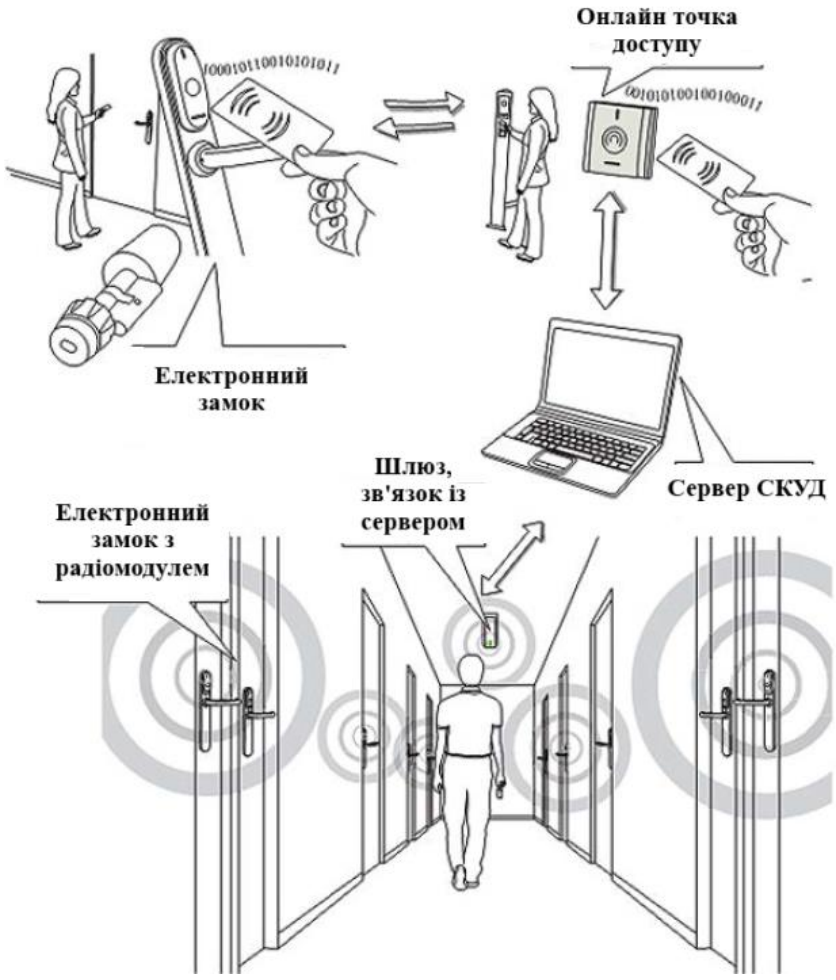


Рисунок 1.8 – Суть комбінованої СКУД

Розробники та виробники комбінованих засобів автентифікації представляють ринку інноваційні рішення, включаючи біометричні карти.

Основною перевагою даної технології є можливість не встановлювати біометричні зчитувачі, а використовувати встановлені зчитувачі смарт-карток. Таким чином, на біометричній карті знаходиться сканер відбитків пальців з 3D-технологій та RFID-чіп, за допомогою якого забезпечується підтримка популярних технологій за стандартом ISO 14443. Такий спосіб поновлення СКУД є дуже економним способом переходу зі застарілих технологій, які використовують проксіміті карти на біометричні технології.

У комбінованих системах контролю та управління доступом карта є не тільки носієм даних про доступ користувача, але використовується в ролі флешки, за допомогою якої база даних СКУД та точки доступу обмінюються інформацією в обох напрямках [11]. Для того, щоб цей обмін відбувався максимально оперативно та комфортно виробляється комбінація різних типів точок доступу в одній системі.

Основна відмінність онлайн-контролерів СКУД комбінованої системи від «звичайних» у тому, що вони тільки працюють у режимі реального часу, але також виконують роль проміжного шлюзу обміну даними між карткою та БД СКУД. У момент проходу через таку точку доступу карта «з'єднується» з БД СКУД і відбувається описаний вище двосторонній обмін даними.

Таким чином, основною метою є вивчення актуальності та перспективності використання комбінованих систем контролю та управління доступом для захисту інформації на підприємстві. Цифровізація суспільства ставить перед сучасним світом має величезну кількість завдань, пов'язаних забезпеченням інформаційну безпеку. Саме за рахунок належного рівня забезпечення інформаційної безпеки сучасні підприємства зможуть обмежити матеріальні та економічні втрати, а також раціоналізувати свою діяльність.

2. ОБҐРУНТУВАННЯ ВИБОРУ ОСНОВНИХ ЗАСОБІВ АВТОМАТИЗАЦІЇ ТА РОЗРОБКА КОМП'ЮТЕРНО-ІНТЕГРОВАНОЇ СИСТЕМИ

2.1 Визначення актуальних вимог та задач при проектуванні інтегрованих систем контролю і управління доступом закритих об'єктів

В даний час в організаціях, в яких необхідно контролювати та обмежувати доступ персоналу в різні приміщення або зони, що охороняються, знайшли широке застосування автоматизовані системи контролю та управління доступом. Ці системи здатні збирати, зберігати, аналізувати та розподіляти інформацію про функціонування всіх систем безпеки та життєзабезпечення організації.

Існує велика кількість різноманітних технологій ідентифікації, які використовують різноманітні фізичні принципи. Основними характеристиками, яких зазвичай керує замовник при виборі конкретної технології для своєї системи, продовжують залишатися: безпека, надійність, швидкість та зручність ідентифікації. Основним питанням при розробці структури системи контролю та керування доступом є оптимальне поєднання ключових характеристик. Одним з основних напрямків розвитку систем контролю та управління доступом є їх інтелектуалізація, передача максимально можливої кількості функцій зі збирання, обробки інформації та прийняття рішень програмно-апаратних комплексів.

Об'єкти закритого типу (ОЗТ) – це спеціальні об'єкти, де зберігається інформація, матеріали або ведуться роботи, що становлять державну таємницю, або об'єкти, для яких встановлено особливий режим відповідно до закону. До них належать військові частини, секретні виробництва, науково-дослідні інститути, об'єкти критичної інфраструктури та інші. Забезпечення безпеки таких об'єктів є пріоритетним завданням, а інтегровані СКУД виступають ключовим компонентом їх захисту. Актуальність проектування таких систем зумовлена посиленням кіберзагроз, ускладненням методів

несанкціонованого доступу та необхідністю дотримання суворих нормативних вимог. У другому розділі кваліфікаційної роботи розглядаються сучасні вимоги та завдання, що постають перед розробниками та проектувальниками СКУД для об'єктів закритого типу.

Головною особливістю ОЗТ є встановлений на них особливий правовий режим, який визначає комплекс обмежувальних, організаційних та технічних заходів. Ця специфіка формує низку унікальних вимог до СКУД такого типу.

Відповідність нормативним документам, тобто система повинна бути спроектована та експлуатуватися у повній відповідності до вимог державних стандартів, наказів та інструкцій (наприклад, ДСТУ, галузеві стандарти Міністерства оборони, Служби безпеки України тощо). Це стосується як апаратної частини (використання сертифікованого обладнання), так і програмного забезпечення (наявність необхідних ліцензій, відповідність вимогам щодо захисту інформації).

Багаторівневий захист (ешелонування), тобто доступ на об'єкт організовується за принципом "зони в зоні". Проектування передбачає створення декількох кордонів захисту, а саме [12]:

- зовнішній периметр - територія об'єкта, контрольована за допомогою турнікетів, шлагбаумів, КПП;

- будівля, вхід у будівлю;

- внутрішні зони - коридори, ліфти, сходові клітки;

- приміщення суворого режиму: секретні сховища, серверні кімнати, лабораторії, операційні.

Обов'язкова ідентифікація та верифікація тобто на ОЗТ застосовуються найбільш надійні методи перевірки особистості. Поруч із традиційними проксиміті-картами використовуються:

- біометричні технології - сканування відбитків пальців, геометрії обличчя, райдужної оболонки ока, вен долоні (це усуває ризик використання чужих або втрачених ідентифікаторів);

- мультифакторна аутентифікація тобто система орієнтована для доступу в критичні зони може знадобитися одночасне пред'явлення картки, сканування відбитка та введення PIN-коду.

Сучасна СКУД для ОЗТ – це не набір розрізнених пристроїв, а єдина інформаційно-керуюча система. Актуальні технічні вимоги включають інтеграцію в єдиний комплекс безпеки, СКУД не може функціонувати ізольовано, вона повинна бути тісно інтегрована з:

- системами відеоспостереження - подія в СКУД (наприклад, спроба несанкціонованого доступу) автоматично ініціює запис відео з найближчих камер, виведення картинки на монітори оператора та підсвічування зловмисника;

- охоронною сигналізацією - спроба відкриття дверей під час тієї години, коли приміщення зачинене, або несанкціоноване проникнення через вікно призводить до спрацьовування тривоги;

- системою пожежної сигналізації та оповіщення, у разі пожежі СКУД автоматично розблокує всі евакуаційні виходи за попередньо розробленими сценаріями, забезпечуючи безперешкодну евакуацію, але водночас фіксуючи події.

Висока доступність та відмовостійкість тобто будь-який простій системи неприйнятний, це досягається за рахунок:

- архітектури "клієнт-сервер" з резервуванням - дубльовані сервери баз даних, автоматичне перемикання при відмові основного сервер;

- автономності контролерів - мережеві контролери доступу повинні зберігати локальну базу користувачів і продовжувати функціонувати навіть при втраті зв'язку з центральним сервером;

- резервного живлення - система повинна коректно працювати протягом заданого часу при відключенні електромережі.

Захищеність від кіберзагроз, тобто сучасна СКУД – це мережева система, а тому вразлива до кібератак. Актуальні вимоги включають:

- шифрування каналів зв'язку між компонентами системи для запобігання перехоплення даних;

- регулярне оновлення ПЗ для усунення вразливостей;

- фізичний та програмний захист серверів від несанкціонованого доступу;

- мережеву сегментацію - відокремлення мережі СКУД від корпоративної мережі для зменшення поверхні атаки.

Масштабованість та гнучкість, тобто система повинна допускати легке розширення та модифікацію без значних переробок: додавання нових точок доступу, змін правил для користувачів, інтеграція з новими підсистемами.

Окрім технічних аспектів, система повинна ефективно вирішувати конкретні функціональні завдання, що є характериними для таких інтегрованих СКУД. Це деталізоване управління правами доступу (система має забезпечувати гнучке налаштування прав для кожного співробітника на основі його посади, допуску та необхідності знати/мати доступ. Реалізується це через рольову модель контролю доступу (можливість налаштування розкладу доступу (дні тижня, години роботи) для кожної зони).

Повний аудит та протоколювання, розуміє під собою фіксування кожної події в системі: успішні та неуспішні спроби проходу, зміни конфігурації, дії оператора. Журнали подій повинні бути захищені від редагування та забезпечувати неспростовність. На основі цих даних формуються звіти для керівництва та перевіряючих органів.

Реалізація правил "Anti-Passback", це правило забороняє повторний вхід на об'єкт або в зону без попереднього виходу. Воно запобігає передачі картки доступу однією особою іншій всередині зони.

Реагування на нештатні ситуації "тривожні" сценарії, при активації тривоги (напад, диверсія) система автоматично блокує або розблоковує певні групи дверей за попередньо підготовленими планами. Примусове закриття/відкриття, коли оператор має можливість дистанційно заблокувати або розблокувати будь-яку точку доступу.

Інтелектуальна аналітика - сучасні системи, які переходять від простого фіксування подій до їх аналізу. Функції аналітики можуть включати [13]:

- виявлення підозрілої активності (наприклад, спроби "підбору" карток);

- контроль тривалого перебування в приміщенні;

- сценарії "забутої відкритої двері".

Проектування СКУД для ОЗТ – це також організаційне завдання, що включає в себе ряд заходів, які повинні бути оговорені, проаналізовані і винесенні для ознайомлення:

- класифікацію та категоризація на етапі проектування необхідно провести детальну класифікацію всіх приміщень об'єкта за рівнем секретності та критичності, а також категоризацію всіх співробітників за рівнем допуску;

- розробка регламентуючих документів, система потребує супутніх документів: інструкція з експлуатації, регламент надання та анулювання прав доступу, план дій у надзвичайних ситуаціях;

- навчання персоналу, тобто адміністратори, оператори служби безпеки та звичайні користувачі повинні пройти належне навчання для ефективної та безпечної роботи з системою.

Проектування інтегрованих СКУД для об'єктів закритого типу – це комплексна та багатопланова задача, що поєднує в собі суворі нормативні вимоги, високі технічні стандарти та глибокі організаційні рішення. Актуальність полягає у створенні не просто системи контролю проходу, а інтелектуального, захищеного та відмовостійкого інформаційного середовища, яке є органічною частиною загального комплексу безпеки об'єкта. Сучасний підхід вимагає інтеграції, аналітики та проактивного захисту, що дозволяє не тільки фіксувати порушення, але й запобігати їм, забезпечуючи надійний захист інтересів національної безпеки.

2.2 Розробка структури та алгоритму роботи комп’ютерно-інтегрованої системи захисту об’єкта закритого типу

Для досягнення надійного та ефективного управління підприємством необхідна її часткова автоматизація, що стосується організації робіт з відповідними ресурсами (людськими, технічними, фінансовими), які забезпечують та поширюють інформацію. Відповідно до регламентних робіт автоматизація здійснюється шляхом впровадження комп'ютерних технологій, що дозволяють знизити трудомісткість дій, пов'язаних з обробкою даних, у тому числі шляхом створення певних шаблонів, а також підвищити оперативність виконання операторами типових задач. У даному розділі запропоновано варіант структури однієї з таких комп'ютерних технологій, а саме системи контролю та управлінь доступом.

Загалом у загальнодоступних літературних джерелах запропоновано кілька, хоч і не дуже розбіжних, визначень СКУД, а саме система, що включає у своїй сукупності програмно-апаратні засоби, тобто засоби контролю та управління доступом, які володіють сумісністю технічних, інформаційних, програмних та експлуатаційних функцій.

Нарівні зі СКУД порівнюються системи охорони та безпеки, для яких основні терміни та визначення введені в системи охорони периметру або системи охоронної сигналізації. На думку авторів, перші з вищезгаданих систем включають ширшу сферу діяльності, до якої можуть входити такі функції як стеження за обраним суб'єктом (об'єктом), аудит комп'ютерних систем та мереж, проведення організаційних заходів щодо безпеки об'єкта. Другі ж системи спрямовані на вирішення вузьких завдань, ніж завдання СКУД, а в деяких випадках такі системи можуть структурно входити до СКУД, особливо якщо йдеться про СКУД спеціального призначення.

Запропоновані етапи розробки загальної структурної схеми СКУД є наступні [14, 15]:

- формування загальних (відповідно до нормативної документації) та спеціалізованих (вимоги до функціональних характеристик засобів СКУД, що враховують специфіку організації) вимог до характеристик СКУД, що розробляється;

- аналіз елементів класифікації із вибором необхідних пунктів (тісно пов'язаний з першим етапом, але за належного підходу в результаті аналізу будуть отримані набагато конкретніші дані щодо майбутньої СКУД з можливим переглядом деяких із загальних вимог);

- розробка моделі СКУД за допомогою обраного математичного апарату;

- порівняльний аналіз готових апаратних або програмно-апаратних рішень, якщо готові рішення не задовольняють вимогам до СКУД або не відповідають умовам подальшої експлуатації необхідний порівняльний аналіз апаратного та програмно-апаратного забезпечення СКУД від різних виробників та у різних поєднаннях;

- розробка структури СКУД відповідно до вимог замовника та з урахуванням територіального рознесення підрозділів організації;

- розробка структури бази даних СКУД та її наповнення (у разі застосування готових рішень цей пункт замінюється лише на наповнення бази даних).

Одним із ключових моментів при вирішенні питань розробки СКУД є компроміс між рівнем контролю персоналу, зон доступу організації та фінансових, організаційних витрат на введення в дію, навчання персоналу, експлуатацію та підтримку у працездатному стані СКУД. Природним бажанням замовника є повний контроль суб'єктів та об'єктів організації, але, як правило, бажане поступається питанням фінансування та ступеню контролю знижується. Можливі і випадки доопрацювання СКУД у бік збільшення контролю як реакції на дії суб'єктів організації у спробі мінімізувати свої фінансові та організаційні втрати від введення СКУД за рахунок експлуатації засобів контролю, що з'явилися через зниження

фінансування на розробку та експлуатацію СКУД або через непродумані організаційні санкції начальників підрозділів.

Приналежність організації до державних чи великих корпорацій, які працюють за «плановим» принципом, накладає на розробку СКУД деяку кількість організаційних обмежень, таких як визначення необхідного складу СКУД (мінімального та максимального) необхідного за відомчим нормативним документам, обґрунтування та включення до плану на наступний календарний період (внесення змін до плану на поточний календарний період), організація та проведення тендеру на розробку СКУД тощо.

Загальні та спеціалізовані вимоги до СКУД, основні та додаткові ознаки класифікації СКУД визначені у відповідних положеннях. Для побудови загальної структури потрібно визначити всі точки доступу d системи контролю та управління доступом як множину D, в якій $d \in D$. Організація в загальному випадку складається з самостійних відділів (підрозділів) або вхідних до управління різною функціональною спрямованістю, що рознесені територіально. Залежно від цього доцільно розділяти сукупність точок доступу на підсистеми, а множина D на I підмножин D_i. У випадку, коли зона доступу є спільною для кількох підсистем підмножини можуть перетинатися або містити одна одну.

Розробку моделі СКУД можна здійснювати із застосуванням різних математичних апаратів. У даному підрозділі наведемо приклад моделі, отриманої з допомогою теорії графів. На рисунку 2.1 наведено план контрольованого об'єкта.

Вхід до зони доступу контролюється точкою доступу d_{18} (основний вхід) та d_9 (запасний вихід). Через основний вхід надається доступ до коридору К1, з якого можливі проходи в приміщення П7, П14 і коридор К2, що здійснюються під контролем точок доступу d_8, d_{16}, d_{17} і d_6 відповідно. Через запасний вихід надається доступ (у виняткових випадках, оскільки він для проходу закритий) у коридор К2, з якого можливі проходи до приміщень

П1-П6, П8, П9, П11, П12, що здійснюються під контролем точок доступу d_1-d_5, d_7 і d_{10}-d_{13} відповідно. З приміщення П8 надається доступ до приміщення П13 під контролем точки доступу d_{14}. З приміщення П9 надається доступ до приміщення П10 під контролем точки доступу d_{15} [16].

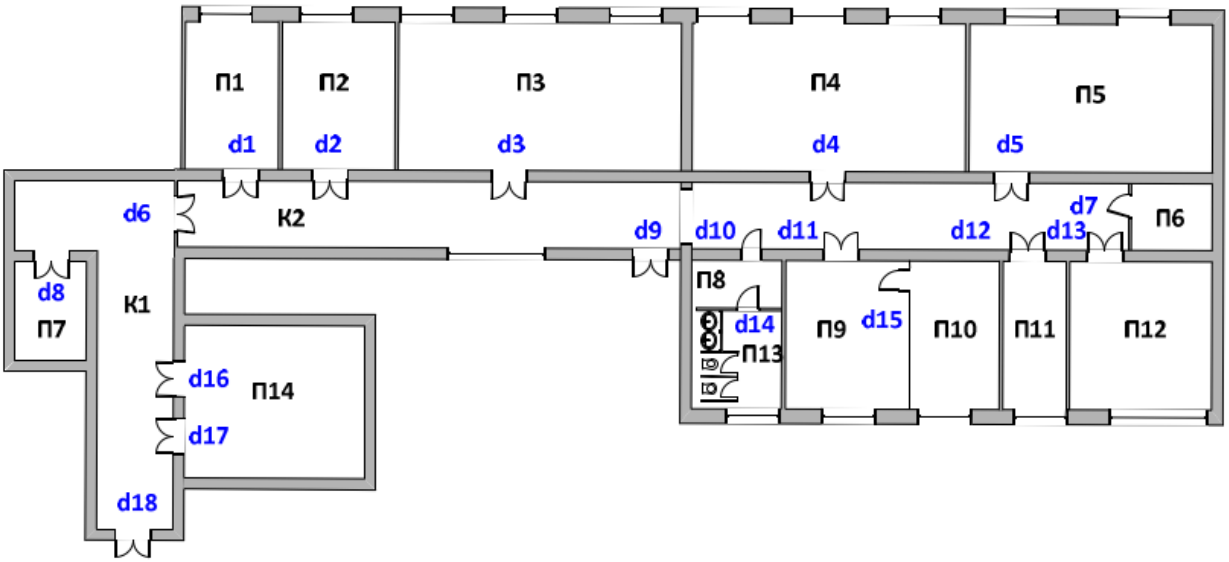


Рисунок 2.1 – План-схема контрольованого об’єкта закритого типу

Взаємозв'язок точок доступу може бути представлений графом, гілки якого визначають можливі шляхи переміщення суб'єктів через точки доступу (тобто можливі коректні маршрути проходження СКУД). На рисунку 2.2 представлений граф моделі запропонованої СКУД тобто об'єкта закритого типу, що визначає взаємозв'язок безлічі точок доступу. В об'єкті, що аналізується є п'ять підсистем контролю керування доступом (підмножин точок доступу). На графі лініями показано взаємозв'язок підмножин D_i (підсистем) безлічі точок доступу D запропонованої СКУД.

Перша підсистема D1 контролює коридор К1, точку доступу до коридору К2 та два приміщення – П7 і П14. Друга підсистема D2 контролює точку доступу в коридор К1 як необхідну умову доступу в коридор К2 і всі приміщення, до яких здійснюється доступ із нього. Третя підсистема D3 контролює доступ лише до приміщенням із коридору К2. Четверта та п'ята підсистеми D4 та D5 контролюють суміжні приміщення з П8 П13 і з П9 П10

відповідно. У розглянутому прикладі дві підмножини D1 і D2 перетинаються, D4 і D5 містяться в третьому, а D3 - другому. Перетин першої D1 та другої D2 підмножин визначає головний вхід як загальну точку доступу d_{18}.

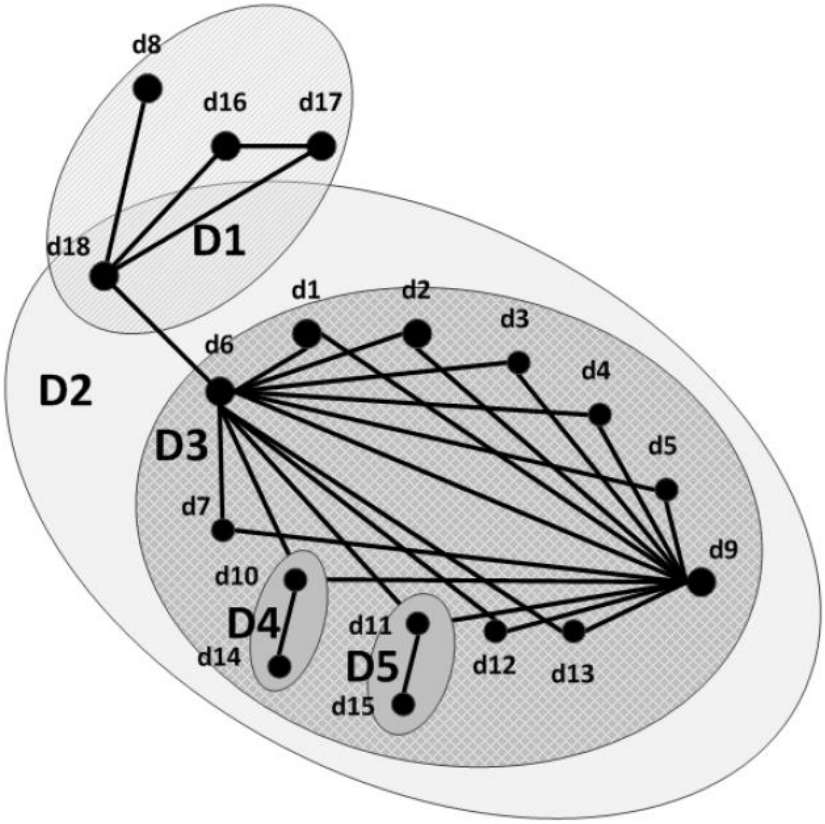


Рисунок 2.2 – Граф взаємозв’язку точок доступу

На рисунку 2.3 представлена структура системи контролю та управління доступом об’єкта закритого типу у загальному вигляді. Користувач за допомогою ідентифікатора (може бути простим або комплексним, наприклад, пристрій радіочастотної ідентифікації суміщений з біометрією користувача) здійснює спробу аутентифікації у точці доступу.

Зчитуючий пристрій передає дані з аутентифікації користувача у контролер СКУД, який може самостійно прийняти рішення про допуск користувача, або запитує через локальну обчислювальну мережу (доцільно використовувати закритий від загальної мережі сегмент) відповідну базу даних через програмно-апаратний комплекс СКУД, після чого при

позитивному рішенні здійснює авторизацію користувача та подає сигнал на виконавчий пристрій, який розблокує перегороджувальний керований засіб.

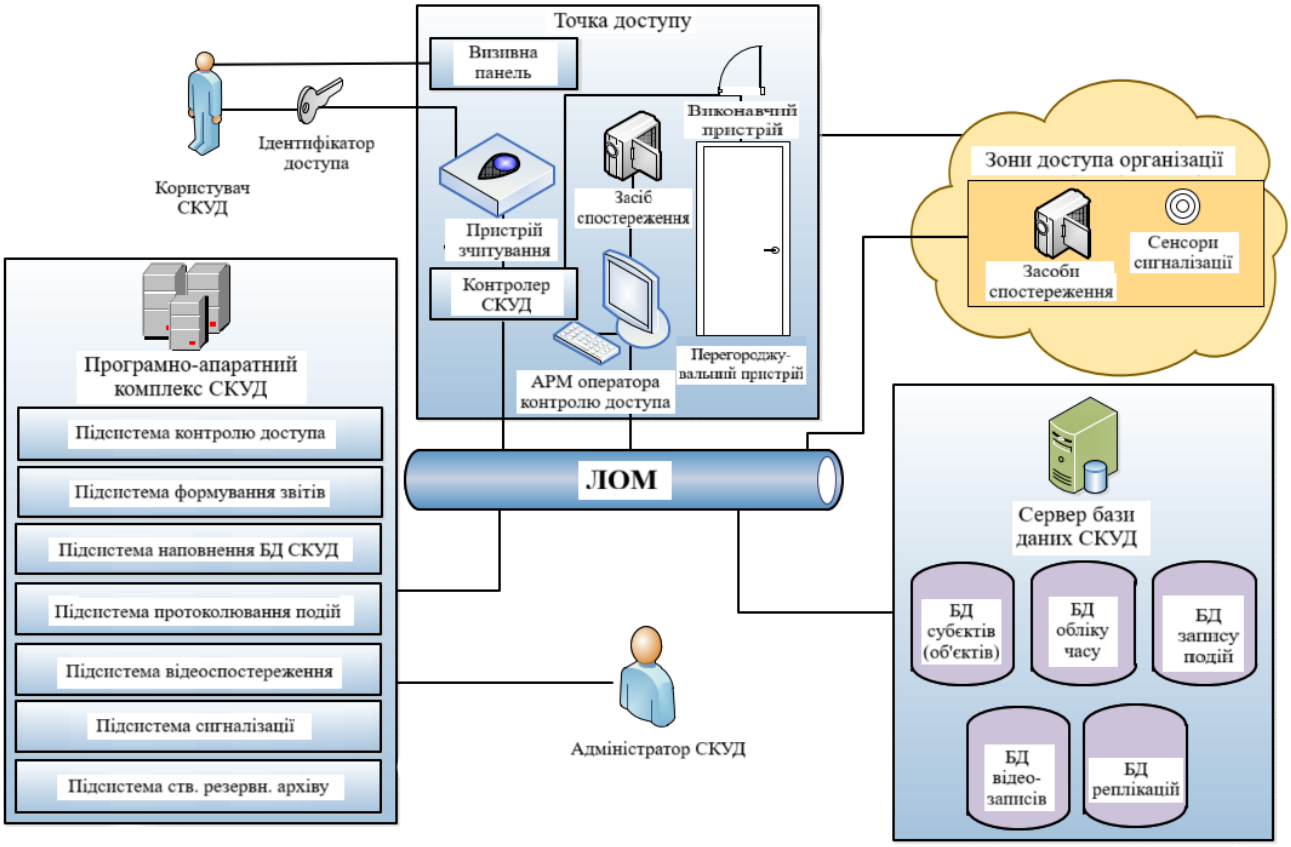


Рисунок 2.3 – Загальна структура запропонованої СКУД

Програмно-апаратний комплекс може включати ряд підсистем, що взаємодіють з відповідними базами даних, що зберігаються на сервері, і засобами спостереження та сигналізації [17]. Наявність сигналізації (пожежної або охоронної) передбачає попередню організаційну роботу з певними охоронними організаціями. Перелік підсистем має рекомендаційний характер і визначається відповідно до вимог та можливостей замовника, але підсистема створення резервну копію, особливо в частині обліку робочого часу, є якщо не обов'язковою, то вкрай рекомендованою для реалізації (термін зберігання подібної інформації визначається в організаційних документах). Управління та налаштування програмно-апаратного комплексу, а також через нього сервера бази даних СКУД, здійснює адміністратор. База даних системи контролю та управління доступом можуть складатися з різних

підсистем, частина з яких повинна бути доступна тільки групі адміністраторів СКУД. Також має бути організаційно визначено порядок подання до відділу (відділення) кадрів та бухгалтерії (фінансового відділу) даних про облік робочого часу.

Заключним етапом є розробка (наповнення) бази даних СКУД. Прикладом логічної моделі представленої бази даних є рисунок 2.4. У даної моделі передбачається мережевий варіант СКУД з можливістю редагування даних по користувачеві (особисті дані, включаючи фото (необхідна при реалізації СКУД у варіанті комплектації на точці доступу АРМ оператора, або у варіанті автоматичного розпізнавання осіб), регламент робочого часу, посада, підрозділ), розклад роботи точок доступу СКУД, дозвіл для користувачів проходу через певні точки доступу та формування звітів [18].

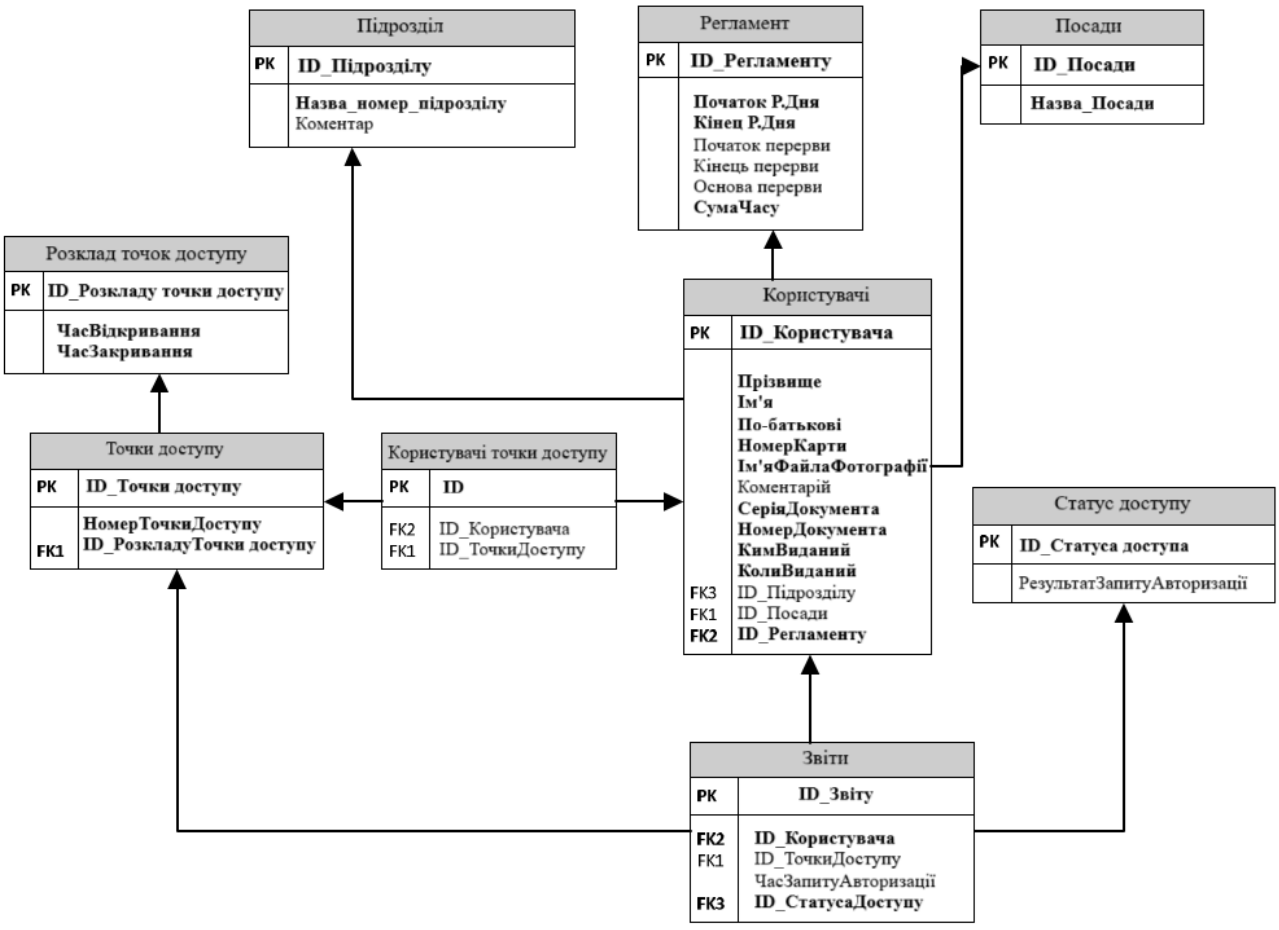


Рисунок 2.4 – Логічна модель бази даних запропонованої СКУД

Таким чином, розроблено структуру системи контролю та управління доступом у загальному вигляді, а також представлено загальні поняття в галузі контролю та управління доступом, запропоновано варіанти моделі СКУД та логічної моделі її бази даних.

2.3 Обґрунтування вибору засобів автоматизації запропонованої структури СКУД

Сучасна автоматизована система контролю та управління доступом є складним технічним комплексом, ефективність якого безпосередньо залежить від коректного вибору засобів автоматизації. Вибір компонентів має ґрунтуватися на комплексному аналізі технічних вимог, економічної доцільності та перспектив розвитку системи. У даній роботі обґрунтовується вибір основних засобів автоматизації для розробки АСКУД, враховуючи сучасні тенденції та вимоги до систем безпеки.

Об'єкти закритого типу характеризуються підвищеними вимогами до безпеки, надійності та захищеності систем керування. Вибір ПЛК для таких об'єктів ґрунтується на наступних ключових вимогах, а саме [19, 20]:

1. Вимоги безпеки та захищеності:
- відповідність стандартам кібербезпеки (IEC 62443);
- фізичний захист від несанкціонованого доступу;
- шифрування даних та комунікацій;
- можливість створення ізольованих сегментів мережі.

2. Вимоги надійності:
- робота в безперервному режимі 24/7;
- ступінь захисту оболонки не нижче IP54;
- діапазон робочих температур -40...+70°C;
- стійкість до електромагнітних перешкод.

До основних критеріїв вибору ПЛК по технічних характеристиках можна віднести: продуктивність, швидкість виконання команд та інструкцій, обсяг пам'яті програми, кількість підключених пристроїв, час реакції на події. Комунікаційні можливості ПЛК високої надійності включають: підтримку інтерфейсів PROFINET, PROFIBUS DP; вбудовані Ethernet порти (2+ для резервування); підтримка OPC UA для інтеграції з SCADA; можливість створення VPN-з'єднань. А також основні функціональні можливості включають: роботу в автономному режимі (зберігання локальної бази користувачів, функціонування при втраті зв'язку з сервером, автоматичне відновлення після збоїв); безпекові функції (апаратне шифрування даних, підтримка цифрових підписів, вбудовані фаєрволи, можливість створення додаткових рівнів аутентифікації). ПЛК якому відповідають усі вище перераховані параметри є Siemens SIMATIC S7-1500, загальний вигляд якого представлений на рисунку 2.5 [21].

Рисунок 2.5 – Загальний вигляд ПЛК Siemens SIMATIC S7-1500

Вибір технологій ідентифікації для СКУД об’єкта закритого типу базується на аналізі рівня безпеки та економічної ефективності:

- RFID технології **(**частота 125 кГц - для зон з помірними вимогами безпеки, частота 13.56 МГц - для зон підвищеної безпеки з підтримкою шифрування);

- біометричні системи **(с**канери відбитків пальців для критичних зон, системи розпізнавання обличчя - для КПП та зон високої прохідності);

- комбіновані рішення **(**використання двофакторної аутентифікації (карта + PIN-код) для особливо важливих об'єктів).

критерії вибору системи ідентифікації

До основних критеріїв вибору систем ідентифікації є [22]:

- безпека (захист від підробки, наявність криптографічних алгоритмів, унікальність ідентифікаторів, можливість відстеження спроб обману);

- **с**тійкість до злому (апаратне шифрування даних, захист від стороннього аналізу, можливість негайного блокування);

- продуктивність (час ідентифікації - ≤ 1 сек, ємність бази шаблонів - ≥ 10 000 записів, швидкість обробки - ≥ 50 ідент./хв.);

- надійність (робота в температурному діапазоні -30...+60°C, ступінь захисту IP67 для зовнішнього встановлення, середній час наробки на відмову ≥ 100 000 годин).

Вибір комбінованої системи ідентифікації на основі HF RFID та біометричних технологій для СКУД об'єкта закритого типу є оптимальним рішенням, що ґрунтується на:

- відповідності вимогам безпеки - забезпечення неспростовності та захисту від підробки;

- гнучкості застосування - можливість адаптації до різних зон контролю;

- масштабованості - поступове впровадження та розширення;

- економічній ефективності - оптимальне співвідношення вартості та рівня безпеки;

- перспективах розвитку - можливість інтеграції з новими технологіями.

Запропонована система забезпечує комплексний підхід до ідентифікації, враховує специфіку об'єкта закритого типу та відповідає сучасним вимогам до безпеки і надійності. Перелік технічних засобів ідентифікації, що використовуються на сучасних СКУД представлено на рисунку 2.7.

а) б) в)

г) д)

Рисунок 2.6 – Технічні засоби ідентифікації для СКУД: а) – біометричні сканери, б) – зчитувачі Proximity карт, в) – зчитувачі RFID міток, г) – термінали розпізнавання обличчя, д) – зчитувачі з NFC модулем.

Рекомендована конфігурація апаратних засобів ідентифікації включає ряд параметрів характерних для об’єктів закритого типу чи об’єктів з підвищеною захищеністю. До апаратних компонентів відносять [23]:

- зчитувачі RFID (Legic advant з підтримкою AES-256, дальність зчитування 5-15 см, антивандальне виконання);

- біометричні сканери (Suprema BioMini 4 з антиспуфінговим захистом, ZKTeco K60 з підтримкою розпізнавання обличчя, HID Signo з комбінованою аутентифікацією);

- програмне забезпечення платформа управління (єдині бази даних користувачів, централізоване ведення журналів подій, інструменти аналітики та звітності);

- модулі безпеки (керування криптографічними ключами, моніторинг спроб несанкціонованого доступу, автоматичне оновлення прошивок).

Перегороджувальні засоби - це фізичні пристрої та конструкції, що створюють матеріальні бар'єри для обмеження та контролю переміщення людей і транспорту на об'єкті. Основні типи перегороджувальних засобів сьогодні на ринку автоматизації представлені широким спектром технічних засобів, а саме:

- дверні системи (стандартні вхідні двері з контролем доступу, протиударні та противозламні двері, обертові двері з інтегрованим контролем, автоматичні розсувні двері);

- турнікетні системи (трипільні турнікети - найпоширеніший тип, роторні турнікети - з обертовими бар'єрами, Full-height турнікети - повновисотні з максимальним захистом, оптичні турнікети - віртуальні бар'єри з інфрачервоними сенсорами);

- бар'єрні системи (шлагбауми - для контролю транспорту, шлюзові кабіни - системи подвійних дверей, підйомні стовпчики - для блокування проїзду, поворотні механізми - для обмеження проїзду).

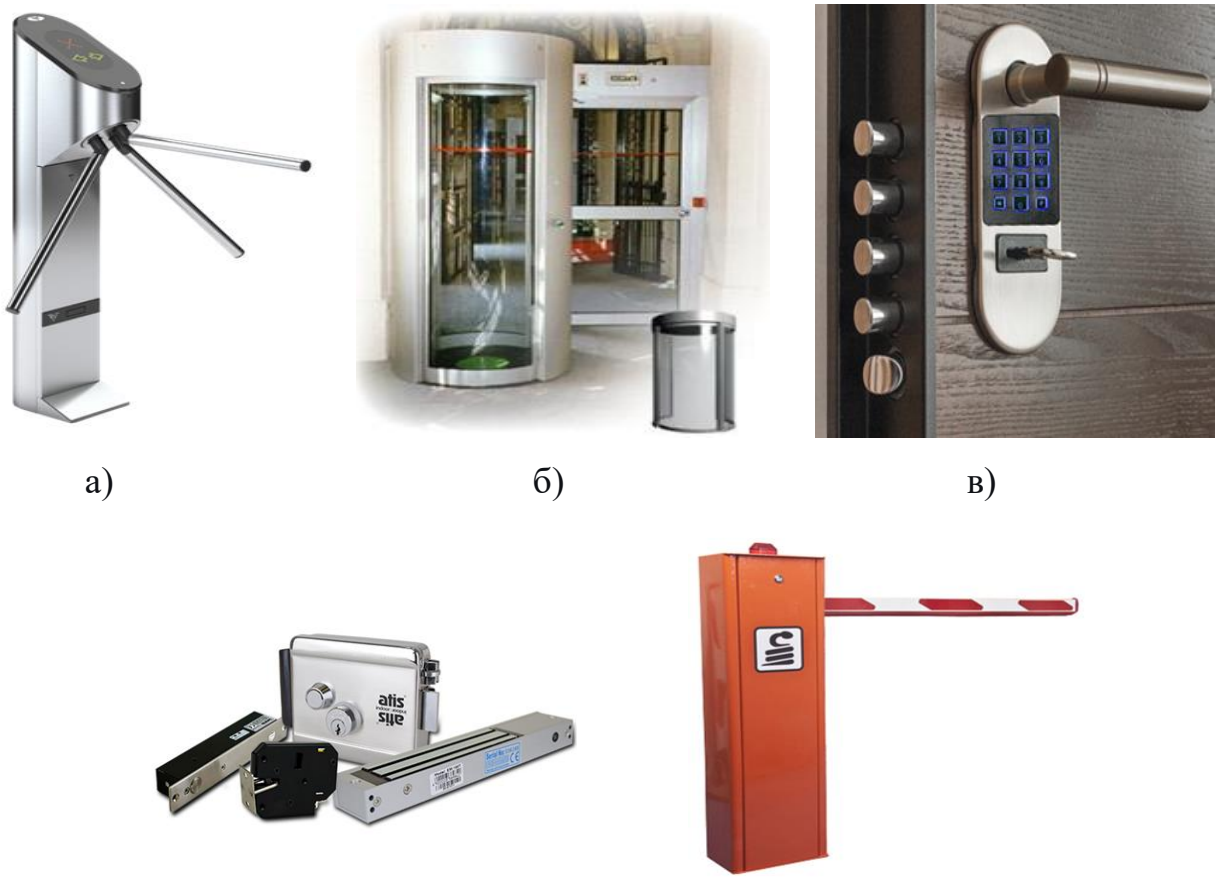
Виконавчі механізми - це пристрої, що безпосередньо реалізують команди системи контролю доступу, забезпечуючи фізичне блокування або розблокування перегороджувальних засобів. Основні типи виконавчих механізмів на ринку автоматизованих засобів представлені наступним чином:

- електромеханічні замки (моторні замки - з електродвигуном для керування, засувні замки - з електромагнітним керуванням, електрорігельні замки - з електричним керуванням ригелем);

- електромагнітні замки (замки зсуву - утримують двері за рахунок магнітного поля, врізні електромагнітні замки - встановлюються в торці двері, замки електромеханічні циліндрові, замки з електричним керуванням циліндром, можливість дистанційного керування);

- дверні закривачі (електромеханічні закривачі з функцією блокування, регульована швидкість закриття дверей).

Керувати та контролювати доступ на об'єкт неможливо лише за допомогою навіть найсучасніших сенсорів та систем контролю. Необхідне обладнання, яке здатне забезпечити або заборонити вільний прохід відповідно до заданого алгоритму представлене широким спектром на світовому ринку засобів автоматизації (рисунок 2.7) [24].



а) б) в)

г) д)

Рисунок 2.7 – Загальний вигляд ряду перегороджувальних пристроїв та втконавчих механізмів СКУД: а) – турнікет, б) – шлюзовий перепускний пристрій, в) – електромеханічний замок, г) електромагнітний виконавчий пристрій, д) – шланкбаун.

Перегороджувальні засоби та виконавчі механізми є фізичною основою будь-якої системи контролю доступу, що забезпечує:

- фізичне обмеження доступу в контрольовані зони;
- примусове виконання рішень системи контролю;
- захист від несанкціонованого проникнення;
- організацію потоків людей і транспорту;
- інтеграцію з іншими системами безпеки.

Правильний вибір цих компонентів визначає ефективність всієї системи контролю та управління доступом і забезпечує необхідний рівень безпеки об'єкта.

Системи безперебійного живлення для СКУД повинні забезпечувати (рисунок 8):

- надійність - безперебійну роботу всіх компонентів;
- стабільність - якісне живлення без перепадів;
- достатній час автономії - для завершення критичних операцій;
- моніторинг - контроль стану системи живлення;
- масштабованість - можливість розширення системи.

Рисунок 2.8 – Загальний вигляд безперебійної системи живлення СКУД

Правильний вибір та налаштування системи живлення є критично важливим для забезпечення безперебійної та безпечної роботи всієї СКУД.

Додаткове обладнання СКУД є критично важливим для:

- забезпечення надійності - системи живлення та резервування

- розширення функціоналу - додаткові модулі та інтерфейси;

- підвищення безпеки - системи моніторингу та захисту;

- спрощення експлуатації - інструменти діагностики та обслуговування;

- забезпечення інтеграції - комунікаційне обладнання та шлюзи.

Правильний вибір додаткового обладнання дозволяє створити повноцінну, надійну та ефективну систему контролю доступу, що відповідає конкретним вимогам об'єкта та забезпечує довготривалу стабільну роботу.

3. РОЗРОБКА МЕТОДУ АСОЦІАТИВНОГО НАВЧАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ФУНКЦІОНУВАННЯ МОЖЛИВОСТЕЙ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ

3.1 Коригування ієрархічних структур, об'єктів систем безпеки методами нейронних мереж

Одним із найефективніших методів порівняльної оцінки технічних та економічних об'єктів є метод аналізу ієрархій (МАІ). Метод набув широкого поширення, сучасні модифікації дозволяють враховувати залежності між об'єктами, зворотні зв'язки, додаткові елементи теорії нечітких множин. Однак численні розрахунки показують, що традиційне застосування МАІ призводить до невиправданого заниження оцінок менш значних об'єктів експертизи. Тому завдання розробки методики використання МАІ з корекцією отриманих результатів порівняльної оцінки видається дуже актуальним.

У третьому розділі кваліфікаційної роботи проводиться порівняльна оцінка кількох варіантів структури інтегрованої системи безпеки (ІСБ) із різними функціональними можливостями методом МАІ. Для корекції отриманих результатів пропонується використання асоціативного методу навчання нейронної мережі.

Коригування ієрархії об'єктів відбувається методами нейронних мереж. Щодо поставлених задач на першому етапі розглядається структура ІСБ і формуються попередні дані про ступінь відносної важливості різних функцій та підсистем ІСБ. Такі дані можуть бути отримані, для прикладу, з літературних, електронних джерел або наближеними числовими методами. Зокрема, у даному розділі використовуються оцінки, отримані з достовірних джерел, науково-дослідних робіт.

Наступним етапом є безпосереднє застосування методу МАІ. Потрібно сформувати матрицю парних порівнянь W згідно з зазначеними правилами,

що складається з елементів w_{ij} відносної переваги і-го об'єкта (у даному випадку - функціональних можливостей) перед j-м об'єктом [24, 25]:

$$W = \begin{pmatrix} 1 & w_{12} & \ldots\ldots & w_{1k} \\ 1/w_{12} & 1 & \ldots\ldots & w_{2k} \\ \ldots & \ldots & \ldots\ldots & \ldots \\ 1/w_{1k} & w_{k2} & & 1 \end{pmatrix}.$$

Така матриця називається зворотно-симетричною, а елементи її першого рядка (ранги) визначаються експертами згідно з лінгвістичною шкалою за принципом: еквівалентно - 1; слабо переважно - 3; трохи переважно - 5 і так далі. Елементи інших рядків також вибираються згідно згаданої лінгвістичної шкалою. Для визначення вектора коефіцієнтів відносної важливості (вектор пріоритетів) об'єктів вирішується рівняння

$$WV = \lambda V, \tag{1}$$

де V - матриця, першим стовпцем якої є вектор пріоритетів; λ — вектор власних чисел.

Інформативним критерієм достовірності визначення рангів є індекс узгодженості (ІУ) матриці парних порівнянь W , який дає інформацію про ступеня порушення узгодженості. Індекс узгодженості розраховується на основі оцінки максимальної величини власного значення матриці за формулою:

$$\text{ІУ} = \frac{\lambda_{max} - m}{m - 1}, \tag{1.1}$$

де m - розмірність матриці парних порівнянь.

Для обернено-симетричної матриці завжди $\lambda_{max} \geq m$. Матриця W вважається добре узгодженою, якщо ІУ<0,1. В результаті рішення рівняння (1) обчислюється вектор пріоритетів

$$V = (V_1, V_2, \ldots, V_m)^T,$$

проте одержане методом МАІ чисельне рішення має серйозний недолік, як правило, менш значущим досліджуваним об'єктам надаються свідомо занижені вагові коефіцієнти V_i.

На третьому етапі для корекції значень коефіцієнтів V_i використано імовірнісну модель асоціативного навчання нейронної мережі. Відомо, що спільне дослідження кількох однорідних об'єктів призводить до математичної моделі лінійної множинної регресії. Розглянувши завдання регресії, у якій вектор-регресор x породжує відгук, що позначається випадковою змінною Z з реалізацією z. Припустимо, що генерація відгуку z визначається імовірнісною моделлю. Представлена наступна конфігурація нейронної мережі, що представлена на рисунку 3.1 і називається моделлю змішування думок експертів і складається К нейронних мереж (модулів), які навчаються з учителем і називають мережами експертів, або просто експертами. Інтегруючий елемент називається "мережа шлюзу". Передбачається, що різні експерти найкраще працюють у своїх галузях вхідного простору згідно ймовірнісної породжувальної моделі безлічі вхідних даних [25].

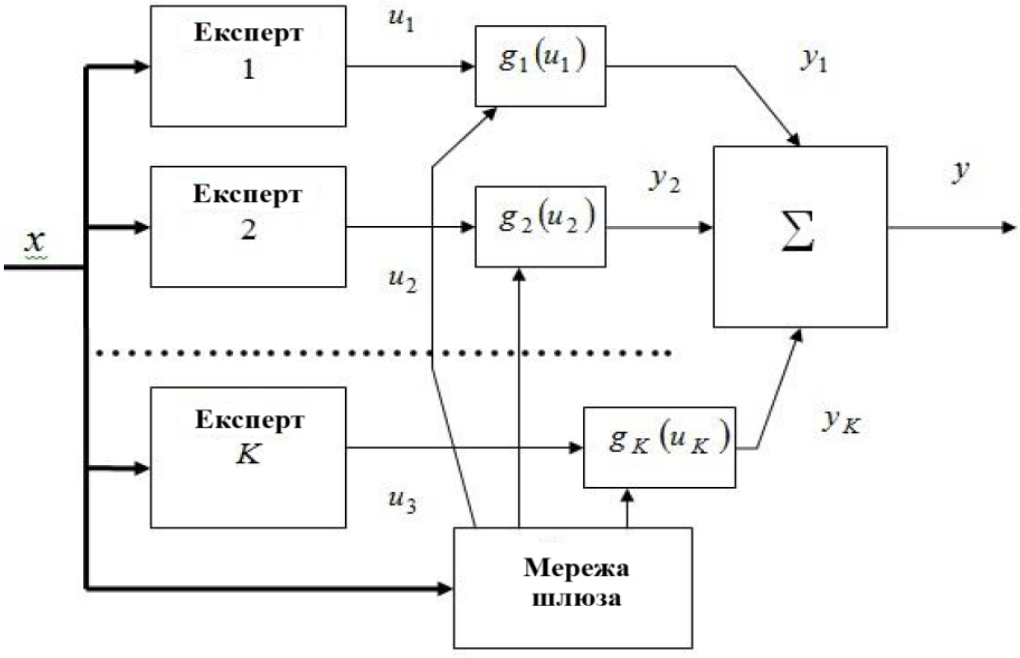


Рисунок 3.1 - Модель змішування оцінок експертів

Кожна з мереж експертів є лінійним фільтром. Таким чином, вихідний сигнал, створений експертом k, є скалярною похідною вхідного вектора x та вектора синаптичних вагів w_k даного нейрона:

$$u_k = w_k^T x, \qquad k = 1,2,\ldots,K. \tag{2}$$

Мережа шлюза містить один шар з нейронів, кожен з яких відповідає одному з експертів. На відміну від експертів, нейрони мережі шлюзу є нелінійними, їх функції активації мають такий вигляд:

$$g(k) = \frac{exp(u_k)}{\sum_{j=1}^{K} exp(u_j)}, \qquad k = 1,2,\ldots,K, \tag{3}$$

де u_k - скалярні похідні (2).

Нормоване перетворення (2) є узагальненням логістичної функції активації для кількох входів. У ній реалізовано узагальнення операції «переможець отримує все», що отримує максимальне значення. Тому функція активації виду (3) називається softmax. Очевидно, що лінійна залежність від вхідного вектора x приводить до нелінійної залежності вихідного значення мережі шлюза від x.

Для імовірнісної інтерпретації ролі мережі шлюза вважається «класифікатором», який відображає вхідний вектор x значення мультиноміальної ймовірності так, щоб різні експерти могли зробити внесок у бажаний відгук. Використання функції активації softmax у мережі шлюза гарантує, що ці ймовірності будуть задовольняти такі умови [26]:

$$0 \le g(k) \le 1, \quad \forall k; \qquad \sum_{k=1}^{K} g(k) = 1.$$

Нехай u_k — вихідний сигнал експерта, тоді загальний вихід буде рівний:

$$y = \sum_{k=1}^{K} g_k(u_k),$$

де g_k - нелінійна функція x.

Припускаючи, що обрано правило k імовірнісної моделі, вихід експерта u_k можна розглядати як умовне середнє значення змінної Z породжуючої моделі:

$$M[Z|x,k]=u_k=w_k^T x,\quad k=1,2,\ldots,K.$$

Позначаючи символом μ_k умовне середнє значення змінної Z, запишемо: $\mu_k=u_k$, k=1,2,...,K. Дисперсія змінної збігається з дисперсією помилки e_k. Тоді приходимо до співвідношення:

$$D[Z|x,k]=1,\quad k=1,2,\ldots,K.$$

Функція щільності розподілу ймовірностей змінної Z з урахуванням припущення про те, що обрано k-е правило ймовірнісної моделі, що породжує (тобто експерт k), може бути записана у такому вигляді [27]:

$$f_Z(z|x,k,\theta)=\frac{1}{\sqrt{2\pi}}exp\left[-\frac{1}{2}(z-u_k)^2\right],$$

де θ - вектор, що поєднує параметри мережі шлюза та параметри експертів моделі. Функція густини ймовірності змінної Z є сумішшю функцій густини ймовірності:

$$\{f_Z(z|x,k,\theta)\}_{k=1}^K,$$

де змішані параметри θ визначаються мережею шлюза. Тому

$$f_Z(z|x,\theta)=\sum_{k=1}^K g_K f_Z(z|x,k,\theta)=\frac{1}{\sqrt{2\pi}}\sum_{k=1}^K g_k\, exp\left[-\tfrac{1}{2}(z-u_k)^2\right]. \qquad (4)$$

Розподіл ймовірності (4) називається асоціативною гаусовою моделлю змішування і є узагальненням звичайної гаусової моделі змішування. Розглянута вище послідовність дій є реалізацією методу занурення чиселової задачі в експертну оболонку у класі DMS (Data Mining System).

3.2 Спосіб формування вихідних даних щодо пріоритетності функцій ІСБ.

З огляду на функціональність ІСБ, тобто реалізацію не однієї, а кількох вихідних функцій: виявлення, оповіщення, управління, контролю та управління доступом, відеоконтролю, протиаварійного захисту та інших,

необхідно будувати моделі та аналізувати надійність ІСБ за кожною функцією окремо, а також різним спільним комбінаціям.

Так як структури ІСБ можуть змінюватися як за складом елементів, так і цілих підсистем, було зроблено функціонально-структурну декомпозицію та розроблено універсальну структурну схему ІСБ у мінімальній конфігурації, яку можна використовувати для формалізованої постановки завдання моделювання та оцінки надійності.

Опис основних функцій f_1 - f універсальної структурної схеми ІСБ в мінімальній конфігурації, отриманої в результаті функціонально-структурної декомпозиції, представлено у таблиці 3.1 [28].

Таблиця 3.1 - Основні функції універсальної структурної схеми ІСБ у мінімальній конфігурації

Функція – позначення і найменування		Номер і найменування підсистеми	
f_1	Функція контролю та управління СОТС, а також гарантованої передачі на верхній рівень ієрархії	1	Система охоронно-тривожної сигналізації (СОТС)
f_2	Функція контролю та управління СПС, а також гарантованої передачі на верхній рівень ієрархії	2	Система пожежної сигналізації (СПС)
f_3	Функція контролю та керування доступом, а також гарантованої передачі інформації на верхній рівень ієрархії	3	Система контролю та управління доступом (СКУД)
f_4	Функція відеоконтролю та спостереження, а також гарантованої передачі відеосигналу на верхній рівень ієрархії	4	Система охоронна телевізійна (СОТ)
f_5	Функція управління життєзабезпеченням, а також гарантована передача інформації на верхній рівень ієрархії	5	Система управління життєзабезпечення (СУЖ)
f_6	Функція передачі інформації між підсистемами в ІСБ, у тому числі перетворення інтерфейсів	6	Мережа передачі даних (СПД) чи локальний контролер ІСБ

f_7	Функція сервера ІСБ (інтеграції, контролю та управління підсистемами безпеки, обробки, зберігання та надання інформації про безпеку об'єкта у заданому вигляді)	7	Система збору та обробки інформації (СЗОІ)
f_8	Функція готовності ІСБ до виконання цільової функції з антитерористичної та антикримінальний захист об'єктів (визначається коефіцієнтом готовності для повністю відновлюваних ІСБ або ймовірністю готовності для змішаних)	8	ІСБ і цілому

Сучасні ІСБ залежно від структури можуть бути як системами одного типу структурно-складних технічних систем (ССТС), коли всі вихідні функції характеризуються лише двома рівнями станів - повної працездатності, безпеки або повної відмови, аварії, та системами 2-го типу ССТС (якісно складними). У якісно-складних ІСБ є вихідні функції, що характеризуються (крім зазначених двох станів) ще деяким числом станів часткової відмови або часткової працездатності, в яких цілі роботи системи реалізуються з різним ступенем ефективності чи ризику функціонування.

У зв'язку з цим розглянуто 8 структур ІСБ, отриманих внаслідок прийняття припущення про працездатність усіх підсистем або про відмову однієї з підсистем та відповідно про невиконання однієї з функцій f_1 - f_8 із таблиці 3.1. Результати аналізу отриманих 8 структур ІСБ з погляду ефективності наведено у таблиці 3.2, де у 4-му стовпці використовується звичайна п'ятибальна шкала оцінки.

Відповідно до лінгвістичної шкали методу МАІ визначаються ранги структур ІСБ з різними функціями (таблиця 3.2, стовпець 7). Для зручності побудови матриці парних порівнянь W упорядкуємо структури, що порівнюються так, щоб при збільшенні номера новозазначених систем Si

ранги зростали (див. таблиці 2, стовпець 6). В результаті будується матриця парних порівнянь [29, 30]:

$$W_S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 8 & 9 \\ 0{,}500 & 1 & 2 & 2 & 3 & 4 & 6 & 8 \\ 0{,}333 & 0{,}500 & 1 & 2 & 3 & 3 & 5 & 7 \\ 0{,}250 & 0{,}500 & 0{,}333 & 1 & 1 & 1 & 5 & 7 \\ 0{,}200 & 0{,}333 & 0{,}333 & 1 & 1 & 1 & 3 & 5 \\ 0{,}167 & 0{,}250 & 0{,}333 & 1 & 1 & 1 & 3 & 5 \\ 0{,}125 & 0{,}200 & 0{,}200 & 0{,}200 & 0{,}333 & 0{,}333 & 1 & 3 \\ 0{,}111 & 0{,}125 & 0{,}143 & 0{,}143 & 0{,}200 & 0{,}200 & 0{,}333 & 1 \end{pmatrix}.$$

Таблиця 3.2 - Аналіз ефективності отриманих структур ІСБ

№ структ. ІСБ	Працездатні підсистеми	Не працездатні підсистеми	Якісна оцінка ефективності виконання цільової функції отриманої структурою ІСБ	Ефективність виконання цільової функції	Позначення та ранги упорядкованих систем	
1	2,3,4,5,6,7	1	задовільно	3,3	S_5	5
2	1,3,4,5,6,7	2	задовільно	3,5	S_4	4
3	1,2,4,5,6,7	3	добре	4,1	S_3	3
4	1,2,3,5,6,7	4	задовільно	3,1	S_6	6
5	1,2,3,4,6,7	5	добре	4,3	S_2	2
6	1,2,3,4,5,7	6	поганно	2,2	S_7	8
7	1,2,3,4,5,6	7	дуже поганно	1,4	S_8	9
8	1,2,3,4,5,6,7	-	відмінно	5,0	S_1	1

З рівняння (1) визначається найбільше власне число λ_{max} = 8,318. Підставивши λ_{max} у формулу (1.1), знашодится індекс узгодженості ІС= 0,045. За формулою ОС = ІС/СС, де СС - значення узгодженості випадкової матриці 8 порядку (рівне 1,42), знайдемо величину відношення узгодженості ОС=0,032. Видно, що як ІС і ОС не перевищують порогового значення 0,1. Це означає, що матриця парних порівнянь W досить добре узгоджена.

З рівняння (1) визначено матрицю власних векторів, перший з яких є вектором пріоритетів для впорядкованих структур

$$V_S = (0{,}753 \quad 0{,}461 \quad 0{,}344 \quad 0{,}207 \quad 0{,}165 \quad 0{,}158 \quad 0{,}072 \quad 0{,}042)^T. \qquad (5)$$

Здійснивши зворотний перехід від упорядкованих структур, позначених S_i до вихідних структур з функціями f_1-f_8. Тоді вищезазначений вектор перетворюється на вигляд

$$V = (0{,}165 \quad 0{,}207 \quad 0{,}344 \quad 0{,}158 \quad 0{,}461 \quad 0{,}072 \quad 0{,}042 \quad 0{,}753)^T,$$

де порядок елементів відповідає нумерації функцій (таблиці 3.1).

Як і слід очікувати, рішення методу MAI не можуть бути застосовані безпосередньо. Значення вектора пріоритетів (5) для менш значущих об'єктів виявилися невиправдано заниженими: проти максимальним значенням 0,753 шостий і сьомий об'єкти мають показники 0,072, 0,042, тобто. менше в 10,46 та 17,93 разів, відповідно. Тому потрібна корекція результатів експертизи.

Застосовується для корекції процедура асоціативного навчання нейронної мережі нормалізованою функцією активації softmax, подаючи на її вхід вектор пріоритетів (5). В основі процедури лежить модель змішування думок експертів, розглянута в підрозділі 3.1 [31-33].

В результаті обробки вектора пріоритетів (15) нейронною мережею з функцією активації softmax отримаємо скоригований вектор пріоритетів

$$V_{\text{корр}} = (0{,}109 \quad 0{,}113 \quad 0{,}130 \quad 0{,}108 \quad 0{,}146 \quad 0{,}099 \quad 0{,}096 \quad 0{,}196)^T.$$

Результати моделювання представлено на рисунку 3.2 де на верхній частині малюнка (рисунок 3.2, а) проілюстровано надмірне придушення оцінок методу аналізу ієрархій для 4, 6, 7 об'єктів. На нижній частині малюнка (рисунок 3.2, б) наведено результати корекції оцінок на основі процедури асоціативного навчання з нормалізованою функцією активації (3), що призводить до зовсім іншої інтерпретації вирішення завдання експертизи.

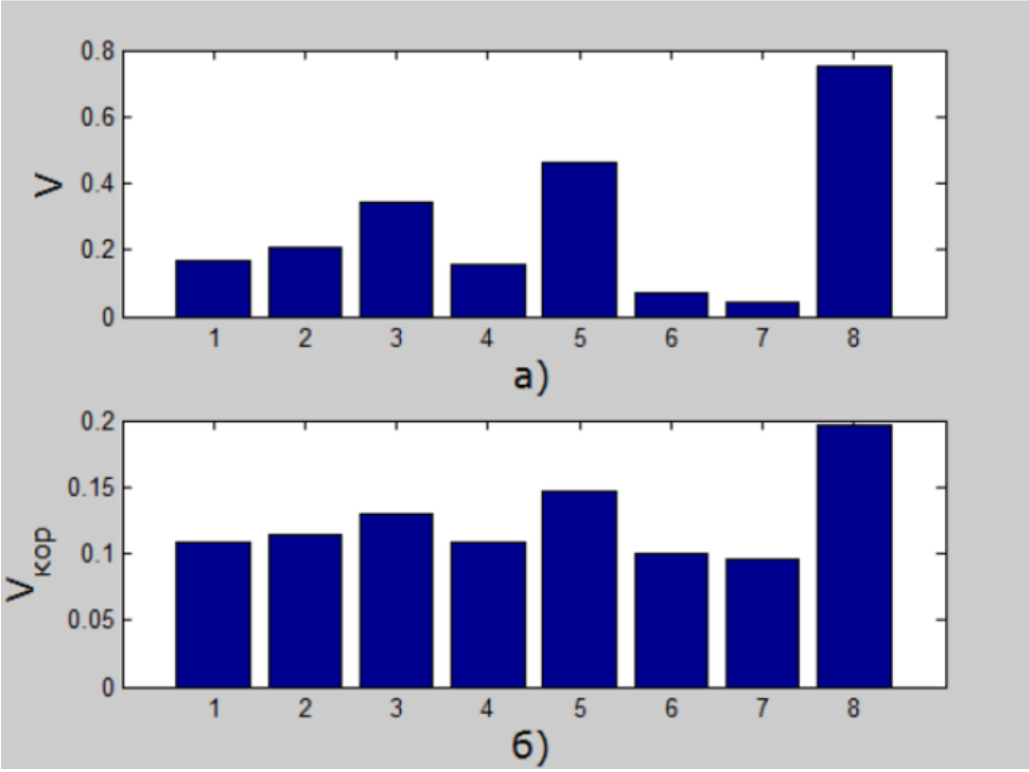


Рисунок 3.2 - Вектор пріоритетів: а) – після застосування методу аналізу ієрархій; б) - після процедури корекції нейронною мережею з функцією softmax

Навіть менш якісні структури порівнюваних ІСБ у результаті отримали деяке «право» на участь в експертизі, що підтверджує віднесення ІСБ до класу якісно-складних систем, у яких є вихідні функції, що характеризуються деяким числом станів часткової відмови або часткової працездатності, а цілі роботи системи реалізуються з різним ступенем ефективності. Обґрунтованість такого підходу підтверджується думкою відомого фахівця в галузі нейронних мереж С. Хайкіна: «Жорсткі рішення, на жаль, призводять до втрати інформації, тоді як м'які рішення її зберігають…».

Загалом розглянуте вище завдання є прикладом практичного використання методу занурення конкретної чисельної задачі в експертну оболонку у класі DMS (Data Mining System), представлену нечітко-множинним методом аналізу ієрархій та асоціативним навчанням нейронної мережі.

ВИСНОВКИ

У представленій магістерській роботі розроблена комп’ютерно-інтегрована система захисту від несанкціонованого проникнення на об’єкт закритого типу. У ході виконання кваліфікаційної роботи проаналізовані системи контролю і управління доступом, що в свою чергу дозволило реалізувати високоефективну інтегровану систему безпеки.

Проведений аналіз сучасних систем контролю та управління доступом довів ефективність інтегрованого підходу до організації безпеки об'єктів закритого типу. Встановлено, що сучасні СКУД повинні поєднувати фізичний захист з кібербезпекою, що дозволяє створити багаторівневу систему захисту. Доведено переваги комбінованих рішень, що інтегрують RFID-технології, біометричні методи та системи відеоаналітики.

Розроблено уніфіковану методологію проектування СКУД, що включає послідовну реалізацію етапів: аналіз вимог безпеки, вибір архітектури системи, інтеграцію компонентів та тестування. Запропоновано підхід до створення масштабованих систем, здатних адаптуватися до змінних умов експлуатації та нових викликів безпеки.

Обґрунтовано ефективність використання багатофакторної аутентифікації та криптографічного захисту даних. Розроблено модель безпеки, що поєднує фізичний контроль доступу з захистом інформаційних потоків, що забезпечує цілісність і конфіденційність даних на всіх рівнях системи.

Встановлено критерії вибору технічних засобів автоматизації, що враховують специфіку об'єктів закритого типу. Визначено необхідність забезпечення високої доступності, відмовостійкості та захищеності системи від сучасних кіберзагроз.

Створено архітектуру комп'ютерно-інтегрованої системи, що забезпечує централізоване управління всіма компонентами безпеки.

Розроблено алгоритми функціонування системи, що реалізують принцип багаторівневого контролю та швидкого реагування на загрози.

Доведено доцільність використання промислових ПЛК Siemens SIMATIC S7-1500, комбінованих систем ідентифікації та захищених мережевих рішень. Обґрунтовано вибір компонентів на основі аналізу їх відповідності вимогам надійності, безпеки та масштабованості.

Запропоновано метод адаптації ієрархічних структур систем безпеки на основі нейромережевих технологій. Розроблено алгоритм динамічного перерозподілу пріоритетів захисту залежно від рівня загрози та критичності об'єктів.

Створено метод формування пріоритетів функцій інтегрованих систем безпеки, що базується на аналізі шаблонів поведінки та прогнозуванні загроз. Доведено ефективність використання асоціативного навчання нейронної мережі для підвищення адекватності реакції системи на зовнішні виклики.

Роботою доведено ефективність запропонованого підходу до створення комп'ютерно-інтегрованих систем захисту для об'єктів закритого типу. Розроблена система забезпечує комплексний захист від несанкціонованого проникнення шляхом інтеграції фізичних та інформаційних засобів безпеки. Використання нейромережевих технологій дозволяє створити адаптивну систему, здатну ефективно протидіяти сучасним загрозам.

Запропонована комп’ютерно-інтегрована система захисту від несанкціонованого проникнення на об’єкт закритого типу, що забезпечує надійну, безперебійну роботу і показує, що при застосуванні методу асоціативного навчання нейронної мережі для функціонування можливостей інтегрованих систем безпеки ефективність якої зростає в рази. Це в свою чергу дає можливість мінімізувати затрати фізичної праці, що значно підвищує надійність роботи такої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Benantar M. Access Control Systems: Security, Identity Management and Trust Models. Berlin : Springer, 2005. 281 с.
2. Sandhu R. S., Coynek E. J., Feinstein H. L., Youman C. E. Role-Based Access Control Models. *IEEE Computer*, 1996, Vol. 29, No. 2, с. 38–47.
3. Ferraiolo D. F., Kuhn D. R. Proposed NIST Standard for Role-Based Access Control. NIST, 2001. 30 с.
4. Ferraiolo D. F., Kuhn D. R., Chandramouli R. Role-Based Access Control. 2nd ed. Boston : Artech House, 2007. 400 с.
5. Ayedh A. T. Systematic Literature Review on Security Access Control: Privacy, BYOD, Authorization. *Applied Sciences*, 2023, Vol. 13, No. 14, Art. 8048.
6. A systematic literature review for authorization and access control models. Journal (ScienceDirect*)*, 2022.
7. Kaur H., Singh A**.** A Comprehensive Review on Access Control Systems amid Global Pandemic. *Scientific Review Journal*, 2022.
8. Exploring the Role of Machine Learning in Enhancing Access Control Systems: A Comprehensive Review. *ResearchGate*, 2023.
9. Punia A. Blockchain-based Access Control: A Systematic Review. *Journal of Cloud Computing* (Springer), 2024.
10. Cobrado U. N. Access Control Solutions in Electronic Health Record (EHR) Systems: A Systematic Review. SSRN, 2024.
11. Бортник Г. Г., Кичак В. М., Стальченко О. В. Системи доступу : підручник. Вінниця : ВНТУ, 2010. 298 с.
12. Гавриленко І. О. Система контролю доступу : магістерська робота. Київ : КПІ ім. Ігоря Сікорського, 2022.
13. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів : Видавництво Львівської політехніки, 2019. 580 с.

14. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навчальний посібник. Харків : ХНЕУ, 2008.
15. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2020.
16. Остапенко О. Інформаційне право України : навчальний посібник. Львів : ЛьвДУВС, 2022. 416 с.
17. DEPS. Системи контролю і управління доступом: від А до Я. Київ : DEPS, 2024.
18. Вишняков В. М. Захист інформації в комп'ютерних системах : навчальний посібник. Київ : КНУБА, 2022.
19. Лупенко С.А., Тиш Є.В. Прикладна теорія цифрових автоматів. Навчальний посібник. Тернопіль: ТНТУ ім. І. Пулюя. 2011. 247 с. 14.
20. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп'ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.
21. Osukhivska H., Tysh I., Lobur T., Shylinska I., Lupenko S. Method for Estimating the Convergence Parameters of Dynamic Routing Protocols in Computer Networks. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT). 2021. Vol. 1. P. 228-231.
22. Тиш Є., Зима О. Вибір критеріїв ефективності безпровідних телеметричних мереж. Матеріали VII науково-технічної конференції "Інформаційні моделі, системи та технології". Тернопіль : ТНТУ. 2019. С. 139.
23. Тиш Є.В., Зима О.В. Методи та засоби підвищення ефективності безпровідних телеметричних мереж. Збірник тез доповідей VIII Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». 2019. С. 101.
24. Оконський М. В., Лупенко С. А., Паламар А. М. Комп'ютерна система для моніторингу метеорологічних параметрів на основі IoT. Збірник тез

доповідей X Міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». 2021. С. 109.

25. Vasylkivskyi I., Ishchenko V., Pohrebennyk V., Palamar M., Palamar A. System of water objects pollution monitoring. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management (SGEM 2017), Vienna, Austria. 2017. Vol. 17, No. 33. P. 355-362.

26. Palamar A. Intelligent control and monitoring module for uninterruptible power supply system. II International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» (MC&FPGA-2020), Kharkiv, Ukraine. 2020. P. 12-13.

27. Луцька Н.М. Дослідження та синтез оптимальних регуляторів для систем автоматизації технологічних комплексів неперервного типу [Текст]: дис. канд. техн. наук : 05.13.07 / Н.М. Луцька – Київ, 2006. – 180С.

28. Теорія автоматичного керування: Підручник. — 2-ге вид., перероб. і догі. К.: Либідь, 2007. — 656 с.

29. Курдюков А.П. Синтез робастного H∞-регулятора для управления энергетической котельной установкой / А.П. Курдюков, В.Н. Тимин // Управление большими системами. – 2009. – № 25. – С. 179–214.

30. Бунке О.С. Автоматизація процесів керування інерційними контурами котлоагрегата теплової електростанції з використанням методу динамічної корекції [Текст]: дис. канд. техн. наук : 05.13.07 / О.С. Бунке – Київ, 2014. – 174 с.

31. Артюх С.Ф. Основы автоматизированных систем управления энергогенерирующими установками электростанций [Текст] / С. Ф. Артюх, М.А. Дуэль, И.Г. Шелепов – Х.: Знание, 1998. – 324 с.

32. ДСТУ Б А.2.4-16:2008. Автоматизація технологічних процесів. Умовні графічні зображення приладів і засобів автоматизації в схемах. – К.: Мінрегіонбуд України, 2009.

33. Клепач М.І. Теорія автоматичного керування. Навчальний посібник. / М.І. Клепач / Рівне: НУВГП, 2007. – 206 с.