Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему Дослідження сучасних методів контролю доступу
(назва теми)
в розподілених системах

Виконав: студент 2 курсу, групи БК-713м

Спеціальності 125 Кібербезпека та захист
(код і найменування спеціальності)
інформації

Освітня програма (спеціалізація)
Системи технічного захисту інформації,
автоматизація її обробки

ПОСТОЛЕНКО М. О.
(ПРІЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р. Ю.
(ПРІЗВИЩЕ та ініціали)
Рецензент ЛИТВИЦЬКИЙ О. П.
(ПРІЗВИЩЕ та ініціали)

2024

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
(код і найменування)
Освітня програма (спеціалізація) Системи технічного захисту інформації, автоматизація її обробки
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри інформаційної безпеки та наноелектроніки
_____ доц., к. ф. -м. н. Андрій КОРОТУН
«_____» _____20___року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ПОСТОЛЕНКА Максима Олександровича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження сучасних методів контролю доступу в розподілених системах
Research on Modern Access Control Methods in Distributed Systems
керівник проєкту (роботи) к.т.н., доцент КОРОЛЬКОВ Роман Юрійович ,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «5» грудня 2024 року № 507
2. Строк подання студентом проєкту (роботи) 10 грудня 2024 року
3. Вихідні дані до проєкту (роботи) Розробити методику впровадження СКУД з урахуванням сучасних технологій, таких як інтеграція з хмарними сервісами та біометричними ідентифікаторами, для підвищення ефективності безпеки на підприємствах.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Теоретичні основи систем контролю доступу (СКУД), історія та сучасний стан розвитку СКУД, особливості впровадження СКУД на підприємствах, аналіз методів контролю доступу, методика впровадження СКУД
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Схеми моделей керування доступом, презентація (11 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Розділ 1	КОРОЛЬКОВ Р.Ю., к.т.н. доцент	07.10.2024	14.10.2024
Розділ 2	КОРОЛЬКОВ Р. Ю., к.т.н. доцент	21.10.2024	28.10.2024
Розділ 3	КОРОЛЬКОВ Р.Ю., к.т.н. доцент	11.11.2024	17.11.2024
Нормоконтроль	КОРОЛЬКОВ Р. Ю., к.т.н. доцент	25.11.2024	1.12.2024

7. Дата видачі завдання «07» жовтня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Постановка завдання роботи.	07.10.2024 – 13.10.2024	Виконано
2	Опрацювання літератури та проведення емпіричного досліження.	14.10.2024 – 20.10.2024	Виконано
3	Аналіз предметної області.	21.10.2024 – 27.10.2024	Виконано
4	Проведення наукового огляду.	28.10.2024 – 10.11.2024	Виконано
5	Оформлення пояснювальної записки.	11.11.2024 – 24.11.2024	Виконано
7	Нормоконтроль та рецензування.	25.11.2024 – 1.12.2024	Виконано
8	Захист дипломної роботи.	2.12.2024 – 8.12.2024	Виконано

Студент(ка) _____ **Максим ПОСТОЛЕНКО**
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ **Роман КОРОЛЬКОВ**
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломного проєкту: 118 с., 12 таб., 36 рис., 1 дод., 36 джерел.

ІДЕНТИФІКАЦІЯ, КОНТРОЛЕРИ, СИНХРОНІЗАЦІЯ, СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ, СТАНДАРТИ

Об’єкт дослідження – процеси забезпечення контролю доступу на підприємствах.

Предмет дослідження – методика впровадження систем контролю та управління доступом із застосуванням сучасних технологій, зокрема інтеграції з хмарними сервісами та біометричними ідентифікаторами.

Мета роботи – розробка методики впровадження СКУД з урахуванням сучасних технологій, таких як інтеграція з хмарними сервісами та біометричними ідентифікаторами, для підвищення ефективності безпеки на підприємствах.

Методи дослідження – аналіз літературних джерел та нормативно-правових актів щодо впровадження СКУД на підприємствах; порівняльний аналіз сучасних систем контролю доступу; визначення потреб та характеристик підприємств для впровадження системи контролю, моделювання процесів інтеграції СКУД з хмарними сервісами; емпіричний аналіз ефективності запропонованих рішень у різних сценаріях використання.

У роботі розглянуті основні типи систем контролю та управління доступом (СКУД): на основі карток, біометрії, кодів доступу, мобільні системи, інтернет системи та гібридні системи. Досліджені способи ідентифікації осіб у системі контролю доступу, з’єднання між пристроями системи. Проведений аналіз переваг та недоліків використання різних типів СКУД, ринок виробників систем контролю доступу.

ANNOTATION

Explanatory note for the diploma project: 118 pages, 12 tables, 36 figures, 1 appendix, 36 references.

ACCESS CONTROL AND MANAGEMENT SYSTEM, CONTROLLERS, IDENTIFICATION, STANDARDS, SYNCHRONIZATION

Object of research: processes for ensuring access control in enterprises.

Subject of research: methodology for implementing access control and management systems using modern technologies, including integration with cloud services and biometric identifiers.

Purpose of the work: development of a methodology for implementing access control systems (ACS) considering modern technologies, such as integration with cloud services and biometric identifiers, to enhance security efficiency in enterprises.

Research methods: analysis of literary sources and regulatory acts regarding the implementation of ACS in enterprises; comparative analysis of modern access control systems; identification of needs and characteristics of enterprises for system implementation; modeling of ACS integration processes with cloud services; empirical analysis of the effectiveness of proposed solutions in various usage scenarios.

The study reviews the main types of access control and management systems (ACS): card-based, biometric, access code-based, mobile systems, internet-based systems, and hybrid systems. It examines methods of individual identification in access control systems and connections between system devices. An analysis of the advantages and disadvantages of using various ACS types and the access control system manufacturers' market is also conducted.

ЗМІСТ

С.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – база даних

БІ – біометричний ідентифікатор

ПП – перегороджувальні пристрої (турнікети, шлагбауми, двері тощо)

СЗІ – система захисту інформації

СКУД – система контролю та управління доступом

AI – Artificial Intelligence (штучний інтелект)

API – Application Programming Interface (інтерфейс прикладного програмування)

AR – Augmented Reality (доповнена реальність)

CE – Conformité Européenne (відповідність європейським стандартам безпеки)

HID – Human Identification Device (ідентифікація людини)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

IoT – Internet of Things (інтернет речей)

LAN – Local Area Network (локальна обчислювальна мережа)

NFC – Near Field Communication (комунікація ближнього поля)

OCR – Optical Character Recognition (оптичне розпізнавання символів)

QR – Quick Response (швидке реагування)

RFID – Radio Frequency Identification (радіочастотна ідентифікація)

TCP/IP – Transmission Control Protocol/Internet Protocol (протокол передачі даних у мережі)

UL – Underwriters Laboratories (стандарт безпеки підрозділу)

VPN – Virtual Private Network (віртуальна приватна мережа)

Wi-Fi – Wireless Fidelity (бездротовий зв'язок для передачі даних)

ВСТУП

Безпека підприємств у сучасному світі є одним із ключових факторів, які визначають їхню успішну діяльність. Захист інформаційних ресурсів, матеріальних цінностей та контроль активності співробітників набувають особливого значення в умовах підвищеної конкуренції, розвитку технологій та зростання кількості кіберзагроз. Важливість цих аспектів зумовлює необхідність впровадження ефективних рішень, які не лише забезпечують захист, а й підвищують продуктивність роботи організації. Одним із найбільш дієвих інструментів для досягнення цих цілей є система контролю та управління доступом (СКУД).

СКУД забезпечує контроль доступу до територій та приміщень підприємства, запобігаючи несанкціонованому проникненню, яке може становити загрозу для майна, інформації чи навіть життя працівників. Завдяки широким функціональним можливостям СКУД дозволяє: ідентифікувати осіб, що мають право доступу; зонувати простір відповідно до рівнів доступу; керувати автоматичними процесами, такими як відкриття дверей, шлагбаумів, турнікетів; вести облік часу перебування співробітників на території підприємства; формувати звіти для аналізу активності працівників та виявлення потенційних ризиків. Ці функції забезпечуються завдяки інтеграції апаратних засобів (контролерів, зчитувачів, виконавчих пристроїв) та програмного забезпечення, яке дозволяє централізовано керувати всіма процесами.

Сучасний розвиток технологій створює нові можливості для вдосконалення СКУД, зокрема через інтеграцію з хмарними сервісами та використання біометричних ідентифікаторів. Такі рішення дозволяють.

1. Підвищити надійність системи. Біометричні ідентифікатори, такі як сканування відбитків пальців, райдужки ока чи розпізнавання обличчя,

унеможливлюють передачу або підробку доступу, що є характерним для традиційних карткових систем.

2. Забезпечити гнучкість і масштабованість. Хмарні сервіси дають змогу віддалено контролювати доступ, зберігати дані та керувати системою навіть для підприємств із розгалуженою структурою.

3. Інтегрувати системи безпеки. Поєднання СКУД із відеоспостереженням, пожежними чи аварійними системами забезпечує комплексний підхід до моніторингу та захисту об’єкта.

З огляду на постійний розвиток загроз, таких як кіберзлочинність, та посилення вимог до захисту інформації, впровадження сучасних СКУД стає не просто вибором, а необхідністю.

Для ефективного впровадження СКУД важливо враховувати специфічні потреби підприємства, такі як розмір та структура, тип діяльності, рівень безпеки. Аналіз потреб і характеристик дозволяє визначити оптимальний склад системи, функціонал та технології, які забезпечать необхідний рівень безпеки.

Розвиток СКУД є важливим етапом у забезпеченні безпеки підприємств. У сучасних умовах інтеграція системи з хмарними сервісами та біометричними технологіями не лише підвищує рівень захисту, але й відкриває нові можливості для ефективного управління підприємством. Актуальність роботи полягає в необхідності розробки адаптованої методики, яка відповідає потребам сучасного бізнесу та дозволяє досягти високих стандартів безпеки.

Об’єкт дослідження – процеси забезпечення контролю доступу на підприємствах.

Предмет дослідження – методика впровадження систем контролю та управління доступом із застосуванням сучасних технологій, зокрема інтеграції з хмарними сервісами та біометричними ідентифікаторами.

Мета роботи – розробка методики впровадження СКУД з урахуванням сучасних технологій, таких як інтеграція з хмарними сервісами та

біометричними ідентифікаторами, для підвищення ефективності безпеки на підприємствах.

Завдання роботи включають:

- аналіз потреб підприємства для СКУД;
- порівняння існуючих методів контролю доступу;
- обґрунтування вибору технологій для впровадження.

Для досягнення поставленої мети було застосовано такі методи: аналіз літературних джерел та нормативно-правових актів щодо впровадження СКУД на підприємствах; порівняльний аналіз сучасних систем контролю доступу (для визначення переваг та недоліків даних видів); визначення потреб та характеристик підприємств (зокрема, інженерно-технічної складової) для впровадження системи контролю, моделювання процесів інтеграції СКУД з хмарними сервісами; емпіричний аналіз ефективності запропонованих рішень у різних сценаріях використання.

У результаті дослідження розроблено методику впровадження СКУД, яка включає: рекомендації щодо вибору апаратних і програмних компонентів; алгоритм інтеграції СКУД з хмарними сервісами; стратегії використання біометричних ідентифікаторів для різних рівнів безпеки.

Наукова новизна полягає в тому, що в роботі запропоновано комплексну методику інтеграції сучасних технологій у СКУД, яка враховує потреби підприємств різного масштабу та специфіки. Вперше було проведено систематичний аналіз ефективності поєднання хмарних технологій і біометричних ідентифікаторів у контексті підприємницької безпеки.

Практичне застосування: методика може бути використана при проектуванні та впровадженні СКУД на підприємствах різного масштабу. Отримані результати є корисними для підвищення рівня захищеності інформації, оптимізації доступу до об’єктів, а також для підвищення довіри клієнтів і співробітників.

1 СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ (СКУД): ТЕОРЕТИЧНІ ЗАСАДИ

1.1 Поняття СКУД та їхній основний функціонал

Системи контролю та управління доступом (СКУД) є невід'ємною частиною сучасних заходів безпеки на підприємствах. Вони забезпечують контроль за доступом до приміщень і ресурсів, захищаючи інформацію, обладнання та персонал від несанкціонованого доступу. СКУД поєднують апаратні засоби, програмне забезпечення та процедури управління для досягнення високого рівня безпеки.

Існує декілька підходів до визначення СКУД. Зокрема, технічна концепція розглядає СКУД, як інтегровані апаратно-програмні комплекси, що забезпечують автоматизований контроль доступу до об'єктів або ресурсів, використовуючи ідентифікаційні засоби (картки, біометричні дані, PIN-коди тощо). СКУД у функціональній парадагмі являють собою системи, що виконують дві основні функції: аутентифікацію користувача (встановлення особи) та авторизацію (надання або обмеження доступу відповідно до встановлених прав). Відповідно до організаційного підходу СКУД – це інструмент забезпечення дисципліни й безпеки, що допомагає управляти потоками співробітників і відвідувачів, а також контролювати доступ до критично важливих зон об'єкта. Після розгляду поданих аспектів можна визначити системи контролю та управління доступом як комплексні системи, що використовують технічні, програмні та організаційні засоби для забезпечення контролю доступу до фізичних або цифрових ресурсів, обмежуючи його на основі встановлених правил і процедур [1].

Алгоритм роботи СКУД базується на послідовності дій, які включають встановлення обладнання, налаштування доступу, ідентифікацію користувачів та виконання відповідних дій системою (рисунок 1.1).

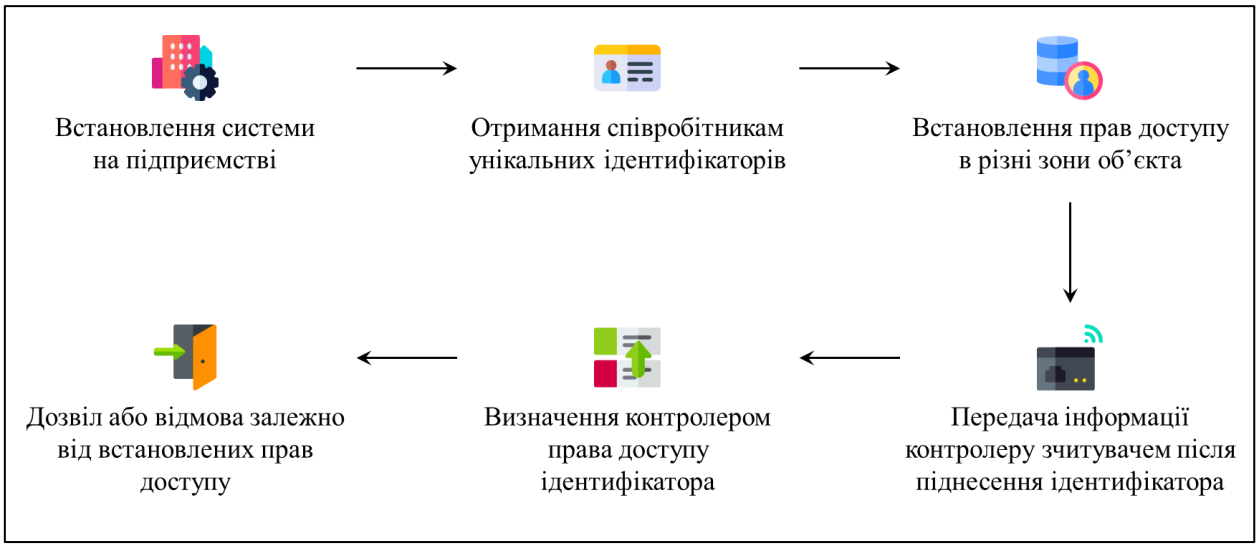

Рисунок 1.1 – Алгоритм роботи СКУД

Робота СКУД починається з фізичного встановлення системи на об'єкті, наприклад, на території підприємства, офісу чи іншого об’єкта. На цьому етапі здійснюється монтаж зчитувачів, контролерів, електронних замків і інших компонентів системи відповідно до специфіки об’єкта та його зон доступу. Обладнання підключається до центрального серверу або хмарної платформи для забезпечення централізованого управління. Встановлення також включає перевірку обладнання на відповідність технічним вимогам і налаштування його для стабільної роботи.

Кожен співробітник підприємства отримує унікальний ідентифікатор, який використовується для ідентифікації в системі. Ідентифікаторами можуть бути безконтактні або магнітні картки, біометричні дані, наприклад, відбитки пальців чи сканування обличчя, або персональні коди для введення на клавіатурі. Унікальність ідентифікатора забезпечує точність і надійність аутентифікації. На цьому етапі відбувається реєстрація ідентифікатора у базі даних СКУД із прив’язкою до відповідного співробітника.

Важливим етапом є встановлення прав доступу для кожного користувача. Для цього адміністратор системи визначає, до яких зон об’єкта співробітники мають право доступу та в які часові проміжки. Наприклад, права доступу можуть бути обмежені тільки робочими годинами або

дозволяти вхід лише до певних приміщень залежно від функціональних обов’язків співробітника. Такий підхід забезпечує персоналізацію доступу та підвищує рівень безпеки.

Коли співробітник підносить свій ідентифікатор до зчитувача, пристрій зчитує унікальний код і передає його контролеру. Цей процес відбувається миттєво та може здійснюватися через безконтактну технологію або через введення коду на клавіатурі. Зчитувач відіграє роль інтерфейсу між користувачем і системою, забезпечуючи передачу інформації без затримок.

Контролер отримує дані від зчитувача і проводить перевірку прав доступу для даного ідентифікатора. Він порівнює отриману інформацію з базою даних, визначаючи, чи має співробітник право входу до конкретного приміщення у цей момент часу. Якщо умови доступу виконані, контролер надсилає сигнал на електронний замок для відкриття дверей.

Відкриття приміщення відбувається тільки за наявності відповідного права доступу. Якщо перевірка ідентифікатора успішна, двері розблоковуються, і співробітник отримує доступ до контрольованої зони. У разі відсутності прав або виявлення помилок ідентифікації, система генерує повідомлення про відмову у доступі. Це повідомлення може бути відображене на екрані зчитувача або передане адміністратору системи.

СКУД працює за принципом точного виконання алгоритму, що гарантує контроль доступу в реальному часі. Інформація про кожен випадок використання системи зберігається в журналі подій, який дозволяє проводити аудит або аналіз діяльності на об'єкті. Такий підхід не тільки підвищує рівень безпеки, але й сприяє ефективному управлінню персоналом та дотриманню вимог внутрішнього регламенту підприємства 1.

Функціонал систем контролю та управління доступом (СКУД) є основою їх ефективності та визначає, як ці системи забезпечують безпеку, автоматизацію та управління доступом на підприємствах. Кожна функція має своє призначення, яке спрямоване на вирішення конкретних завдань з контролю доступу, забезпечення безпеки та оптимізації операційних процесів.

Широкий спектр завдань, які виконують СКУД, можна умовно розділити на кілька груп: основні, додаткові та аналітичні. Перелік функцій згідно з даної класифікації подано в таблиці 1.1.

Таблиця 1.1 – Функції системи контролю та управління доступом

Тип функції	Функція СКУД
Основна	Ідентифікація користувача (за допомогою карток, біометрії, кодів).
Основна	Контроль доступу до приміщень або зон з обмеженим доступом.
Основна	Запис і зберігання даних про всі спроби доступу.
Основна	Інтеграція з іншими системами безпеки (відеоспостереження, охоронна сигналізація).
Додаткова	Моніторинг присутності співробітників на об'єкті.
Додаткова	Управління графіком роботи та обліком робочого часу.
Додаткова	Генерація звітів про доступ та аномальні дії.
Додаткова	Дистанційне управління доступом через мережу.
Аналітична	Аналіз поведінки користувачів у системі.
Аналітична	Виявлення підозрілих дій (наприклад, багаторазові невдалі спроби входу).

Ідентифікація користувачів є однією з ключових функцій СКУД. Це розпізнавання особи, яка намагається отримати доступ до певного приміщення чи зони. Цей процес реалізується через різноманітні технології, такі як:

- фізичні носії: картки (RFID, магнітні), браслети, жетони;
- біометричні параметри: відбитки пальців, розпізнавання обличчя, райдужки ока.

– коди доступу: введення PIN-коду або пароля.
Ця функція дозволяє забезпечити чіткий облік, унеможливити несанкціонований доступ і забезпечити персоналізацію дій у системі.

Контроль доступу є другою основною функцією СКУД. Так, система обмежує доступ до певних зон відповідно до прав, встановлених для конкретного користувача чи групи осіб. Завдяки цьому забезпечується захист конфіденційних зон або обладнання, стає можливим налаштування різних рівнів доступу для співробітників, відвідувачів або підрядників, а також фіксування час входу та виходу, що також дозволяє проводити аудит безпеки.

Реєстрація подій – функція, яка дозволяє СКУД вести журнал усіх дій і подій, пов'язаних із доступом. Фіксуються час, дата та ідентифікація користувача, записуються спроби несанкціонованого доступу, забезпечується збереження інформації для подальшого аналізу або розслідування інцидентів. Це важливий інструмент для аналітики, моніторингу та створення звітів.

СКУД також дозволяють централізовано або локально налаштовувати права доступу. Це передбачає:

– призначення прав залежно від посади, рівня доступу або розкладу роботи тощо;

– динамічну зміну параметрів у разі переведення співробітника, звільнення чи зміни робочих процесів;

– автоматичне оновлення політик доступу через інтеграцію з іншими системами управління персоналом.

Наступною функцією є інтеграція з іншими системами: відеоспостереження, пожежної сигналізації, охоронними системами чи ERP-системами. Завдяки цьому усі системи працюють як єдиний механізм для забезпечення безпеки, стає технічно можливим автоматично реагувати на події, наприклад, відключати доступ у разі пожежі. Додатково забезпечується оптимізація управління ресурсами через обмін даними між підсистемами.

СКУД забезпечує автоматичний облік робочого часу персоналу. Це означає, що фіксується час приходу та відходу співробітників, що в

подальшому дозволяє створювати звіти про запізнення, прогули чи понаднормову роботу. Ця функція також інтегрується із зарплатними системами для автоматизації нарахувань.

Функцією цих систем є й обмеження доступу в разі виникнення небезпечної ситуації (наприклад, пожежі чи зламу). СКУД можуть автоматично блокувати або відкривати доступ до певних зон. Наприклад, може відбуватися блокування критичних зон для зупинки зловмисників або автоматичне відкриття дверей для евакуації персоналу під час надзвичайних ситуацій.

СКУД часто включають функцію віддаленого управління, що дозволяє: контролювати доступ із мобільного додатку чи комп’ютера, налаштовувати права доступу у реальному часі, миттєво реагувати на інциденти навіть поза межами об'єкта.

Особливістю архітектури систем контролю та управління доступом є масштабованість і змінність конфігурації. Системи можуть бути розширені або модифіковані залежно від змін у структурі підприємства. Наприклад, може відбуватися додавання нових точок доступу, інтеграція з новими технологіями чи зміна політики безпеки.

Сучасні СКУД також придатні до інтеграції з мобільними технологіями. Вони найчастіше використовують мобільні додатки для забезпечення доступу без використання фізичних карток, надання тимчасових прав доступу через QR-коди або посилання та оповіщення про події в реальному часі.

Аналітика та звітність є ще однією функцією таких систем. СКУД генерують дані, які можуть використовуватись для створення звітів про активність, ефективність роботи співробітників та безпеку об’єкта. Це дозволяє прогнозувати можливі загрози, оптимізувати політики доступу, контролювати завантаженість певних зон.

Функціонал СКУД є надзвичайно багатогранним і дозволяє вирішувати як завдання безпеки, так і питання автоматизації бізнес-процесів. Завдяки

широким можливостям налаштування, інтеграції та аналітики, ці системи стали важливим елементом сучасного управління підприємствами.

Системи контролю і управління доступом (СКУД) стають важливим елементом сучасних підприємств, забезпечуючи безпеку, оптимізацію процесів і підвищення ефективності. Однак їх впровадження супроводжується як значними перевагами, так і низкою обмежень (таблиця 1.2). Аналіз цих аспектів допоможе зрозуміти, чи є такі системи доцільним рішенням для конкретного підприємства.

Таблиця 1.2 – Переваги та недоліки впровадження СКУД

№	Переваги	Недоліки
1	Підвищення рівня безпеки	Висока вартість впровадження
2	Ефективне керування персоналом	Технічні проблеми
	Зниження витрат	Проблема конфіденційності
	Простота використання	Ризик хакерських атак
	Гнучкість	Залежність від електропостачання
	Зручність	Проблеми з інтеграцією

Однією з основних переваг СКУД є підвищення рівня безпеки. Вони дозволяють мінімізувати ризики несанкціонованого доступу до об'єктів підприємства, захищати матеріальні та інформаційні ресурси, а також забезпечувати фізичну безпеку працівників і відвідувачів. Інтеграція із системами відеоспостереження та сигналізації дає можливість оперативного реагування на потенційні загрози.

СКУД є інструментом ефективного керування персоналом. Вони автоматизують процеси обліку робочого часу, дозволяють відстежувати переміщення співробітників у межах об'єкта та контролювати дотримання трудової дисципліни. Такі функції сприяють підвищенню продуктивності праці та оптимізації використання робочого часу.

Зниження витрат є ще однією перевагою СКУД. Завдяки автоматизації процесів контролю доступу підприємства можуть зменшити витрати на фізичну охорону. Крім того, використання таких систем зменшує витрати, пов'язані з втратами матеріальних цінностей через крадіжки або порушення.

СКУД характеризуються простотою використання. Сучасні системи розроблені таким чином, щоб забезпечувати інтуїтивно зрозумілий інтерфейс для користувачів і адміністраторів. Це мінімізує потребу в спеціальному навчанні та прискорює впровадження систем.

Гнучкість є ще однією важливою рисою СКУД. Вони можуть бути адаптовані до потреб конкретного підприємства, включаючи розширення функціоналу чи інтеграцію з іншими системами, такими як ERP або CRM.

Зручність СКУД полягає у можливості віддаленого моніторингу та керування. Багато сучасних рішень пропонують мобільні додатки або хмарні платформи, що дозволяє адміністраторам мати доступ до системи будь-де і будь-коли.

Одним із основних недоліків СКУД є висока вартість впровадження. Це стосується як початкових витрат на закупівлю обладнання, так і витрат на встановлення, налаштування та обслуговування системи. Для малих підприємств така інвестиція може бути фінансово обтяжливою.

Технічні проблеми також можуть стати суттєвою перешкодою. Поломка обладнання, збої у програмному забезпеченні або інші технічні несправності можуть призвести до простою підприємства або втрати доступу до приміщень.

Питання конфіденційності є важливим аспектом, особливо для систем, які обробляють біометричні дані або персональну інформацію. Недотримання стандартів захисту даних може призвести до порушення законодавства та втрати довіри співробітників.

Хакерські атаки становлять серйозну загрозу для сучасних СКУД, особливо тих, які працюють через Інтернет або зберігають дані у хмарних сервісах. Злом системи може поставити під загрозу безпеку підприємства. В Україні протягом останніх років кібератаки суттєво впливали на роботу різних

секторів, включаючи системи контролю і управління доступом (СКУД) на підприємствах. Одним із найвідоміших прикладів була атака NotPetya у 2017 році, яка паралізувала діяльність багатьох українських підприємств, включаючи державні установи та великі компанії. Ця атака була спрямована на шифрування даних і впливала на критичні інфраструктури, що також ускладнило доступ до приміщень, захищених СКУД, через відсутність доступу до серверів і баз даних.

У 2022 році спостерігалося зростання атак, які були частиною гібридної війни. Наприклад, під час початку російського вторгнення в лютому 2022 року хакери здійснили атаки на енергетичну інфраструктуру та державні установи, використовуючи шкідливе програмне забезпечення HermeticWiper. Подібні інциденти часто впливають на СКУД, оскільки відключення електрики та порушення мережевого з'єднання обмежують їхню функціональність.

Додатково, у 2023 році зафіксовано численні атаки, спрямовані на отримання доступу до критичних даних через слабкі місця в інфраструктурі кібербезпеки. У деяких випадках компрометація мереж дозволяла зловмисникам маніпулювати системами доступу, створюючи потенційні загрози для фізичної безпеки об’єктів [2].

Кібератаки такого типу демонструють необхідність інтеграції кращих практик кіберзахисту для СКУД, включаючи шифрування даних, резервні копії, вчасні оновлення систем а також регулярний моніторинг мережевої активності для попередження інцидентів

Залежність від електропостачання є ще одним недоліком СКУД. У разі перебоїв з електроенергією система може припинити функціонування, якщо не передбачено резервного живлення.

Проблеми з інтеграцією можуть виникати, коли підприємство намагається поєднати СКУД із вже існуючими системами безпеки або управління. Це може потребувати додаткових витрат на налаштування та зміну інфраструктури.

СКУД є потужним інструментом для підвищення безпеки та оптимізації бізнес-процесів. Їх переваги, такі як автоматизація, гнучкість і зручність, роблять їх невід'ємною частиною сучасних підприємств. Однак перед впровадженням слід ретельно оцінити недоліки, включаючи витрати, технічні ризики та можливі проблеми з конфіденційністю. Успішне використання СКУД залежить від їх адаптації до конкретних потреб підприємства, а також від забезпечення належного технічного обслуговування та захисту даних.

1.2 Історія розвитку СКУД

Історія СКУД бере свій початок у другій половині XX століття, коли технологічний прогрес у галузі електроніки, інформатики та механіки заклав основу для розвитку інноваційних систем контролю доступу. Розвиток цих систем пройшов кілька ключових етапів, кожен із яких був визначений технологічними досягненнями, змінами в підходах до безпеки та еволюцією потреб у різних сферах діяльності. Перебіг основних етапів разом з часовими межами подано в таблиці 1.3.

Перші спроби регулювання доступу були пов'язані з використанням механічних пристроїв, таких як ключі та замки і відбувалися ще в давні часи. Замки використовуються вже понад 6000 років. Один із ранніх прикладів був виявлений у руїнах Ніневії, столиці стародавньої Ассирії. Ці виназоди являли собою дерев'яний штифтовий замок, який складався із засуву, дверної арматури або насадки та ключа. Замки навісної конструкції з'явилися у Стародавньому Єгипті. Археологічні знахідки таких пристроїв відносяться до II-III століть нашої ери. Також замок був знайдений серед руїн палацу на Близькому Сході близько 930 року. до н. е. Цей пристрій, який отримав популярність як перший у світі замок з тумблером, він перекочував з Єгипту до Греції та Риму і навіть був знайдений у руїнах по всьому Близькому Сходу

та Європі. Дерев'яний замок був виявлений у Персії на охоронній брамі палацу Саргона II, який царював з 722 по 705 р.р. до н. е. Проривом у галузі створення нових замикаючих пристроїв можна завдячувати англійському винахіднику Й. Браму, який у 1784 році отримав патент на торцевий рамковий замок. Довгий час вважалося, що відкрити цей замок без руйнування неможливо. У XIX ст. американський інженер Л. Йель-молодший вніс радикальні інновації у виробництво замків, які лягли в основу сучасних замків із ключем та циліндром.

Таблиця 1.3 – Етапи розвитку СКУД

Період	Назва	Основні технології
До 1960-х	Ранні етапи	Механічні пристрої: ключі, замки
1960-1970-ті роки	Період електромеханічних систем	Електронні замки, панелі з кнопковими кодами
1980-ті роки	Перехід до електронних СКУД	Магнітні картки, мережеві системи, програмовані права доступу.
1990-ті роки	Поява біометричних технологій	Сканери відбитків пальців, розпізнавання обличчя та райдужки ока
2000-ті роки	Розвиток мережевих та інтелектуальних СКУД	Хмарні рішення, інтеграція із системами відеоспостереження, додатки для мобільних пристроїв
2010-2020-ті роки	Сучасний розвиток СКУД	Штучний інтелект (ШІ), біометрія нового покоління, інтеграція з IoT, децентралізовані системи на основі блокчейну

Хоча ці системи існували протягом століть, вони мали суттєві обмеження: ключі могли бути легко загублені або скопійовані. Не було можливості гнучкого управління правами доступу, наприклад, обмеження часу входу.

Однак механічні системи мали велике значення: вони створили основу для розуміння потреби у впорядкованому та персоналізованому доступі до приміщень.

З розвитком електротехніки у 1960-х роках почали з’являтися електромеханічні системи, які додали нові можливості до контролю доступу. Електронні замки дозволили керувати доступом за допомогою сигналів. Панелі з кнопковими кодами впровадили перші спроби ідентифікації користувачів без використання фізичних ключів.

Електромеханічні системи були обмежені з точки зору функціональності та безпеки, але вони започаткували ідею автоматизованого контролю доступу.

1980-ті стали поворотним моментом у розвитку СКУД завдяки впровадженню мікропроцесорних технологій. Головні інновації цього періоду включали використання магнітних карток. Вони дозволяли зчитувати інформацію та персоналізувати доступ для кожного користувача. Також тривав розвиток мережевих систем. Це дало змогу створювати бази даних користувачів, які могли динамічно оновлюватися. Настав час програмованих права доступу. Адміністратори могли встановлювати різні рівні доступу залежно від часу, ролі чи зони.

Перевагами електронних СКУД можна вважати підвищення гнучкості та ефективності систем і значне зменшення ризику підробки ключів.

У 1990-х роках відбувся прорив у сфері ідентифікації завдяки біометричним технологіям. Ці системи почали використовувати унікальні фізіологічні та поведінкові характеристики користувачів. Сканери відбитків пальців стали першими популярними біометричними пристроями. Розпізнавання обличчя та райдужки ока отримало розвиток завдяки прогресу в галузі камер та алгоритмів обробки зображень. Біометричні СКУД

дозволили суттєво підвищити рівень безпеки завдяки унікальності кожного користувача. Водночас вони були дорогими та складними у впровадженні.

З поширенням інтернету та розвитком інформаційних технологій у 2000-х роках системи СКУД стали інтегруватися з іншими інформаційними системами. Хмарні рішення дозволили централізовано зберігати та обробляти дані про користувачів. Інтеграція з відеоспостереженням підвищила рівень моніторингу. Додатки для мобільних пристроїв відкрили нові можливості для управління доступом. Ці системи отримали поширення у великих корпоративних структурах, банках, аеропортах та інших стратегічно важливих об'єктах.

Насьогодні системи контролю та управління доступом досягли високого рівня автоматизації, інтеграції та інтелектуалізації. Сучасні тенденції включають використання штучного інтелекту (ШІ) для аналізу поведінки користувачів та прогнозування ризиків (рисунок 1.2).

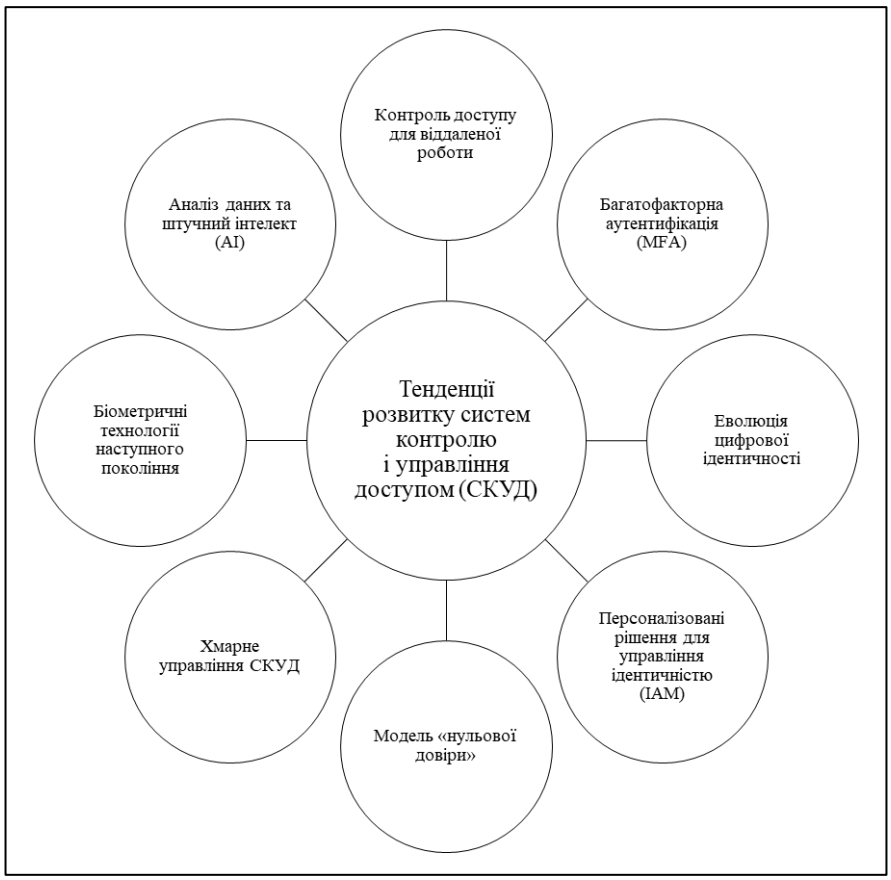

Рисунок 1.2 – Тенденції розвитку СКУД

Активно розвивається біометрія нового покоління, така як аналіз венозної системи або емоцій. Інтеграція з IoT (інтернетом речей) дозволяє керувати доступом через смарт-пристрої. Децентралізовані системи на основі блокчейну забезпечують високий рівень захисту даних. Сучасні СКУД охоплюють різноманітні функції, включаючи аналітику, технології безконтактного доступу, дистанційне управління, інтеграцію з системами управління будівлями (BMS) та автоматизацію бізнес-процесів.

Еволюція систем контролю доступу демонструє стрімкий розвиток від простих механічних замків до високотехнологічних інтегрованих рішень. Кожен етап історії розвитку СКУД відображає зміну підходів до безпеки, що диктується соціальними, технологічними та економічними потребами. Сьогодні СКУД є невід'ємною частиною інфраструктури багатьох об'єктів, що забезпечує високий рівень захисту, зручності та гнучкості.

Не можна не зазначити, що розвиток систем контролю та управління доступом (СКУД) у пострадянських країнах, включаючи Україну, впродовж багатьох років значно відставав від світових стандартів. Це відставання зумовлено історичними, економічними, технологічними та культурними факторами. Однак із часом ситуація почала змінюватися, особливо в останнє десятиліття.

У Радянському Союзі технології контролю доступу розвивалися насамперед у контексті військово-промислового комплексу та об'єктів стратегічного значення. СКУД для комерційного чи широкого цивільного використання практично не впроваджувалися. Основні рішення, що застосовувалися, включали прості механічні замки, а в кращому випадку — електромагнітні чи релейні системи для обмеження доступу в лабораторії чи закриті військові установи.

Після розпаду СРСР економічна криза 1990-х років сповільнила впровадження нових технологій, включаючи СКУД. Більшість підприємств та організацій зосереджувалися на виживанні, а не на інноваціях у сфері безпеки.

На відставання, першочергово, впливали проблеми технологічного характеру. Спостерігалася відсутність власного виробництва: пострадянські країни залежали від імпортованих технологій, зокрема з Європи, США або Азії. Через високі ціни на західні рішення масове впровадження сучасних СКУД було обмеженим. Рівень стандартизації був низьким. На відміну від країн із розвиненими ринками, у пострадянському середовищі довгий час бракувало чітких стандартів щодо інтеграції та роботи СКУД. Наприклад, міжнародні стандарти ISO або UL почали впроваджуватися значно пізніше і часто лише на вимогу міжнародних компаній, які відкривали офіси в регіоні. Використовувалися застарілі технології. Системи ідентифікації у вигляді магнітних карток або простих PIN-кодів залишалися домінуючими в той час, як у світі розвивалися біометричні, багаторівневі та адаптивні системи доступу.

Економічні труднощі в Україні та інших пострадянських країнах також відіграли важливу роль у відставанні. Інвестиції в системи безпеки вважалися необов’язковими витратами, і навіть великі підприємства часто обмежувалися мінімальними рішеннями. Висока вартість сучасних рішень стримувала масове впровадження.

На ситуацію впливали й особливості інфраструктури та культури. У пострадянських країнах інфраструктура часто не відповідала вимогам для встановлення сучасних СКУД. Старі будівлі, відсутність належних комунікаційних систем та інші фактори створювали перешкоди для впровадження новітніх технологій. Крім того, на багатьох підприємствах культурні особливості управління безпекою (наприклад, надія на "людський фактор") були бар'єром для автоматизації процесів.

Варто зазначити, що з початку 2010-х років ситуація почала покращуватися. Відбувся вихід на ринок міжнародних компаній, з'явилися глобальні постачальники, які пропонують сучасні рішення, адаптовані до локальних умов. Відбулося зростання попиту на високий рівень безпеки: після початку військових дій у 2014 році та посилення загроз безпеки підприємства

в Україні почали активніше інвестувати в сучасні системи захисту. Спостерігався розвиток місцевих компаній: українські виробники почали пропонувати конкурентоспроможні рішення за нижчими цінами.

Наразі українські підприємства активно впроваджують сучасні СКУД із біометрією, інтеграцією з відеоспостереженням, автоматичним збором даних та підтримкою адаптивної ідентифікації. Однак рівень їх впровадження поки що не досягає західних стандартів, особливо на малих та середніх підприємствах.

Відставання пострадянського простору у розвитку СКУД було спричинене сукупністю історичних, економічних і технічних факторів. Однак сучасні тенденції демонструють поступову інтеграцію в глобальні процеси. Завдяки міжнародній співпраці, впровадженню стандартів і зростанню попиту на безпеку Україна та інші країни регіону мають значний потенціал для досягнення передового рівня у сфері СКУД.

1.3 Загальні вимоги до СКУД

СКУД забезпечують санкціонований доступ до приміщень, інтеграцію з іншими системами безпеки (відеоспостереження, охоронні системи) та дозволяють відслідковувати потоки персоналу і ресурсів на підприємстві. Вимоги до таких систем можуть варіюватися залежно від типу об'єкта та рівня необхідної безпеки.

Для забезпечення надійної та якісної роботи системи в Україні були розроблені стандарти та нормативно-правові акти, що регулюють встановлення та експлуатацію систем контролю та управління доступом, зокрема на підприємствах. Крім безпосередньої безпеки об’єктів дані документи стосуються збереження та захисту персональних даних (див. таблицю 1.4).

Таблиця 1.4 – Документи, що регулюють функціонування СКУД

Документ	Змістове наповнення
Закон України «Про захист персональних даних» (№2297-VI від 01.06.2010) [3]	Даний закон регулює обробку та захист персональних даних, що є важливим для систем СКУД, які можуть обробляти інформацію про працівників або відвідувачів
Постанова «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» №373 від 29.03.2006	Документ, який затверджує правила захисту інформації в інформаційних і телекомунікаційних системах. СКУД часто є частиною таких систем, що вимагає дотримання цих норм
ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Чинний від 01.07.1997 р.	Стандарт, який описує порядок проведення робіт із технічного захисту інформації, що є основою для побудови безпечних систем, включаючи СКУД
НД ТЗІ 3.7-003-05. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [4]	Документ, який регламентує створення комплексних систем захисту інформації, до яких належать і системи контролю доступу.
ДСТУ EN 50134-7:2017 «Системи тривожної сигналізації. Суспільні системи сигналізації». Чинний від 01.08.2017 р. [5]	Стандарт, який регулює загальні вимоги до систем тривожної сигналізації, зокрема їхню структуру, компоненти, способи інсталяції, обслуговування та рівні захисту від злому.

Продовження таблиці 1.4

Документ	Змістове наповнення
ДСТУ EN 50136-1:2014 «Системи тривожної сигналізації. Системи передавання тривожних сповіщень та устаткування». Чинний від 01.08.2019 р.	Стандарт, який визначає вимоги до передачі сигналів у системах безпеки, охоплюючи характеристики каналів зв'язку, надійність і класифікацію за рівнями продуктивності.

У таблиці наведено основні нормативно-правові акти, виконання яких є обов’язковим під час встановлення систем контролю та управління доступом на підприємствах. Завдяки ним, забезпечується безпека та конфіденційність даних працівників та відвідувачів. Проте цей перелік є не вичерпним, і варто розглянути також актуальні світові та європейські документи, які також регулюють впровадження та функціонування СКУД. Наприклад, до таких документів належать ISO/IEC 27001, ISO/IEC 24762, EN 50133, UL 294. У таблиці 1.5 подано загальний зміст цих документів. Ці стандарти використовуються як основа для проєктування, впровадження та перевірки систем контролю доступу на підприємствах та доступні на офіційних платформах ISO, EN, або UL, а також у міжнародних стандартизаційних організацій.

Таблиця 1.5 – Світові стандарти, які регулюють СКУД

Документ	Змістове наповнення
ISO/IEC 27001 [6]	Цей стандарт стосується управління інформаційною безпекою, включаючи аспекти доступу до приміщень і інформаційних систем. Він визначає вимоги до впровадження політик і процедур для захисту доступу.

Продовження таблиці 1.5

Документ	Змістове наповнення
ISO/IEC 24762	Пропонує керівні принципи для безперервності інформаційних послуг, включаючи контроль доступу до критично важливих ресурсів.
EN 50133	Цей стандарт охоплює системи сигналізації та контролю доступу для використання в додатках безпеки, включаючи вимоги до системи, компонентів і їх використання в конкретних умовах
UL 294:2018 [7]	Стандарт описує мінімальні вимоги до конструкції, продуктивності та функціонування обладнання для контролю доступу, яке забезпечує регулювання входу/виходу або доступ до пристроїв через електричні, електронні або механічні засоби. UL 294 також враховує різні рівні безпеки для обладнання (від I до IV)

Насамкінець варто підкреслити, що для впровадження СКУД варто враховувати не тільки нормативно-правові вимоги, але й особливості кожного підприємства, включаючи внутрішні політики конфіденційності, необхідність інтеграції з IT-інфраструктурою та захисту від кібератак, про що йтиметься у Розділі 2 даної роботи.

1.4 Основні технічні характеристики СКУД

Швидкість реакції є фундаментальним параметром для будь-якої системи СКУД, оскільки вона визначає час від моменту активації (наприклад, зчитування ідентифікатора) до виконання дії (відкриття дверей, подачі

сигналу, чи іншої відповіді). Сучасні системи демонструють швидкість реакції на рівні від 0,2 до 1 секунди, залежно від типу ідентифікації. Наприклад, біометричні системи на основі відбитків пальців зазвичай мають час реакції близько 0,5 секунди, тоді як використання RFID-карт (рисунок 1.3) дозволяє досягати показників у межах 0,2–0,3 секунди. Затримка може варіюватися залежно від складності алгоритмів верифікації та умов експлуатації, наприклад, за високого навантаження або при обробці даних у хмарному середовищі.

Рисунок 1.3 – Приклади RFID-міток

Точність ідентифікації визначається здатністю системи коректно встановити особу або авторизувати доступ. У біометричних СКУД точність вимірюється коефіцієнтами помилок, серед яких найбільш важливими є рівень хибного прийняття (False Acceptance Rate, FAR) та рівень хибного відхилення (False Rejection Rate, FRR). У передових системах FAR може досягати значення 0,0001%, що еквівалентно одній помилці на мільйон спроб. Для FRR типовими є показники у межах 0,1–0,5%, що забезпечує високу надійність навіть у складних умовах експлуатації. Точність може погіршуватися через зовнішні фактори, наприклад, фізичне забруднення сенсорів або недосконаліть бази даних.

Підтримка протоколів є важливою характеристикою для інтеграції СКУД із іншими компонентами інфраструктури. Більшість сучасних систем підтримують протоколи, такі як Wiegand, OSDP (Open Supervised Device Protocol), а також IP-базовані протоколи. OSDP, наприклад, забезпечує двосторонній шифрований зв’язок між зчитувачами та контролерами, що підвищує безпеку системи. Водночас протоколи TCP/IP є ключовими для інтеграції з мережевими системами, дозволяючи віддалене адміністрування та моніторинг. Підтримка декількох протоколів забезпечує гнучкість і дозволяє інтегрувати СКУД в гібридні мережі.

Енергоспоживання є ще одним важливим аспектом. Більшість СКУД працює на основі живлення постійним струмом 12-24 В і потребує резервних джерел живлення для забезпечення безперервної роботи у разі відключення електроенергії.

Системи контролю та управління доступом (СКУД) поділяються на рівні безпеки залежно від їхньої здатності забезпечувати захист, ідентифікацію, контроль та управління доступом до об’єктів. Класифікація рівнів безпеки від I до IV (рисунок 1.4) дозволяє адаптувати обладнання до вимог конкретних умов експлуатації, загроз та об'єктів. Кожен рівень має свої особливості, технічні характеристики, сфери застосування, переваги та недоліки. Обладнання I рівня безпеки забезпечує мінімальний базовий захист. Його основною метою є запобігання несанкціонованому доступу до приміщень із низьким ризиком.

До прикладів такого обладнання належать електромеханічні замки та карткові рідери без криптографічного захисту. Вони характеризуються обмеженою функціональністю, оскільки пропонують лише локальний доступ. Іншою особливістю є підтримка простих ідентифікаторів, таких як PIN-коди або магнітні картки.

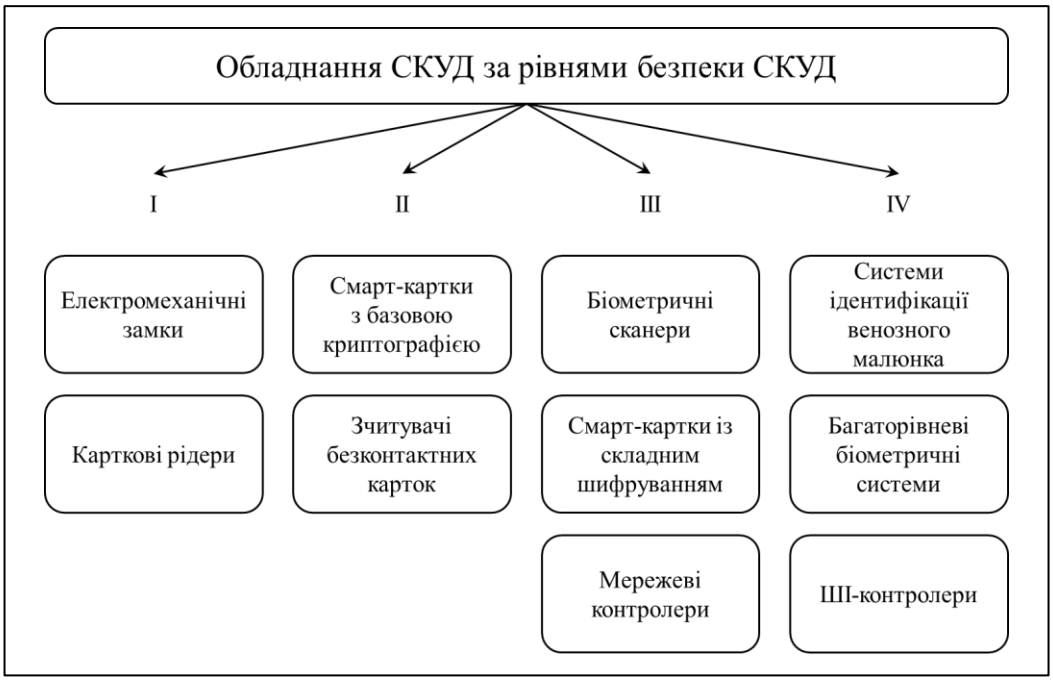

Рисунок 1.4 – Класифікація рівнів безпеки

Обладнання I рівня безпеки застосовують у житлових будинках, невеликих офісних приміщеннях, об'єкт, де відсутній високий ризик втрати даних чи матеріальних активів. Серед переваг – низька вартість встановлення та обслуговування та простота використання. До недоліків можна віднести низький рівень захисту від вандалізму та злому та вразливість до підробки або втрати ідентифікаторів.

Обладнання II рівня безпеки забезпечує середній рівень захисту, підходить для об'єктів із помірними вимогами до безпеки.

Серед прикладів такого обладнання – и смарт-картки з базовою криптографією та зчитувачі безконтактних карток. Вони підтримують базову авторизацію користувачів, оброблюють дані локально або мережно, а також виявляють обмежену стійкість до підробки карток. Обладнання I рівня безпеки використовують для малого та середнього бізнесу, шкіл та освітніх закладів, складських приміщень із середньою цінністю майна [8].

Їхніми перевагами є баланс між вартістю та рівнем захисту та можливість інтеграції з іншими системами автоматизації будівель. Серед

недоліків – обмежений рівень захисту від складних атак і можливість втрати або клонування карток.

Обладнання III рівня безпеки забезпечує високий рівень безпеки для критичних об’єктів. Ці системи інтегрують різні технології ідентифікації для забезпечення багаторівневого захисту. До такого обладнання належать біометричні сканери (відбитки пальців, розпізнавання обличчя), смарт-картки із складним шифруванням, мережеві контролери з обробкою даних у реальному часі.

Таке обладнання підтримує багаторівневий доступ (комбінація карток і біометрії), є стійким до зовнішнього втручання, включно з криптографічним захистом даних та здатне до інтеграції з відеоспостереженням. Його використовують банки та фінансові установи, аеропорти та транспортні вузли та промислові об’єкти з підвищеним ризиком.

До переваг належать високий рівень захисту від зовнішніх та внутрішніх загроз і гнучкість у налаштуванні доступу для різних груп користувачів. Недоліками можна вважати високу вартість встановлення та обслуговування та складність в адмініструванні для непідготовлених користувачів.

Обладнання IV рівня безпеки призначене для стратегічно важливих об'єктів, де безпека має критичне значення. Прикладами є системи ідентифікації венозного малюнка, багаторівневі біометричні системи. контролери із застосуванням штучного інтелекту для аналізу поведінкових ознак.

Воно характеризується інтеграцією з хмарними платформами для централізованого моніторингу, реалізацією адаптивної ідентифікації на основі поведінкових моделей та використанням блокчейн-технологій для збереження даних про доступ. Обладнання IV рівня безпеки застосовується для об’єктів оборонної промисловості, урядів та стратегічно важливих інфраструктурних об’єктів і дослідницьких центрів з високим рівнем конфіденційності.

Перевагами є максимальний рівень безпеки, можливість інтеграції з іншими системами захисту та здатність до адаптації до нових загроз у

реальному часі. Серед недоліків – надзвичайно висока вартість реалізації та складність обслуговування та необхідність залучення висококваліфікованого персоналу.

Рівні безпеки обладнання СКУД відображають еволюцію технологій та їхню адаптацію до потреб користувачів. Кожен рівень має свої переваги та обмеження, що визначаються сферами застосування, технічними характеристиками та ризиками. У сучасному світі системи III та IV рівнів стають дедалі популярнішими через зростаючі загрози безпеці, водночас рівні I та II залишаються актуальними для невеликих об'єктів із помірними вимогами до захисту.

Таким чином, технічні характеристики СКУД визначають їхню функціональність, надійність та ефективність у забезпеченні безпеки. Кожен компонент системи повинен бути адаптований до специфічних умов експлуатації, а інтеграція всіх елементів у єдину архітектуру є критичним фактором для успішної роботи системи.

1.5 Класифікація систем СКУД

Системи контролю та управління доступом (СКУД) класифікуються за кількома ключовими параметрами, які визначають їхню функціональність, масштаби застосування, рівень інтеграції, способи ідентифікації користувачів та рівень безпеки. Така класифікація дає можливість чітко розуміти особливості кожного типу системи й обирати оптимальне рішення залежно від потреб об'єкта (рисунок 1.5).

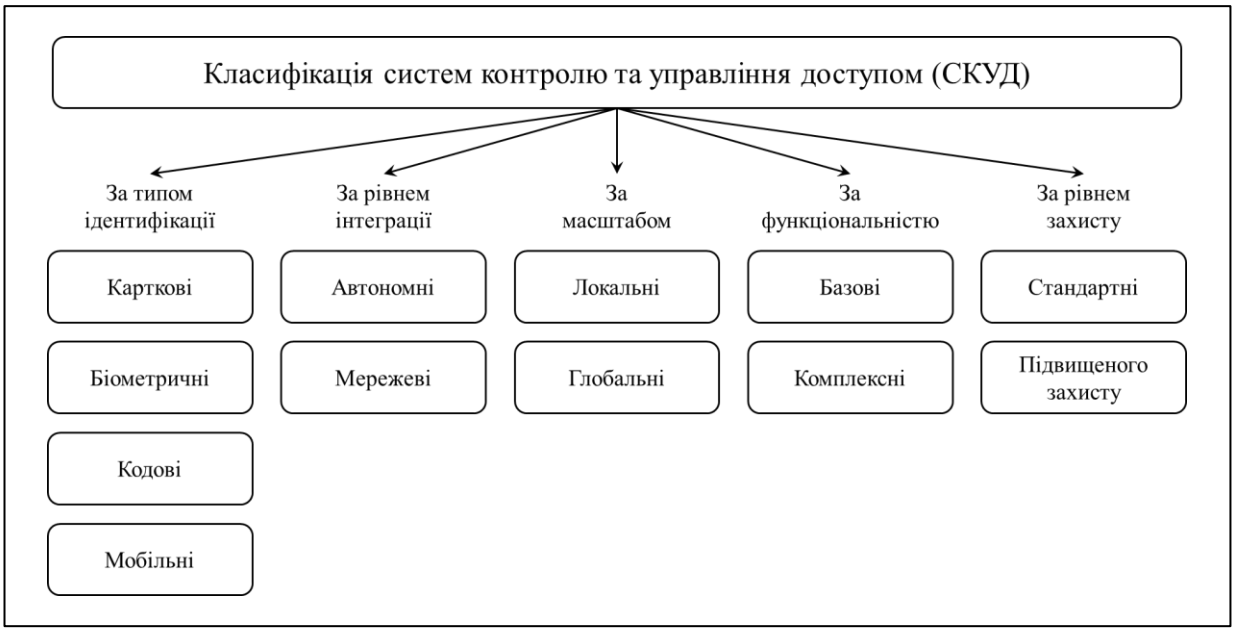

Рисунок 1.5 – Класифікація СКУД

Один із найважливіших критеріїв класифікації СКУД – тип ідентифікації, який визначає спосіб розпізнавання користувача. Традиційно використовуються карткові системи, в яких основним ідентифікатором є фізична картка з RFID-чипом, магнітною смугою або контактним чипом. Вони є зручними та простими в експлуатації, але мають обмеження, такі як вразливість до втрати картки. Новітні технології пропонують біометричні системи, які використовують унікальні фізичні характеристики людини — відбитки пальців, райдужку ока чи риси обличчя. Вони забезпечують найвищий рівень захисту, але потребують значних інвестицій у впровадження. Альтернативою є кодові системи, що базуються на введенні PIN-кодів, та мобільні системи, які використовують смартфони чи спеціальні додатки як ключ доступу. Останні набувають популярності завдяки інтеграції зі смарт-пристроями та високій зручності використання 10.

Інший важливий аспект — рівень інтеграції. Автономні СКУД працюють локально, без підключення до мережі чи центрального сервера, що робить їх ідеальними для невеликих об'єктів із базовими вимогами до безпеки. Даний тип систем застосовується у банківській сфері, для обмеження доступу

до банкоматів, в адміністративних, освітніх та суспільних закладах, приватних будинках.

Основними характеристиками автономних СКУД є:

– самостійне керування роботою периферійних елементів та контроль точки доступу.

– основна функція – обмеження доступу до об’єктів, що контролюються.

– можливість інтеграції системи антискрімінгу, що дозволяє запобігти несанкціонованим діям зловмисників.

Недоліком такого типу СКУД є обмежена функціональність. Натомість мережеві системи пропонують централізоване управління, масштабованість та інтеграцію з іншими системами, такими як відеоспостереження або облік робочого часу. Це дозволяє контролювати доступ у реальному часі, навіть на великих підприємствах із багатьма філіями. Даний тип СКУД використовується на великих промислових або офісних об’єктах з великою кількістю робітників та відвідувачів.

До характеристик мережевих систем належать:

– можливість контролювати присутність та пересування працівників на робочих місцях, обмежувати доступ до об’єктів за часом, розподіляти зони доступу, оперативно вносити зміни та додавати нові функції;

– одночасне керування значною кількістю пунктів пропуску;

– необхідність розробки програмного забезпечення для бази даних, що містить картку кожного працівника, яка включає фотографію та особисті дані;

– управління великою кількістю точок доступу та з’єднує всі контролери з керуючим комп’ютером.

З точки зору масштабів застосування, СКУД можна поділити на локальні та глобальні. Локальні системи охоплюють один об’єкт, забезпечуючи контроль доступу до його окремих зон. Вони характеризуються простотою установки та низькими витратами. Глобальні системи охоплюють кілька об'єктів і створюють єдину інфраструктуру безпеки, що підходить для

корпорацій чи урядових установ. Вони потребують складного серверного обладнання й ретельного налаштування, але забезпечують централізований моніторинг і аналітику.

Ще одним аспектом є функціональність системи. Базові СКУД виконують лише функцію контролю доступу, зосереджуючись на захисті об'єкта від несанкціонованого проникнення. Вони є бюджетними та доступними, однак не враховують потреби в аналітиці чи обліку робочого часу. Комплексні системи інтегруються з іншими інструментами управління, наприклад, відеоспостереженням, пожежною сигналізацією чи ERP-системами, створюючи багаторівневу інфраструктуру безпеки.

Рівень безпеки, який забезпечують СКУД, також є критерієм класифікації. Стандартні системи підходять для об’єктів із низькими ризиками, забезпечуючи базовий контроль доступу. Для об'єктів із високими вимогами до безпеки (наприклад, банки, лабораторії чи військові об'єкти) використовуються системи підвищеного захисту, що включають багаторівневу автентифікацію, шифрування даних і захист від кібератак.

В основі класифікації також можуть бути технічні характеристики та функціональні можливості системи. СКУД варіюються за кількістю точок доступу, які вони здатні контролювати. Це може бути одна точка (наприклад, двері до офісу) або безліч місць у рамках великого підприємства чи корпорації. Параметр пропускної здатності визначає, наскільки швидко система може обробляти ідентифікацію користувачів. Висока пропускна здатність необхідна в місцях із великим потоком людей, наприклад, на вокзалах або стадіонах. У залежності від типу системи, вона може підтримувати від кількох десятків до сотень тисяч записів у базі даних. Залежно від середовища використання та умов експлуатації, СКУД можуть працювати у приміщеннях із різними кліматичними умовами, на відкритих територіях або у складних умовах (висока вологість, запиленість, вібрації тощо).

За рівнем ідентифікації доступу системи поділяються на:

– одноріневі системи, де ідентифікація проводиться за однією ознакою, наприклад, введенням PIN-коду або зчитуванням карти. Ці системи прості, але менш надійні, оскільки втрачена картка чи викритий код можуть бути використані зловмисниками;

– багаторівневі системи, які використовують кілька ознак ідентифікації (наприклад, комбінацію карти та біометричних даних). Вони значно підвищують рівень безпеки, але вимагають більш складного технічного оснащення та налаштування;

Ця класифікація дозволяє вибрати систему, яка найкраще відповідає потребам конкретного підприємства, враховуючи його розміри, бюджет, організаційні процеси та потенційні загрози. У сучасних умовах ключовими трендами є розвиток біометричних та мобільних систем, інтеграція СКУД у загальну IT-інфраструктуру компаній та підвищення кібербезпеки.

1.6 Основні компоненти СКУД

Системи контролю і управління доступом (СКУД) складаються з ряду компонентів, кожен з яких виконує специфічну функцію для забезпечення безпеки, автоматизації та інтеграції з іншими системами. Основними складниками є перегороджувальні пристрої, зчитувальні пристрої, контролери, програмне забезпечення, додаткове обладнання, а також інші допоміжні компоненти, які забезпечують функціональність і надійність системи [9].

Перегороджувальні пристрої (ПП) є фізичним бар’єром між об'єктом і зовнішнім середовищем, який забезпечує обмеження доступу та контроль над переміщенням. Вони включають турнікети, шлагбауми, електромеханічні та електромагнітні замки, а також поворотні брами (рисунок 1.6).

Рисунок 1.6 – Приклади перегороджувальних пристроїв (ПП)

Турнікети, наприклад, можуть забезпечувати прохід до 30 осіб на хвилину, що робить їх придатними для зон з високою інтенсивністю руху, таких як аеропорти чи метрополітени. Електромагнітні замки, які зазвичай мають утримувальну силу до 500–1200 кг, є ефективними у забезпеченні захисту дверей і шлюзів, при цьому їх надійність залежить від стабільності енергопостачання.

Ідентифікатори є ключовими елементами систем контролю і управління доступом (СКУД), які забезпечують ідентифікацію користувачів для надання або обмеження доступу до об'єктів. Вони існують у різних формах, залежно від технологічних підходів, ступеня захисту, швидкості ідентифікації та специфічних потреб системи. Основними типами ідентифікаторів є фізичні, біометричні, цифрові та багатофакторні.

Фізичні ідентифікатори включають картки, брелоки та інші носії з унікальними кодами. Найпоширенішими є RFID-картки, які працюють у низькочастотному діапазоні (125 кГц) або високочастотному діапазоні (13,56 МГц). Високочастотні картки, такі як стандарт MIFARE Classic, мають обсяг пам'яті до 4 КБ, що дозволяє зберігати додаткову інформацію, наприклад, про

доступні зони. RFID-картки забезпечують дальність зчитування до 1 метра залежно від потужності антени зчитувача, проте їх недоліком є можливість копіювання, якщо не застосовуються додаткові заходи захисту, такі як шифрування даних. Брелоки мають аналогічні характеристики, але їх часто використовують як зручніший варіант для носіння.

Біометричні ідентифікатори ґрунтуються на унікальних фізіологічних або поведінкових характеристиках особи (рисунок 1.7). Відбитки пальців є найбільш поширеним методом, оскільки кожна особа має унікальний візерунок папілярних ліній. Сучасні сенсори забезпечують роздільну здатність 500–1000 точок на дюйм, що дозволяє досягати точності до 99,99% у визначенні особи. Розпізнавання обличчя використовує алгоритми комп'ютерного зору та нейронних мереж. Наприклад, сучасні системи на базі моделей глибокого навчання можуть ідентифікувати особу за менш ніж 0,5 секунди, навіть у складних умовах освітлення або з частковим перекриттям обличчя. Розпізнавання райдужної оболонки ока має найвищу точність серед біометричних методів, із рівнем хибного прийняття (FAR) на рівні 0,0001%. Однак цей метод вимагає дорожчого обладнання, що обмежує його масове використання.

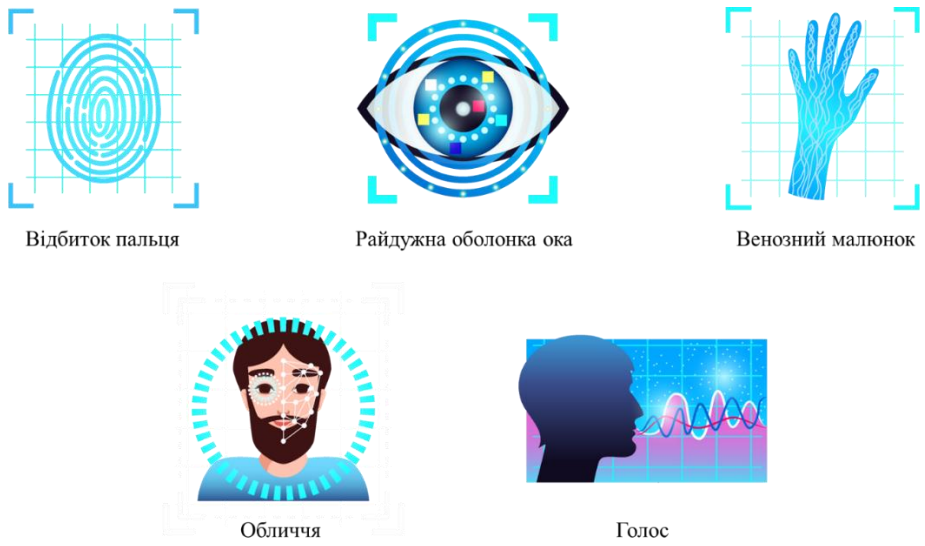

Рисунок 1.7 – Приклади біометричних ідентифікаторів

Цифрові ідентифікатори представляють собою коди або цифрові ключі, що зберігаються у мобільних додатках, смарт-картках або інших цифрових пристроях. QR-коди, наприклад, є популярним рішенням завдяки простоті використання і здатності кодувати до 4296 символів. Смартфони зі встановленими додатками для генерації одноразових кодів доступу (наприклад, Google Authenticator) дозволяють підвищити безпеку, використовуючи алгоритми TOTP (Time-Based One-Time Password). Цифрові ідентифікатори також підтримують шифрування, що унеможливлює їх перехоплення у процесі передачі.

Багатофакторні ідентифікатори поєднують кілька методів для забезпечення додаткової безпеки. Наприклад, система може вимагати як фізичний носій (RFID-картка), так і біометричну верифікацію (відбиток пальця). Це значно знижує ймовірність несанкціонованого доступу, оскільки зловмисник повинен подолати кілька рівнів захисту. Багатофакторні методи є особливо популярними в об'єктах з підвищеними вимогами до безпеки, таких як банківські установи чи дата-центри.

У такий спосіб ідентифікатори СКУД представляють собою широкий спектр технологій, кожна з яких має свої переваги та обмеження. Вибір відповідного типу ідентифікатора залежить від специфіки об'єкта, кількості користувачів, рівня загроз і доступного бюджету. Інтеграція різних типів ідентифікації у багатофакторні системи стає все більш актуальною тенденцією, яка дозволяє поєднувати зручність, точність і безпеку.

Контролери є центральними елементами систем контролю і управління доступом (СКУД), які виконують функції обробки даних, прийняття рішень щодо доступу та управління периферійними пристроями. Типи контролерів можна класифікувати залежно від їх архітектури, функціональності, способу підключення та можливостей інтеграції. Основні типи включають автономні, мережеві, гібридні та спеціалізовані контролери, кожен із яких має специфічні характеристики і застосування.

Автономні контролери є найбільш базовим типом, що працює незалежно від центрального сервера. Вони підходять для невеликих об'єктів із обмеженою кількістю точок доступу, наприклад, офісів або складів. Такі пристрої зазвичай оснащені вбудованою пам’яттю для зберігання даних про 500–5000 користувачів і можуть підтримувати прості механізми авторизації, такі як RFID-карти або PIN-коди. Наприклад, автономний контролер з обсягом пам’яті 32 КБ може обробляти до 20 000 подій у реальному часі. Одним із обмежень є відсутність можливості масштабування та інтеграції з іншими системами, що робить цей тип менш придатним для великих або комплексних об'єктів.

Мережеві контролери є більш складними пристроями, що працюють у зв'язці з центральним сервером через TCP/IP або інші мережеві протоколи. Цей тип контролерів забезпечує високу гнучкість, масштабованість і можливість інтеграції з іншими системами, такими як відеоспостереження, пожежна сигналізація або ERP-системи. Наприклад, мережевий контролер із пропускною здатністю 100 Мбіт/с може одночасно обробляти до 50 000 користувачів і кілька тисяч подій за секунду. Завдяки підтримці протоколу OSDP такі контролери дозволяють встановлювати шифровані канали зв’язку, що підвищує загальний рівень безпеки системи. Їх використання є оптимальним для об'єктів із великою кількістю точок доступу, таких як торгові центри, університети чи промислові підприємства.

Гібридні контролери поєднують можливості автономних і мережевих пристроїв, забезпечуючи як локальну обробку даних, так і віддалене управління через мережу. Цей тип підходить для об'єктів середнього розміру або розподілених систем, де окремі підрозділи повинні функціонувати незалежно у випадку втрати зв'язку з сервером. Наприклад, гібридний контролер з двоядерним процесором ARM Cortex-A53 може забезпечувати обробку даних для 10 000 користувачів у локальному режимі, одночасно синхронізуючи дані з сервером після відновлення зв'язку. Особливо

корисними є такі пристрої в ситуаціях, коли потрібна висока надійність і відмовостійкість системи.

Спеціалізовані контролери призначені для виконання конкретних завдань і часто інтегруються з іншими технологіями, такими як біометричні системи або системи обліку робочого часу. Наприклад, контролери, розроблені для інтеграції з системами розпізнавання обличчя, можуть мати вбудовані графічні процесори для обробки зображень у реальному часі. Такі пристрої здатні аналізувати до 10 000 зображень за секунду з точністю до 99,9%. Іншим прикладом є контролери для об'єктів критичної інфраструктури, які підтримують двофакторну аутентифікацію та резервне живлення для забезпечення безперервної роботи в умовах перебоїв з електропостачанням.

Різноманітність типів контролерів СКУД дозволяє вибирати оптимальне рішення залежно від вимог об'єкта, його масштабу, рівня безпеки та можливостей інтеграції. Розвиток технологій, зокрема впровадження машинного навчання та хмарних обчислень, сприяє підвищенню продуктивності та функціональності сучасних контролерів, розширюючи їхнє застосування у різних сферах.

Програмне забезпечення (ПЗ) забезпечує адміністрування системи, моніторинг та аналіз подій. Типовий програмний модуль дозволяє створювати бази даних користувачів, управляти доступом у реальному часі, а також інтегрувати систему з іншими елементами інфраструктури, такими як відеоспостереження чи системи обліку робочого часу. Сучасне ПЗ, наприклад, може обробляти понад 10 000 запитів доступу одночасно, забезпечуючи швидкість обробки до 100 мс на кожний запит. Важливим є також використання хмарних рішень, які дозволяють управляти доступом дистанційно через веб-інтерфейси або мобільні додатки.

Додаткове обладнання включає блоки живлення, акумуляторні батареї, сирени та індикатори. Наприклад, блоки живлення з резервним акумулятором можуть підтримувати роботу системи до 8 годин у разі перебоїв у

електропостачанні. Сирени з гучністю понад 110 дБ та світлові індикатори використовуються для попередження про спробу несанкціонованого доступу.

До інших компонентів СКУД належать інтеграційні модулі, комутатори, сервери та шифрувальні пристрої. Інтеграційні модулі забезпечують зв'язок з іншими системами, такими як автоматизовані дверні механізми або системи кондиціонування, що активуються на основі подій у СКУД. Сервери з високою продуктивністю дозволяють зберігати великі обсяги даних про доступ і події, тоді як шифрувальні пристрої гарантують безпеку передачі даних між компонентами системи. Наприклад, використання 256-бітного AES-шифрування є стандартом для захисту інформації у сучасних системах СКУД.

Таким чином, компоненти СКУД взаємодіють у комплексній системі, забезпечуючи високу ефективність, безпеку та масштабованість. Технічна досконалість кожного елемента є ключовим фактором у забезпеченні загальної надійності системи.

2 ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ПІДПРИЄМСТВІ

Впровадження системи контролю та управління доступом (СКУД) на підприємстві є складним багатокроковим процесом, який вимагає детального аналізу, планування та інтеграції. Головною метою цього процесу є забезпечення безпеки, контроль доступу до певних зон підприємства, автоматизація процесів і підвищення ефективності управління. Алгоритм впровадження СКУД охоплює аналіз потреб, розробку технічного завдання, вибір і встановлення обладнання, навчання персоналу та забезпечення інтеграції із вже існуючими системами (рисунок 2.1).

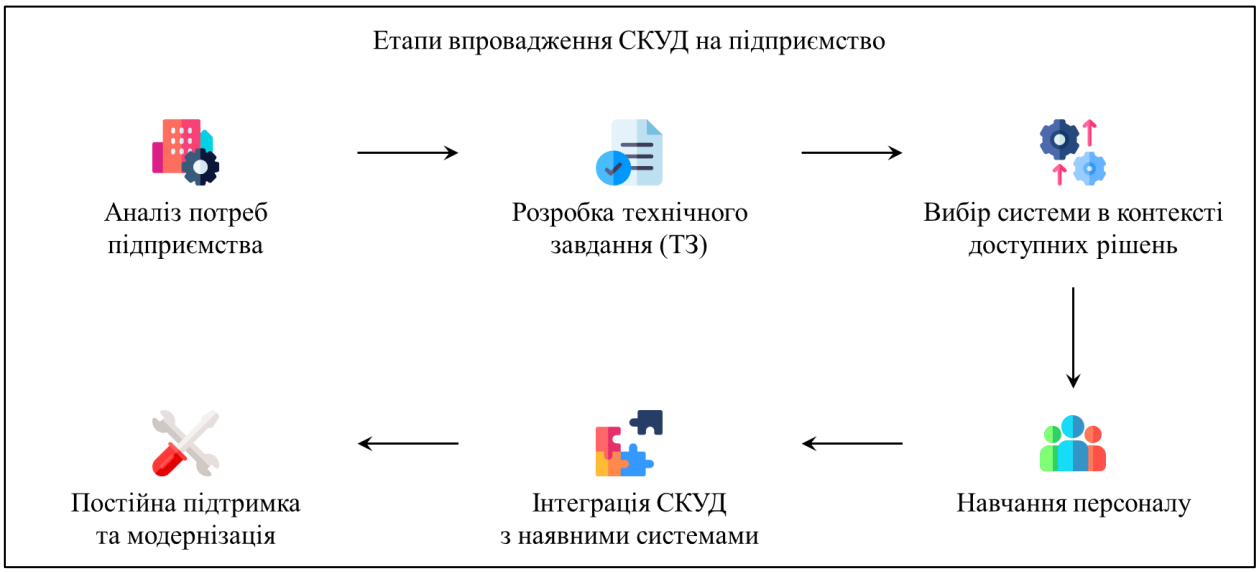

Рисунок 2.1 – Алгоритм впровадження СКУД

Першим етапом є аналіз потреб підприємства. Він містить визначення зон доступу, які потребують контролю, та оцінку потенційних ризиків. Підприємство має враховувати специфіку своєї діяльності, потік співробітників і відвідувачів, а також технічні вимоги. Наприклад, виробничі підприємства можуть потребувати захисту особливо небезпечних зон, тоді як

офіси більше орієнтовані на розмежування доступу між співробітниками та відвідувачами. Важливим аспектом цього етапу є залучення до процесу керівництва, служби безпеки та ІТ-відділу для розробки загальної стратегії.

Наступним кроком є розробка технічного завдання (ТЗ), що формує основу для вибору обладнання та програмного забезпечення. У технічному завданні мають бути чітко прописані вимоги до системи: кількість точок доступу, необхідний рівень ідентифікації, інтеграція з іншими системами безпеки, потреби у звітності тощо. Цей документ також має враховувати специфічні умови експлуатації, наприклад, можливість роботи системи у складних кліматичних умовах або у зонах з високим рівнем запиленості.

На етапі вибору системи проводиться аналіз ринку доступних рішень. Враховуються такі фактори, як технічні характеристики обладнання, його сумісність з існуючими системами, вартість, а також рівень технічної підтримки, яку пропонує постачальник. Наприклад, для об'єктів критичної інфраструктури можуть знадобитися багаторівневі системи з використанням біометричної ідентифікації, тоді як для невеликих офісів достатньо систем із картковим доступом.

Інсталяція обладнання є технічно складним етапом, що включає встановлення фізичних пристроїв (зчитувачів, замків, турнікетів), прокладання кабельних трас та інтеграцію програмного забезпечення. Важливою складовою цього етапу є тестування системи, яке передбачає перевірку її працездатності, надійності і відповідності технічному завданню. Наприклад, тестування може включати перевірку коректності зчитування карток або біометричних даних, симуляцію аварійних ситуацій та аналіз логів доступу.

Навчання персоналу відіграє критично важливу роль у забезпеченні ефективності роботи СКУД. Співробітники служби безпеки повинні отримати навички роботи з системою, включаючи введення нових користувачів, управління правами доступу та реагування на можливі інциденти. ІТ-відділ

також повинен бути ознайомлений із технічними аспектами підтримки системи.

Інтеграція СКУД із вже існуючими системами є фінальним етапом. Сучасні СКУД можуть бути об’єднані з відеоспостереженням, пожежною сигналізацією, ERP-системами та іншими корпоративними рішеннями. Це дозволяє створити єдину платформу управління безпекою, яка забезпечує зручність моніторингу та координації дій.

Після впровадження системи важливо забезпечити її постійну підтримку та модернізацію. Це включає регулярне оновлення програмного забезпечення, перевірку обладнання та аналіз ефективності роботи системи. Наприклад, підприємства можуть періодично проводити аудит доступів для виявлення потенційних слабких місць або перегляду політик доступу у зв’язку зі змінами у структурі організації.

Таким чином, впровадження СКУД на підприємстві є багатогранним процесом, який вимагає міждисциплінарного підходу, технічної компетентності та стратегічного планування. Правильно реалізована система не лише забезпечує високий рівень безпеки, а й оптимізує управлінські процеси, створюючи нові можливості для контролю та аналізу.

2.1 Визначення потреб підприємства

Система контролю і управління доступом (СКУД) є ключовим інструментом забезпечення безпеки та ефективності функціонування сучасних підприємств. Перед встановленням такої системи необхідно ретельно проаналізувати потреби організації (рисунок 2.2), щоб вибрати найбільш оптимальне обладнання та забезпечити інтеграцію з існуючими бізнес-процесами [10]. У цьому тексті розглянемо основні потреби підприємств, як вони впливають на вибір СКУД, та проаналізуємо приклади з різних сфер

діяльності. Забезпечення безпеки – одна з головних причин встановлення СКУД – це потреба у забезпеченні безпеки об’єкта. Це включає захист від несанкціонованого доступу до приміщень, захист матеріальних цінностей, а також забезпечення безпеки співробітників. Для банків, наприклад, важливо контролювати доступ до сховищ, серверних кімнат та зон обслуговування клієнтів. У таких випадках потрібна система з біометричними ідентифікаторами або смарт-картками, яка дозволяє вести детальний облік входу та виходу.

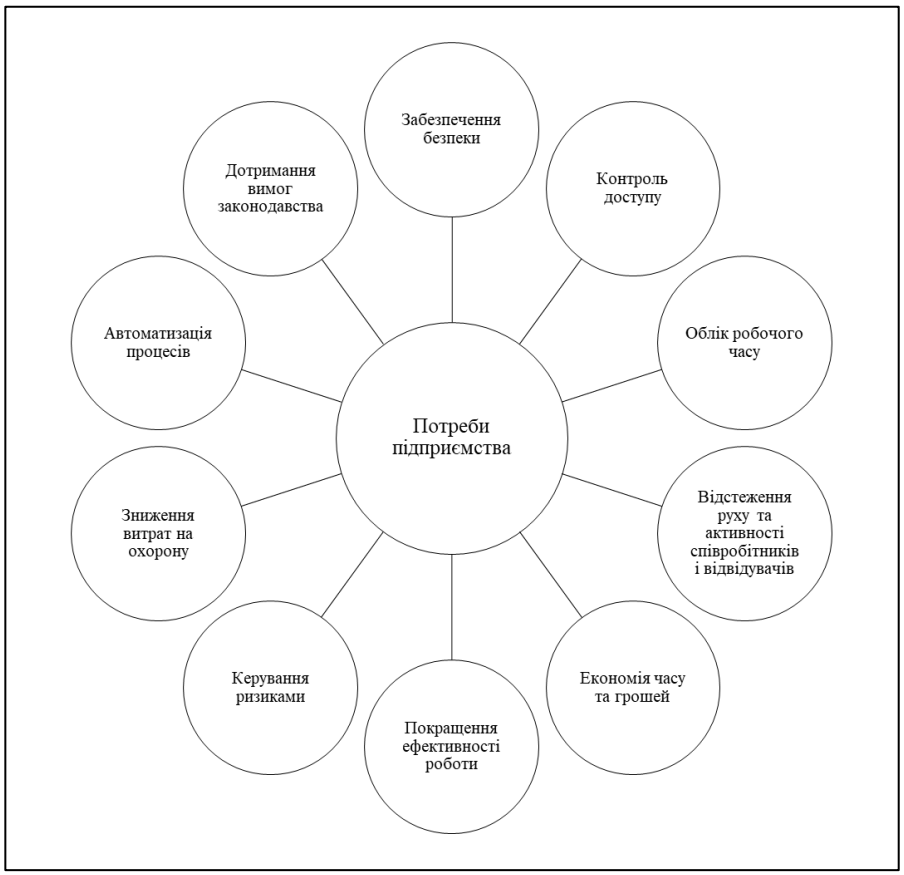

Рисунок 2.2 – Потреби підприємства, які впливають на вибір СКУД

Контроль доступу – СКУД забезпечує точний контроль за тим, хто, коли і куди має доступ. Для аеропортів, де безпека є критично важливою, необхідно розподіляти рівні доступу між працівниками різних служб: обслуговування літаків, митний контроль, адміністративний персонал. У таких випадках

використовують багаторівневі системи доступу з інтеграцією відеоспостереження.

Облік робочого часу – автоматизація обліку робочого часу допомагає підприємствам відстежувати години, проведені співробітниками на роботі, і запобігати порушенням трудової дисципліни. На харчових виробництвах, де важливий контроль за дотриманням санітарних норм, СКУД можуть бути інтегровані з дезінфекційними станціями для обов’язкового проходження співробітників.

Відстеження руху та активності співробітників і відвідувачів – СКУД дозволяють реєструвати пересування співробітників і відвідувачів, що важливо для розслідування інцидентів та оптимізації процесів. У готелях, наприклад, системи можуть забезпечувати доступ до номерів за допомогою індивідуальних ключ-карт, фіксуючи всі дії гостей і персоналу.

Економія часу та грошей – СКУД зменшують потребу у фізичній охороні, автоматизуючи процеси контролю доступу. Для невеликих офісів це може бути простий домофон із функцією відео, тоді як для великих заводів потрібні масштабні мережеві системи. Економія коштів відбувається за рахунок мінімізації людського фактора та скорочення витрат на охорону.

Покращення ефективності роботи – ефективна СКУД може бути інтегрована з ERP-системами для автоматичного оновлення даних про працівників і контроль робочого процесу. У сучасних IT-компаніях, де важливим є захист інтелектуальної власності, такі системи інтегрують із програмами для моніторингу використання робочих місць.

Керування ризиками – СКУД дозволяють знижувати ризики витоку інформації та інших загроз. Для фармацевтичних підприємств це включає доступ до виробничих приміщень лише уповноважених осіб, що зменшує ймовірність помилок або навмисних порушень у виробництві 12.

Зниження витрат на охорону – автоматизація процесів, пов'язаних з доступом, зменшує необхідність у великій кількості охоронців. Наприклад, на

складах роздрібних мереж можна застосовувати турнікети з RFID-ідентифікаторами, які зменшують кількість необхідного персоналу охорони.

Автоматизація процесів та дотримання вимог законодавства – СКУД забезпечують відповідність законодавчим нормам, зокрема у сфері захисту персональних даних. Для медичних установ це може бути важливо у контексті обмеження доступу до зон зберігання медичних препаратів.

Потреби кожного підприємства визначають тип системи, яку необхідно встановити. Вибір залежить від кількості працівників, рівня безпеки, необхідності інтеграції з іншими системами. У банках потрібні системи з високим рівнем шифрування даних, тоді як у торгових центрах акцент робиться на простоті використання клієнтами. Для виробничих підприємств важлива стійкість обладнання до екстремальних умов, наприклад, до пилу чи вологи.

Ретельний аналіз потреб перед встановленням СКУД дозволяє не лише забезпечити безпеку, а й підвищити ефективність роботи підприємства, скоротити витрати та автоматизувати бізнес-процеси.

2.2 Розробка технічного завдання (ТЗ) для впровадження СКУД

Розробка технічного завдання (ТЗ) для системи контролю і управління доступом (СКУД) є одним із ключових етапів впровадження цієї системи, оскільки саме на цьому етапі визначаються основні вимоги, функціональні можливості, архітектура системи та інші аспекти, необхідні для її створення. ТЗ виступає основним документом, який регламентує технічні, організаційні та експлуатаційні характеристики СКУД, а також служить базою для оцінки якості виконання проєкту.

Процес розробки технічного завдання починається з детального аналізу об'єкта, для якого планується впровадження СКУД, та визначення вимог. Цей

аналіз включає оцінку архітектурних, інженерних та організаційних особливостей об'єкта, визначення кількості входів і виходів, що потребують контролю, а також оцінку типу об'єкта (офіс, виробничий комплекс, склад тощо). На цьому етапі враховуються специфічні потреби замовника, такі як необхідність інтеграції з іншими системами, включаючи відеоспостереження, системи охоронної сигналізації або програмне забезпечення для управління персоналом.

Важливим є аналіз мережевого трафіку, оскільки СКУД інтегрується із сервером, де передаються дані. Для визначення необхідної пропускної здатності мережі розраховують трафік:

$$B = \sum_{i=1}^{n} D_i \times R_i, \tag{2.1}$$

де B – загальний обсяг трафіку (біт/с),

D_i – обсяг даних від і-го пристрою (біт),

R_i – частота передачі даних і-го пристрою (разів/с),

n – кількість пристроїв.

Після аналізу проводяться консультації із замовником, щоб уточнити очікування щодо системи. Наприклад, обговорюється рівень безпеки, який повинен забезпечувати СКУД, необхідність ведення архівів подій, кількість користувачів, які матимуть доступ, і можливість розподілу прав доступу за різними критеріями (посада, час доби, день тижня тощо).

На основі отриманої інформації складається перелік функціональних вимог до СКУД. Ці вимоги деталізують, які функції повинна виконувати система: автоматичний облік робочого часу, блокування доступу за певними умовами, створення звітів, інтеграція з іншими системами або навіть управління доступом у реальному часі.

Функціональні вимоги включають також специфікації для апаратного забезпечення (контролери, картрідери, біометричні сканери) та програмного забезпечення (веб-інтерфейс для адміністраторів, мобільні додатки для користувачів). На цьому етапі може бути прийнято рішення про використання специфічних технологій, таких як радіочастотна ідентифікація (RFID), NFC або розпізнавання облич.

Далі розробляється базовий проєкт архітектури майбутньої системи. Він включає визначення компонентів, які будуть використані, їх взаємодію між собою та із зовнішніми системами. У цьому документі визначається, чи буде система централізованою або децентралізованою, які канали зв'язку будуть використовуватися для передачі даних (дротові або бездротові технології), а також способи збереження і обробки даних (локально чи у хмарному середовищі).

Архітектура також передбачає опис заходів з безпеки, таких як шифрування даних, захист від несанкціонованого доступу до мережі та резервування даних для забезпечення безперебійної роботи системи.

На основі зібраної інформації створюється технічне завдання, яке структуровано за чітким планом (рисунок 2.3) і включає всі аспекти, що були визначені під час аналізу. У ТЗ детально описуються:

- загальні положення, включаючи мету створення СКУД, опис об'єкта і ключові вимоги замовника;
- технічні характеристики компонентів системи, їхня сумісність і очікуваний термін служби;
- функціональні можливості системи та критерії, за якими буде оцінюватися її відповідність заданим вимогам;
- вимоги до надійності, безпеки та продуктивності;
- вимоги до монтажу, налагодження та інтеграції;
- вимоги до навчання персоналу і технічної підтримки.

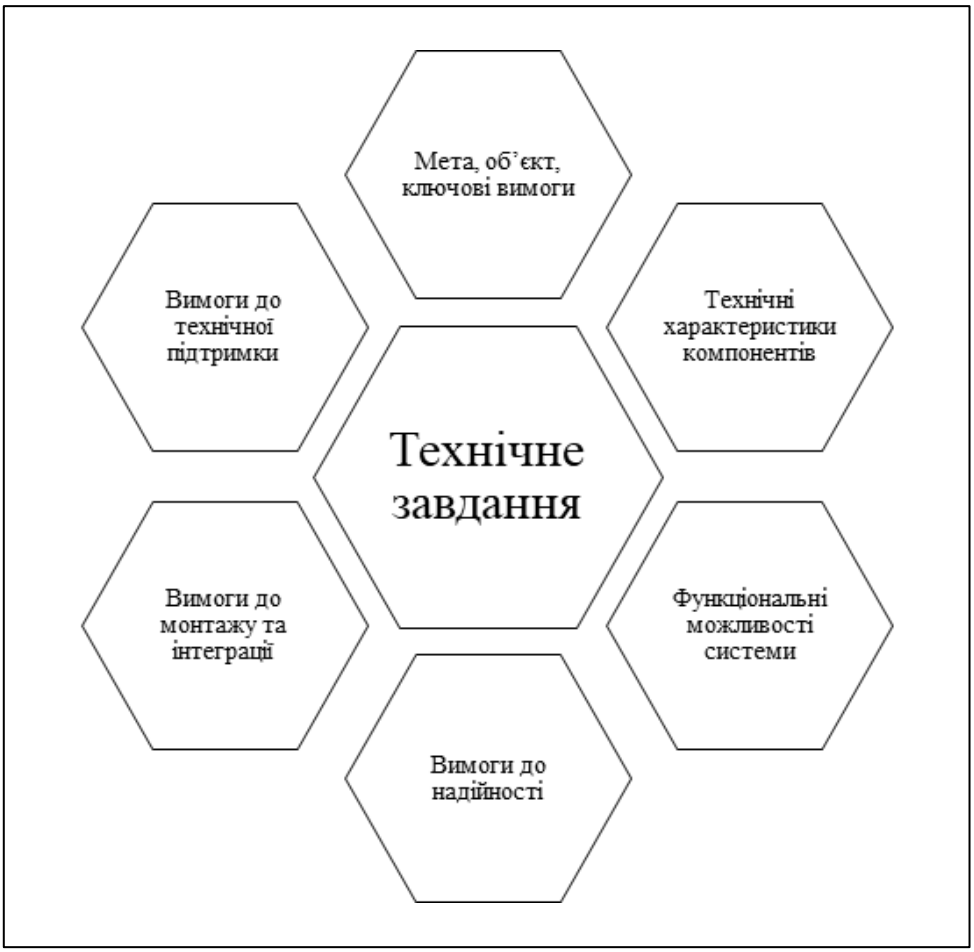

Рисунок 2.3 – Основні компоненти технічного задання

Фінальним етапом є узгодження ТЗ із замовником. Це може включати кілька раундів уточнень і доопрацювань, оскільки замовник повинен переконатися, що всі його потреби враховані. Затверджене ТЗ стає юридично обов'язковим документом, який фіксує взаємні зобов'язання сторін і слугує основою для подальшого проєктування, постачання та впровадження системи.

Розробка ТЗ вимагає комплексного підходу, високого рівня технічної експертизи та тісної співпраці з замовником. Без якісно складеного технічного завдання всі наступні етапи можуть бути ризикованими, оскільки недооцінені вимоги або прорахунки на цьому етапі можуть призвести до перевищення бюджету, затримок у реалізації чи навіть нездатності системи виконувати свої основні функції.

2.3 Вибір системи в контексті доступних рішень

У зв’язку з актуалізацією проблеми безпеки ринок СКУД знаходиться на етапі актиного розвитку та зростання конкуренції. Питання забезпечення безпеки є нагальним як для приватної власності, так і для комерційних приміщень. Сучасні виробники пропонують різні варіанти СКУД, що відрізняються за комплектацією, використаними технологіями та вартістю.

Серед поточних тенденцій можна виділити інтеграцію зі штучним інтелектом, мобільними та хмарними технологіями, машинним навчанням, розвиток та розширенням Інтернету речей (IoT) і біометрії, що дозволяє СКУД більш точно та ефективно виконувати свої функції. У сучасному світі існує декілька основних типів СКУД, кожен із яких має свої особливості, переваги, недоліки та найкращі сфери застосування.

СКУД на основі карток використовують ідентифікаційні карти, що містять унікальний код або електронний чип, для авторизації доступу до приміщень. Вони зазвичай складаються з зчитувачів, що працюють з магнітними, RFID- або смарт-картами. Карти комунікують із зчитувачем через дротові, бездротові або контактні інтерфейси (кабель «вита пара», Bluetooth, NFC, RFID, протокол Wiegand). СКУД на основі карток вирізняються простотою установки та використання, але вони можуть бути вразливими до крадіжки, втрати карт, копіювання чи підробки. Ще одним недоліком є необхідність фізичного контакту, що стало гострою проблемою під час пандемії Covid-19. Вони оптимальні для великих організацій із помірним рівнем безпеки. Такі системи найкраще підходять для корпоративних офісів, де необхідно забезпечити швидкий і простий доступ для багатьох користувачів.

СКУД на основі біометрії застосовують фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, сканування обличчя, сітківки або райдужної оболонки ока, розпізнавання голосу як ключ до

ідентифікації. Біометричні СКУД включають сенсори для зчитування відбитків пальців, сканери обличчя або інших біометричних параметрів, які передають інформацію до системи для порівняння із записаними шаблонами. Комунікація відбувається з допомогою. Вони забезпечують високий рівень безпеки завдяки унікальності фізіологічних характеристик. Біометричні дані неможливо втратити чи передати, проте актуальним залишається ризик підробки. Коректність їхньої роботи може залежати від умов середовища, наприклад, освітлення або стану шкіри. Вартість установки та обслуговування таких систем значно вища, а обробка даних потребує потужного обладнання. Біометричні системи є доречними для об'єктів із високими вимогами до безпеки, таких як банки або дослідницькі центри.

СКУД на основі кодів доступу функціонують через введення спеціального коду на клавіатурі, що відкриває доступ до контрольованої зони. Вони використовують клавіатури для введення персональних кодів, які порівнюються із збереженими в базі даних. Системи на основі кодів доступу є доступними та простими в установці та управлінні. Однак вони мають нижчий рівень безпеки, оскільки коди можуть бути вгадані або передані іншим особам. Складністю у використанні також є ризик забування коду доступу користувачем. Такі системи можуть бути ефективними для невеликих офісів або приватних будинків [11].

Мобільні системи контролю і управління доступом використовують смартфони або інші мобільні пристрої, зокрема через NFC, Bluetooth або мобільні додатки, для аутентифікації (рисунок 2.4). Вони покладаються на мобільні пристрої та використовують технології Bluetooth, Wi-Fi, NFC або мобільну мережу 3G, 4G, 5G для взаємодії з замками чи зчитувачами. Мобільні СКУД зручні завдяки широкому поширенню смартфонів, але вони залежать від стабільності програмного забезпечення і безпеки мобільних мереж. Такі системи стають популярними у готелях і коворкінгах, де користувачі змінюються часто.

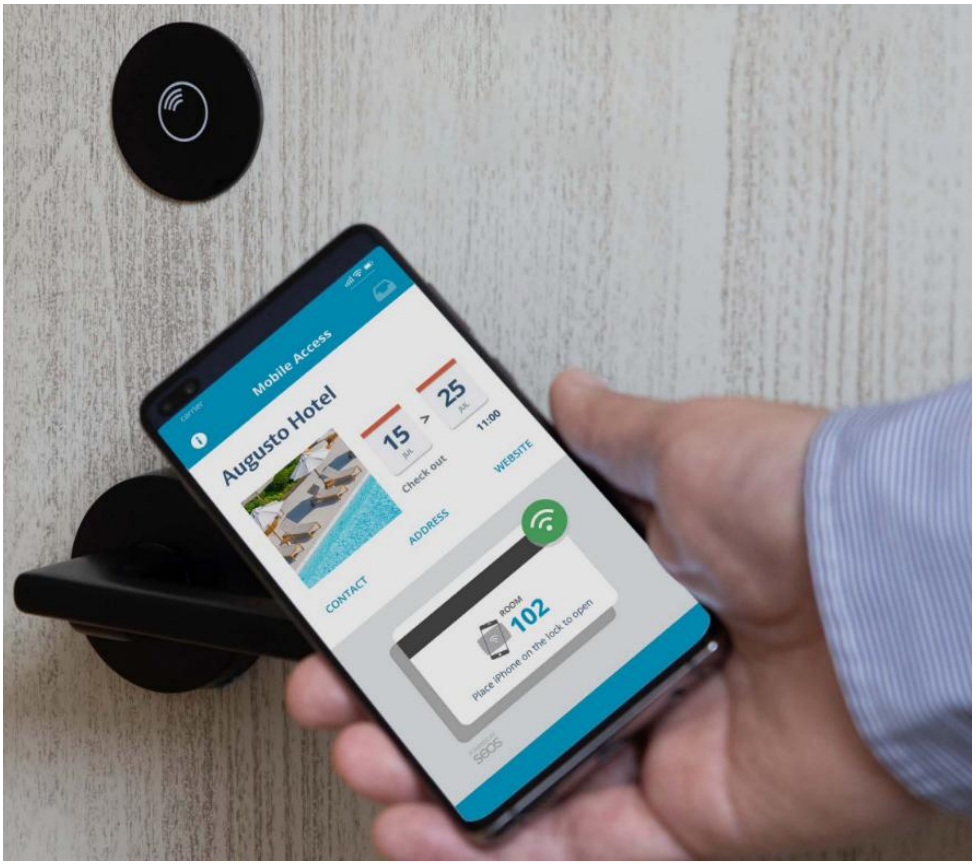

Рисунок 2.4 – Приклад використання мобільної системи в готелі

Інтернет системи контролю і управління доступом інтегруються в хмарні платформи, дозволяючи управління доступом через Інтернет і забезпечуючи віддалений моніторинг. Інтернет СКУД потребують серверів або хмарних платформ для зберігання та обробки даних, а пристрої можуть підключатися через Ethernet, Wi-Fi або мобільні мережі. Інтернет системи дозволяють централізоване управління та віддалений доступ, однак можуть бути вразливими до кібератак, а також вимагають стабільного підключення до Інтернету. Інтернет СКУД є оптимальними для організацій із розгалуженою структурою, таких як мережі магазинів або багатофіліальні компанії.

Гібридні системи об’єднують кілька методів аутентифікації, наприклад, комбінацію карток, біометрії та мобільних технологій, для підвищення рівня безпеки. Комунікація може відбуватися з допомогою низки технологій: Wiegand, Wi-Fi, Bluetooth, NFC, протоколів TCP/IP, HTTP, HTTPS тощо

(рисунок 2.5). Гібридні системи інтегрують різні типи зчитувачів і сенсорів, поєднуючи локальні та мережеві способи комунікації. Гібридні системи є найбільш гнучкими, забезпечуючи високий рівень захисту, але їх складність і вартість можуть бути перешкодою для малих підприємств. Гібридні системи застосовуються на об’єктах із різними рівнями доступу, наприклад, в аеропортах або великих промислових комплексах.

Зважений вибір СКУД із урахуванням специфіки задач забезпечує оптимальне поєднання безпеки, зручності та економічної ефективності.

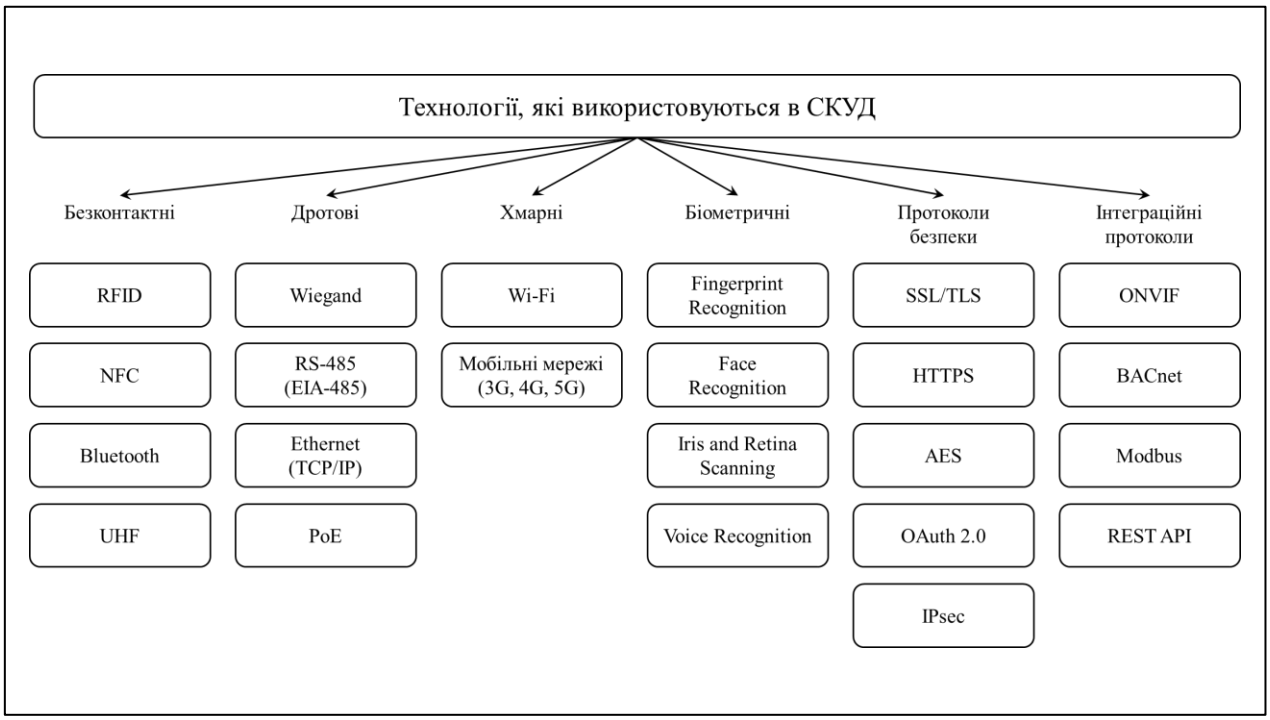

Рисунок 2.5 – Технології комунікації СКУД

Сучасний ринок систем безпеки представлений широким спектром компаній, які пропонують рішення для забезпечення безпеки підприємств та організацій. Серед основних гравців виділяються як міжнародні гіганти з багаторічною історією (Bosch Security System Inc., Honeywell International Inc., Tyco International Ltd., Johnson Controls International plc), так і локальні компанії, що спеціалізуються на індивідуальних рішеннях («Захід-Комп’ютер», «Електронні технології безпеки», «Інтелтех» та Ajax Systems).

Нижче розглянуто переваги та недоліки даних виробників, їхній внесок у галузь і особливості продукції.

У таблиці 2.1 подано характеристику виробників СКУД, включаючи їхню назву, країну походження та особливості.

Таблиця 2.1 – Світові та українські виробники СКУД

Назва	Країни	Особливості
Bosch Security System	Німеччина	Висока якість продукції, інноваційність, високі ціни, обмежена локалізація.
Honeywell International	США	Широкий вибір продукції, інтеграція з іншими системами, надійність; висока вартість, відсутність пробної версії.
Tyco International	Швейцарія	Адаптація до потреб клієнтів, багаторічний досвід; низький рівень технічної підтримки, проблеми з безпекою, висока вартість.
Johnson Controls International	США	Інтегровані рішення, гнучкість, якість; обмежена функціональність для великих підприємств, високі ціни.
Захід-Комп'ютер	Україна	Низькі ціни, індивідуальний підхід; обмежений асортимент.
Електронні технології безпеки	Україна	Високі технічні характеристики, гнучкість; обмежена функціональність для великих підприємств, недостатній міжнародний досвід.
Інтелтех	Україна	Широкий асортимент, індивідуальний підхід; низький рівень технічної підтримки, відсутність безкоштовної пробної версії.
Ajax Systems	Україна	Високі технічні характеристики, інноваційність, простота використання; висока вартість, обмеження для великих підприємств.

Компанія Bosch Security System, заснована у Німеччині в 1886 році, є одним із провідних світових виробників систем безпеки. Її основною перевагою є висока якість продукції, яка відповідає найвищим стандартам надійності та функціональності. Bosch активно впроваджує інноваційні рішення, пропонуючи широкий асортимент продуктів і сервісів. Крім того, стабільність компанії та її технічна підтримка є важливими факторами для багатьох клієнтів. Водночас недоліками є високі ціни, які роблять продукцію менш доступною для малого та середнього бізнесу, а також відсутність української локалізації на деяких продуктах, що може ускладнити інтеграцію для місцевих споживачів.

Американська компанія Honeywell International, заснована в 1906 році, відома своєю високою якістю продуктів і рішень, які забезпечують надійність і безпеку. Її перевагами є широкий вибір продукції, інтеграція з іншими системами та репутація надійного виробника. Проте висока вартість рішень і відсутність пробної версії для тестування обмежують доступність продукції для нових користувачів.

Tyco International зі Швейцарії, заснована в 1960 році, пропонує широкий асортимент рішень, які адаптуються до індивідуальних потреб клієнтів. Її багаторічний досвід дозволяє ефективно впроваджувати розробки. Проте компанія часто отримує негативні відгуки через низький рівень технічної підтримки, що створює труднощі для користувачів. Крім того, питання безпеки продуктів залишається проблематичним, а висока вартість може відлякати потенційних клієнтів.

Johnson Controls International, заснована в США у 1885 році, має значний досвід у розробці систем і пропонує інтегровані рішення для бізнесу. Її продукти вирізняються високою якістю, а компанія відома своєю гнучкістю у задоволенні потреб клієнтів. Однак для великих підприємств функціональність деяких систем є обмеженою, а асортимент продукції менш широкий порівняно з конкурентами. Як і у випадку з іншими міжнародними гравцями, ціни залишаються високими.

Серед українських компаній можна виділити Захід-Комп'ютер, засновану в 1997 році. Вона спеціалізується на розробці власного програмного забезпечення та обладнання, що дозволяє забезпечувати індивідуальний підхід до потреб клієнтів. Її продукція приваблює низькими цінами, але обмежений асортимент і недостатній досвід на міжнародному ринку залишають компанію в тіні міжнародних конкурентів.

Компанія Електронні технології безпеки, заснована у 1994 році, також займається розробкою програмного забезпечення й обладнання. Її рішення вирізняються високими технічними характеристиками та гнучкістю. Однак обмежена функціональність для великих підприємств і недостатній досвід роботи на міжнародному ринку є суттєвими недоліками.

Інтелтех, заснована у 2000 році, пропонує широкий асортимент продуктів і орієнтована на індивідуальні потреби замовників. Проте недоліками є низький рівень технічної підтримки, що може впливати на задоволення клієнтів, а також відсутність безкоштовної пробної версії.

Серед молодих українських компаній особливо виділяється Ajax Systems, заснована в 2011 році. Її продукція характеризується високими технічними характеристиками, інноваційністю та простотою використання. Проте деякі функції недоступні у базовій версії, а висока вартість і обмеження для великих підприємств роблять її рішення менш універсальними.

Аналіз виробників систем безпеки демонструє, що кожен із них має свої унікальні переваги та недоліки. Міжнародні компанії приваблюють якістю та надійністю, але можуть бути менш доступними через високу вартість і недостатню локалізацію.

Українські виробники, навпаки, забезпечують конкурентоспроможні ціни та адаптацію до потреб місцевого ринку, але стикаються з викликами у вигляді обмеженого асортименту та недостатнього досвіду на міжнародній арені. Вибір виробника залежить від конкретних потреб підприємства, бюджету та вимог до функціональності систем.

2.4 Інсталяція обладнання СКУД

Інсталяція обладнання системи контролю і управління доступом (СКУД) є ключовим етапом її впровадження. Вона потребує ретельного планування, точності виконання та дотримання технічних вимог. Основним завданням цього кроку є фізична установка пристроїв та їхнє інтегрування у функціональну систему, що забезпечує контроль доступу до певних зон.

На першому етапі інсталяції здійснюється підготовка об’єкта. Це включає детальну перевірку місць, де буде розміщено обладнання, на предмет відповідності технічним умовам. Монтажні зони повинні мати відповідні характеристики, зокрема міцність стін чи стель, доступ до джерел живлення, а також достатній рівень захищеності від впливу навколишнього середовища. Наприклад, зчитувачі, встановлені на вулиці, мають відповідати стандарту IP65, що забезпечує захист від пилу та води.

Другим кроком є прокладання кабельних трас (рисунок 2.6). Вони забезпечують зв’язок між компонентами системи: контролерами, зчитувачами, замками, датчиками та сервером. Кабельні траси прокладаються із застосуванням спеціальних каналів або труб, що запобігають їх механічному пошкодженню.

Рисунок 2.6 – Спеціальні канали й труби для кабелів

У разі використання мережевих з’єднань для передачі даних, слід дотримуватися вимог до екранування та мінімізації перешкод, серед яких:

- використовувати екрановані кабелі (STP або FTP) для зменшення впливу електромагнітних завад, забезпечити якісне заземлення екрану кабелю на обох кінцях, щоб уникнути накопичення індуктивних струмів, перевірити якість екрану (суцільність та відсутність пошкоджень) під час монтажу;
- прокладати кабелі подалі (мінімальна відстань 30-50 см) від джерел електромагнітних перешкод (електродвигуни, трансформатори, кабелі високої напруги або освітлювальні системи);
- прокладати сигнальні кабелі та кабелі живлення в окремих трасах, уникати перехрещення кабелів під кутом менше 90°;
- надійно заземляти всі металеві конструкції, які використовуються для підтримки кабелів (кабель-канали, лотки), дотримуватися правил організації загальної заземлювальної системи, щоб уникнути різниці потенціалів;
- використовувати високоякісні конектори з металевими корпусами для збереження цілісності екрану, переконатися в щільному з'єднанні кабелю з конектором для забезпечення надійного контакту;
- установлювати EMI-фільтри (фільтри електромагнітних завад) на критичних ділянках, застосовувати захисні обмежувачі напруги (TVS-діоди, варистори) для запобігання впливу імпульсних завад;
- використовувати кабелі з мідними провідниками, які мають низький опір і забезпечують стабільну передачу сигналів;
- після монтажу перевірити якість сигналу за допомогою тестера кабелів або спектроаналізатора, вимірювати рівень перешкод у робочому середовищі та адаптуйте маршрут кабелів, якщо це необхідно;
- у випадках високого рівня електромагнітних завад використовувати оптоволоконних кабелів, які є нечутливими до електромагнітного впливу.

Наступним кроком є монтаж ключових компонентів системи [12]. Спершу встановлюються контролери – основні обчислювальні пристрої, що управляють доступом. Їх розміщують у захищених місцях, часто в спеціальних

монтажних шафах. Далі встановлюються зчитувачі, що забезпечують зчитування ідентифікаційних даних з карт, брелоків або біометричних пристроїв. Розташування зчитувачів має бути зручним для користувачів, наприклад, на висоті близько 1,2-1,5 метра від підлоги.

Варто враховувати оптимізацію розташування пристроїв. Так, під час розташування точок доступу на території підприємства враховують їх кількість та відстань між ними. Середня ефективність охоплення обчислюється як:

$$E = \frac{\sum_{i=1}^{N} A_i}{S} \tag{2.2}$$

де E – ефективність покриття,

A_i – площа покриття точки,

S – загальна площа території,

N – кількість пристроїв.

Після цього встановлюються виконавчі механізми, такі як електромагнітні або електромеханічні замки. Їх монтують безпосередньо на дверях або інших об’єктах, які контролюються. Замки з електромагнітним принципом дії забезпечують високу надійність і простоту експлуатації, тоді як електромеханічні моделі можуть використовуватися для забезпечення аварійного виходу. Особливу увагу приділяють налаштуванню сил зчеплення, що має відповідати стандартам безпеки.

На завершальному етапі монтажу проводиться встановлення серверного обладнання. Це можуть бути фізичні сервери або хмарні рішення. Сервери забезпечують обробку даних, зберігання журналів доступу та інтеграцію з іншими інформаційними системами. Їхня установка передбачає підключення до локальної мережі, налаштування системи безперебійного живлення та забезпечення фізичної безпеки.

Інсталяція СКУД завершуються підключенням усіх компонентів до електромережі та проведенням первинного тестування. На цьому етапі перевіряється функціональність окремих пристроїв, таких як зчитувачі та замки, а також цілісність усієї системи. Усі елементи мають функціонувати у відповідності до проектних вимог. Несправності, які можуть виникнути під час тестування, усуваються, а система проходить контрольну перевірку.

Завершальна фаза включає документування усіх параметрів встановленого обладнання, таких як конфігурації зчитувачів, номери використовуваних кабелів та місця розташування ключових елементів. Ці дані зберігаються у технічній документації та є основою для подальшого технічного обслуговування.

2.5 Навчання персоналу користуванню СКУД

Навчання персоналу під час встановлення системи контролю та управління доступом (СКУД) на підприємстві є критично важливим етапом, що забезпечує ефективне функціонування системи, безпеку інформаційних та фізичних ресурсів, а також оптимізацію операційних процесів. Без належної підготовки співробітників навіть найсучасніша система може стати джерелом помилок, збоїв або навіть серйозних інцидентів безпеки. Тому підхід до навчання повинен бути системним і враховувати різні рівні відповідальності та компетенції співробітників.

Головною метою навчання персоналу під час впровадження СКУД є забезпечення їхньої здатності ефективно використовувати систему відповідно до функціональних обов'язків. Знання принципів роботи, правил експлуатації та можливостей системи зменшує ризики людських помилок, покращує продуктивність і підвищує рівень інформаційної та фізичної безпеки

підприємства. Крім того, це сприяє розвитку культури безпеки, що є невід'ємною частиною сучасного корпоративного середовища.

Навчання персоналу може здійснюватися різними методами, які мають бути адаптовані до рівня підготовки працівників і специфіки їхніх обов'язків:

- інтерактивні лекції та семінари, які надають базові знання про СКУД, її функціональність, основні компоненти та правила експлуатації;
- практичні тренінги, під час яких співробітники мають можливість безпосередньо взаємодіяти з системою, виконувати типові завдання, такі як авторизація, вхід і вихід із зон доступу, реагування на тривожні сигнали;
- електронні навчальні курси для самостійного опанування основних принципів роботи системи;
- симуляції та моделювання інцидентів, що дозволяють відпрацювати дії у разі надзвичайних ситуацій;
- індивідуальні консультації для ключових співробітників, які відповідають за управління доступом або мають розширені повноваження.

Кожна категорія співробітників повинна опанувати специфічний набір навичок відповідно до їхньої ролі в експлуатації СКУД. Наприклад, рядові працівники повинні:

- розуміти основні принципи роботи системи;
- виконувати базові операції, такі як авторизація за допомогою картки доступу, введення PIN-коду або використання біометричних даних;
- знати правила поведінки у разі блокування доступу чи інших збоїв системи.

Менеджери середньої ланки мають додатково:

- аналізувати журнали доступу для моніторингу активності;
- контролювати дотримання політик безпеки у підрозділах;
- координувати дії між службами у разі порушень або технічних проблем.

Для IT-відділу навчання повинно включати:

– глибоке розуміння архітектури СКУД, її апаратних та програмних компонентів;

– навички налаштування системи, включаючи встановлення програмного забезпечення, інтеграцію з іншими корпоративними системами та оновлення прошивки;

– знання процедур резервного копіювання та відновлення даних;

– вміння проводити діагностику збоїв, віддалений моніторинг системи та усунення технічних несправностей.

Служба безпеки є ключовим користувачем СКУД, відповідальним за адміністрування системи та реагування на інциденти. Навчання співробітників цієї служби повинно включати такі аспекти:

– навички введення нових користувачів у систему, включаючи створення облікових записів, реєстрацію карток доступу або біометричних даних;

– управління правами доступу, включаючи створення груп користувачів, налаштування рівнів доступу до різних зон та зміну цих параметрів у разі потреби;

– знання алгоритмів реагування на різні типи інцидентів, таких як несанкціонований доступ, збої обладнання або тривожні сигнали;

– здатність аналізувати дані із системи для виявлення аномальної активності або потенційних загроз;

– проведення інструктажів для інших співробітників щодо безпечного використання системи.

Для забезпечення ефективності навчання важливо розробити структурований навчальний план, який включає теоретичні та практичні заняття, а також регулярні перевірки знань. Співробітники повинні пройти оцінювання на різних етапах навчання, щоб упевнитися в їхній готовності до роботи із системою. Навчання має бути періодичним, з оновленням знань відповідно до змін у системі чи політиках безпеки.

Загалом, успішне впровадження СКУД можливе лише за умови повного залучення персоналу до процесу навчання. Це забезпечує не лише ефективне використання технічних засобів, але й формує відповідальне ставлення до питань безпеки на підприємстві, що є критичним фактором у сучасному бізнес-середовищі.

2.6 Інтеграція СКУД з іншими системами

Інтеграція системи контролю і управління доступом (СКУД) із вже існуючими системами є критично важливим етапом, який забезпечує ефективність та синергію нових рішень з поточною інфраструктурою організації. Цей процес включає кілька ключових аспектів, що охоплюють технічну, організаційну та безпекову складові. Нижче розглянути, як саме відбувається інтеграція СКУД із іншими системами, враховуючи всі необхідні кроки.

Перший етап інтеграції СКУД з наявними системами передбачає комплексний аналіз наявної інфраструктури (рисунок 2.7). Це включає вивчення архітектури систем, які вже функціонують у приміщенні або організації.

Сюди належать мережеві системи, сервери, програмне забезпечення для управління ресурсами (ERP), системи управління безпекою (відеоспостереження, пожежна сигналізація тощо) та HR-платформи, що ведуть облік працівників. Інженери та системні адміністратори вивчають технічні специфікації, протоколи передачі даних, сумісність програмних інтерфейсів (API) та фізичні обмеження (наприклад, типи замків, датчиків і кабелів).

На основі проведеного аналізу розробляється детальний план інтеграції. На цьому етапі визначаються точки взаємодії СКУД з іншими системами,

наприклад, через API, SDK (Software Development Kit) або протоколи інтеграції, такі як BACnet, OPC або OSDP. Крім того, враховуються можливі конфлікти між системами, наприклад, через несумісність форматів даних чи різні рівні доступу.

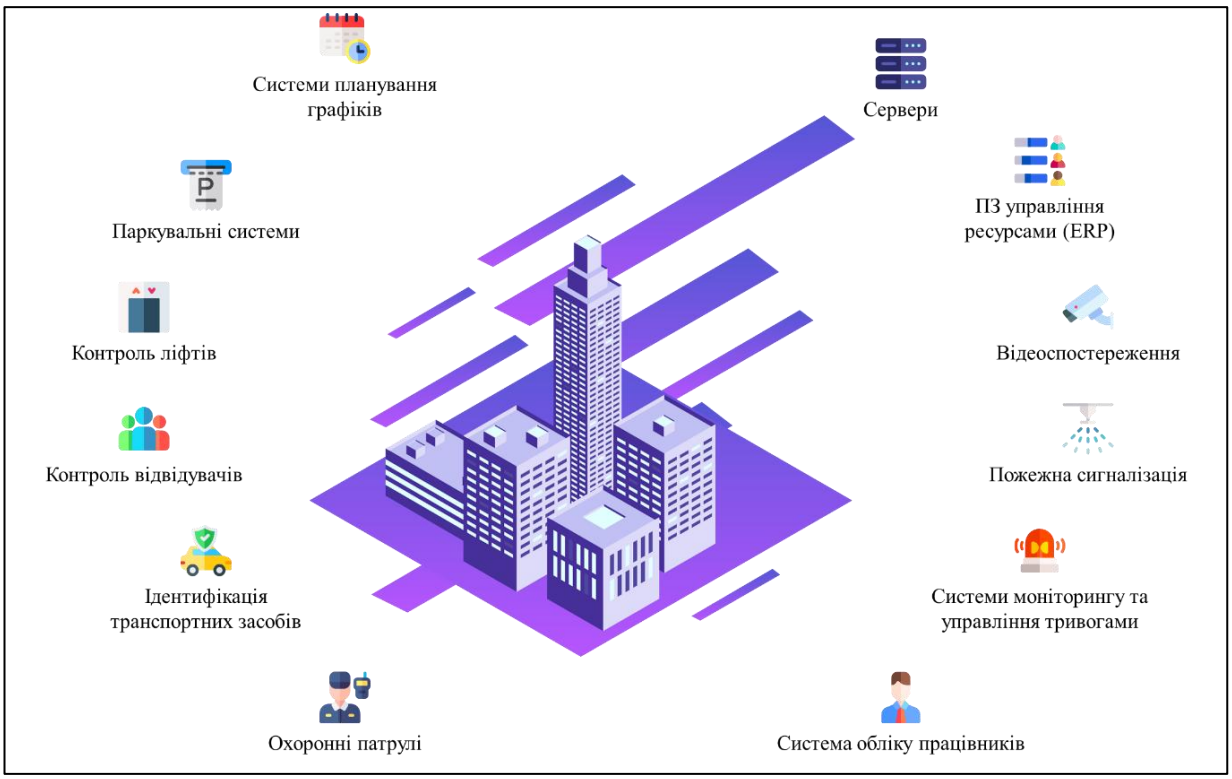

Рисунок 2.7 – Системи, з якими відбувається інтеграція

Розробка стратегії включає створення карти потоків даних між СКУД і цільовими системами. Наприклад, інформація про персонал із HR-системи має бути автоматично доступна в базі СКУД для створення облікових записів співробітників і налаштування прав доступу. Відеоспостереження може синхронізуватися з точками доступу, щоб у разі спрацювання датчика фіксувалися відповідні відеозаписи.

На етапі реалізації інтеграції починається фізичне та програмне з’єднання СКУД із іншими системами. Інженери налаштовують мережеве підключення для передачі даних між компонентами системи. Це може

включати встановлення шлюзів, серверів та інших проміжних пристроїв, необхідних для забезпечення сумісності.

Якщо СКУД працює через хмарну платформу, реалізується інтеграція через відповідні API або протоколи захищеного з'єднання (наприклад, HTTPS). У випадку локального розташування СКУД, підключення може здійснюватися через внутрішню корпоративну мережу або VPN для забезпечення безпеки.

Після інтеграції проводиться комплексне тестування роботи системи. Мета цього етапу — виявити можливі помилки або несумісності. Наприклад, перевіряється, чи коректно передаються дані між СКУД та іншими системами, чи всі датчики та точки доступу працюють відповідно до заданих правил. Тестування охоплює як функціональну перевірку (перевірка окремих компонентів), так і системне тестування (оцінка роботи всіх систем у взаємодії). Особлива увага приділяється сценаріям із підвищеним ризиком, наприклад, спробам несанкціонованого доступу, одночасному великому навантаженню на мережу чи аварійним ситуаціям.

Інтеграція передбачає також підготовку персоналу до роботи із системою. Навчання включає інструкції щодо використання нових функцій, наприклад, управління доступом через інтегровану HR-систему або перегляд подій у реальному часі через систему відеоспостереження. Одночасно створюється технічна документація, яка описує всі аспекти інтеграції: від деталей підключення до інструкцій для адміністратора. Це забезпечує можливість швидкого усунення можливих проблем у майбутньому. Інтеграція СКУД — це не одноразова дія, а тривалий процес. Після запуску системи потрібен моніторинг її роботи для виявлення вузьких місць чи можливих покращень. Наприклад, можна налаштувати більш детальні правила для аналітики відеоспостереження чи підключити нові пристрої.

Отже, інтеграція СКУД із вже наявними системами потребує ґрунтовного аналізу, детального планування, технічної реалізації, тестування, навчання персоналу та постійного супроводу.

3 ЗАХИСТ РОЗПОДІЛЕНИХ СИСТЕМ: ОГЛЯД МЕТОДІВ КОНТРОЛЮ ДОСТУПУ ДЛЯ ХМАРИ, БЛОКЧЕЙНУ, IOT ТА SDN

3.1 Рішення для контролю доступу

У цьому розділі розглянуто різні підходи до контролю доступу (дискреційний, обов'язковий, на основі атрибутів, ролей та політик) разом зі стандартними механізмами впровадження (списки контролю доступу, матриці, списки можливостей) та застосуваннями (групові політики).

Списки контролю доступу (ACL) складаються з правил, які надають або відмовляють у доступі до конкретних ресурсів. ACL управляється одним або декількома елементами керування доступом (ACE), що визначають правила для конкретного користувача або ідентифікатора безпеки. Нові записи зазвичай додаються в кінці ACL. ACL можуть бути впроваджені в різних доменах, наприклад, файлових системах та мережах, через програмні або апаратні рішення, такі як Тригерна контент-адресована пам'ять (TCAM) для прискорення обробки запитів. ACL впроваджуються в різних операційних системах, включаючи популярні Linux та Windows, демонструючи гнучкість як засіб безпеки для систем та інфраструктур.

Файлова система ACL обмежує доступ до файлів і каталогів, вказуючи операційним системам, які користувачі мають право доступу до певних ресурсів і які привілеї надаються користувачам. Файлові системи ACL є ефективним і безпечним захисним механізмом. Коли ACL для файлових систем налаштовані та розгорнуті правильно, вони забезпечують високий рівень захисту даних і підтримуються їх власниками. Крім того, алгоритм перевірки дозволів є досить простим для впровадження та перевірки.

Проте, система сканує ACL під час кожного початкового доступу до об'єкта, що займає більше часу, ніж доступ через запис у матриці управління доступом. Крім того, розуміння того, які файли доступні для суб'єкта, може бути обчислювально дорогим залежно від способу зберігання даних. Таким

чином, якщо суб'єкт покидає систему або змінює роль, може виникнути необхідність пошуку всіх файлів, пов'язаних із цим користувачем.

Мережеві ACL працюють шляхом фільтрації доступу до мережі, вказуючи мережевим пристроям (наприклад, маршрутизаторам і комутаторам), які типи трафіку дозволені і які дії дозволені. Наприклад, ACL може визначати джерело та призначення адреси, протокол зв'язку (UDP або TCP), номери портів тощо. Нещодавно було проведено дослідження інтеграції Software-Defined Networking з Active Directory, з аналізом, як ACL можуть бути використані для забезпечення безпеки в поєднанні з політикою сегментації, що визначається програмним забезпеченням, групуючи статичні та динамічні ACL, пов'язані з трафіком [13]. Існують різні відомі проблеми, такі як складність збереження ACL у конфігураціях пристроїв та можливість їх зміни у разі компрометації пристрою.

Загалом, проблеми з використанням цієї техніки виникають через труднощі адміністраторів мережі в управлінні ACL у складних середовищах. Виділяють дві конкретні проблеми.

1) Сканування ACL іноді проводиться неефективно в лінійний час для кожного вхідного пакету даних.

2) Неефективні або надлишкові правила також можуть з’являтися. Правила вважаються непотрібними, коли вони стосуються пакетів, які не з’являються у реальному трафіку. Правило є непотрібним, коли інші попередні правила вже охоплюють його цільові пакети.

Список можливостей може бути токеном або квитком, що надає доступ суб'єкту до об'єктів у комп'ютерній системі. Суб'єкт оцінюється на основі списку можливостей перед наданням доступу до конкретного об'єкта.

ACL можна узагальнити до матриці управління доступом. Цей механізм реалізується як масив клітинок з колонкою для кожного об'єкта і рядком для кожного суб'єкта [14]. Запис у певній клітинці визначає режим доступу суб'єкта до відповідних об'єктів. Колонка представляє список доступу до об'єкта; рядок еквівалентний профілю доступу суб'єкта (Таблиця 3.1).

Таблиця 3.1 – Матриця управління доступом

Користувач	Файл А	Файл Б	Файл С	Результат
Аліса	RW	R	R	OK
Борис	RW	RW	R	OK
Левко	RW			OK
Павло	R		R	
Віктор			R	OK

Групові політики є функцією операційних систем на основі UNIX та Microsoft Windows, включаючи розподілені середовища, такі як Microsoft Active Directory, які контролюють робоче середовище облікових записів суб'єктів. Групові політики забезпечують централізоване управління та конфігурацію операційних систем, налаштувань користувачів і додатків, що дозволяє ефективно керувати ACL. Групові політики можуть бути використані, коли різні користувачі взаємодіють із системою контролю доступу. Усередині групи користувачі мають спільні дозволи.

На рисунку 3.1 показано можливість адміністратора додавати нову політику до групової політики яка потім реалізується через Active Directory для кількох користувачів, настільних ПК та серверів. Автоматизація для впровадження безпеки Windows у великих і складних сучасних системах створює можливості для зловмисників експлуатувати систему, коли присутня неправильна конфігурація або вразливість. Багато організацій не можуть ефективно контролювати всі аспекти процесу, який залежить від ручної конфігурації ACL і групових політик, з додаванням і видаленням правил у різний час різними адміністраторами системи. Автори представляють концептуальну реалізацію та документацію для автоматизації процесу та виконання перевірок на послідовність, щоб мінімізувати ризик неправильних налаштувань, які можуть бути ненавмисно внесені адміністраторами.

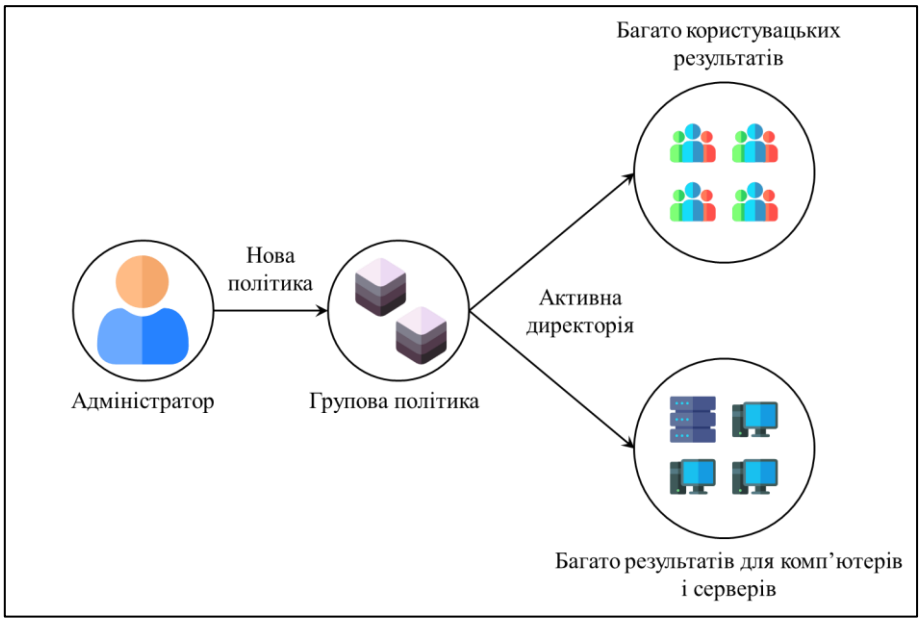

Рисунок 3.1 – Приклад застосування групової політики

Дискреційне управління доступом (DAC) є методом авторизації, який обробляє ідентифікацію запитувача або правила доступу (авторизації) за допомогою критеріїв оцінки, наданих довіреними комп'ютерними системами, для обмеження доступу до об'єкта (Рисунок 3.2). DAC реалізується з використанням ACL і вважається життєздатним рішенням для управління доступом, коли кількість користувачів і ресурсів є невеликою. DAC є найпоширенішим рішенням для управління доступом в операційних системах Windows і на основі UNIX. Однак воно має кілька недоліків у середовищах на основі хмари. По-перше, неспроможність полегшити управління процесами на рівні адміністратора. По-друге, власник об'єкта, який надає доступ до об'єкта іншим користувачам, може створити проблему безпеки. По-третє, складність аудиту відіграє роль. У системі DAC відстеження даних є складним завданням, оскільки це не централізована система, що дозволяє адміністраторам моніторити лише локальний потік кожної ACL. DAC залежить від підтримки ACL системою. Необхідне постійне надання та відкликання дозволів на доступ.

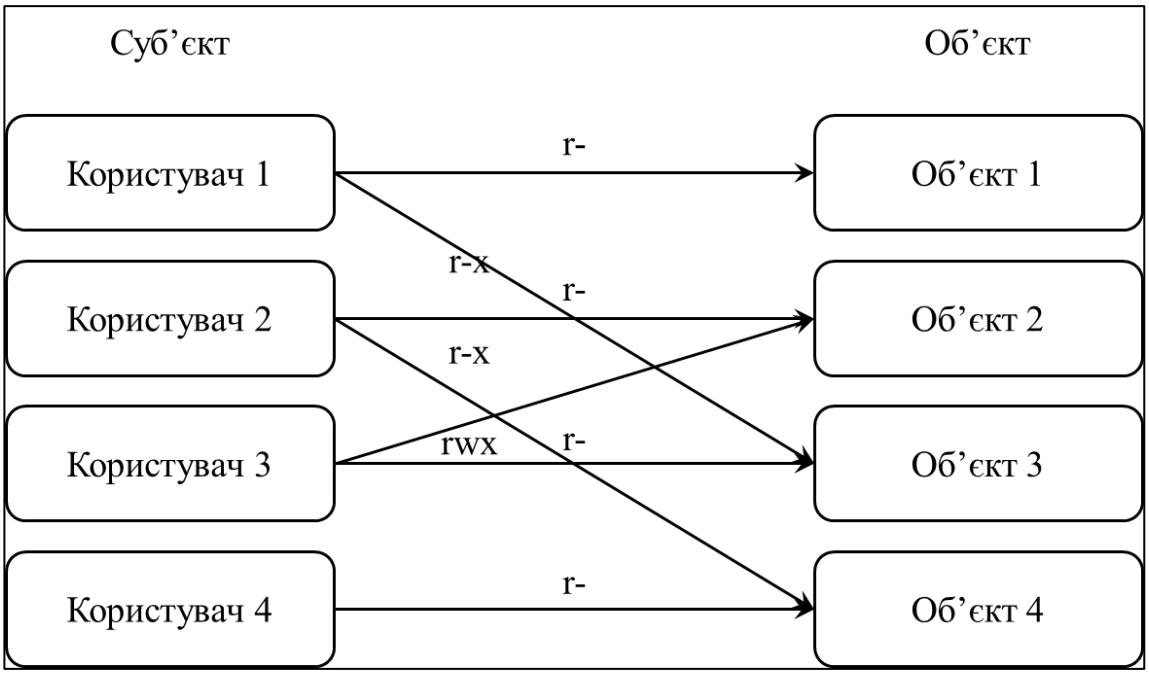

Рисунок 3.2 – Модель DAC

Крім того, DAC має мінімальну негативну авторизаційну силу. Значний недолік, пов'язаний із відсутністю контролю над потоком інформації. Дійсно, дані можуть бути дубльовані між об'єктами, що дозволяє неавторизованим суб'єктам отримати доступ до копій даних, навіть якщо власник не надав доступ суб'єкту до оригінальних даних.

Обов'язкове управління доступом часто використовується в організаціях із суворими вимогами до безпеки, таких як уряди та державні служби. MAC контролює доступ, порівнюючи мітки безпеки, які вказують на рівень чутливості або критичності системних ресурсів. Це вимагає створення різних рівнів допуску безпеки та асоціювання об'єктів у системі з одним із цих рівнів безпеки. На практиці кожному об'єкту може бути присвоєна мітка, така як: некласифікований, конфіденційний, секретний або цілком таємний. Доступ до рівня, вищого за власний допуск суб'єкта, заборонений (Рисунок 3.3). MAC використовує рівень доступу суб'єкта та мітки об'єктів для примусового контролю доступу, який виконується системою. Маркування об'єктів полягає в попередньому визначенні їх рівня безпеки.

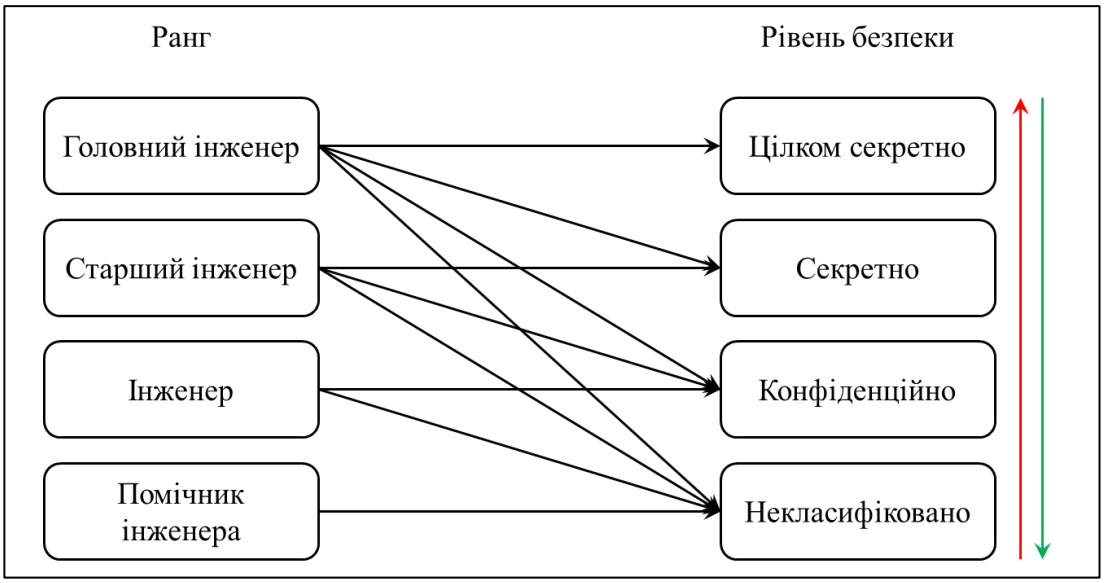

Рисунок 3.3 – Модель MAC

Це означає, що суб'єкти не можуть змінювати дозволи, оскільки тільки адміністратор має таку можливість. Наприклад, вони не можуть надавати доступ іншим користувачам до об'єктів, до яких вони самі мають доступ. Відомо, що MAC має відкриті проблеми. По-перше, MAC створює значний попит на технічне обслуговування для оновлення списку у зв'язку з розширенням бази користувачів та їх зміною під час розвитку бізнесу. Рішення також погано масштабується, оскільки нові користувачі та інформація потребують постійних оновлень конфігурацій об'єктів та облікових записів. Крім того, впровадження рішення MAC є дорогим і складним через високу залежність від довірених компонентів та додатків для міток і властивостей MAC.

Контроль доступу на основі правил (RuBAC) еволюціонує з традиційного підходу MAC. Це дозволяє подолати обмеження в управлінні складними дозволами, які початкове рішення не може вирішити. Прикладом такої моделі є модель розширення на основі семантичних правил для обробки політик доступу. Інший приклад підходу на основі правил – це контроль доступу на основі граток (LBAC), де грати використовуються для визначення багатошарової політики безпеки. Конкретним застосуванням до систем

охорони здоров'я є поєднання рівнів чутливості та інших категорій для об'єктів прирівнюється до рівнів безпеки [15]. Це демонструється як грати, що деталізують ієрархічні відносини рівнів безпеки. Коли рівень безпеки залежить від суб'єктів та об'єктів:

- рівень безпеки, пов'язаний з об'єктами, відображає класифікацію безпеки;
- рівень безпеки, пов'язаний з об'єктами, забезпечує класифікацію за допомогою збереженої інформації;
- рівень безпеки, пов'язаний з суб'єктом, визначається чутливістю інформації;
- суб'єкти в одній категорії мають однаковий рівень дозволу на безпеку.

В управлінні доступом на основі атрибутів (Рисунок 3.4) доступ та авторизація визначаються атрибутами, пов'язаними з суб'єктом та об'єктом доступу. Всі об'єкти та суб'єкти мають набір пов'язаних атрибутів, таких як місцезнаходження, створення та права доступу. Доступ до об'єктів надається або забороняється залежно від відповідності атрибутів об'єкта та суб'єкта. ABAC є гнучким та ефективним рішенням для встановлення правил безпеки або політик на основі атрибутів або умов навколишнього середовища [16]. Одним з обмежень ABAC є складність аудиту. Для забезпечення безпеки та дотримання нормативних вимог важливо точно знати, до яких ресурсів користувач має доступ. У порівнянні з RBAC, цей процес є трудомістким, оскільки він вимагає перегляду та перевірки кожного атрибута суб'єкта. Проте, ABAC є універсальним рішенням для масштабування користувачів та об'єктів, дозволяючи легко оновлювати атрибути та керувати політиками. Це значно знижує кількість ручної роботи з налаштування контролю доступу. Атрибути, пов'язані з суб'єктами, включають: посаду, статус або роль, історію входу, ідентифікацію за відбитками пальців та мережеве розташування. Атрибути, пов'язані з об'єктами, включають: доступ, метадані та властивості файлів або баз даних.

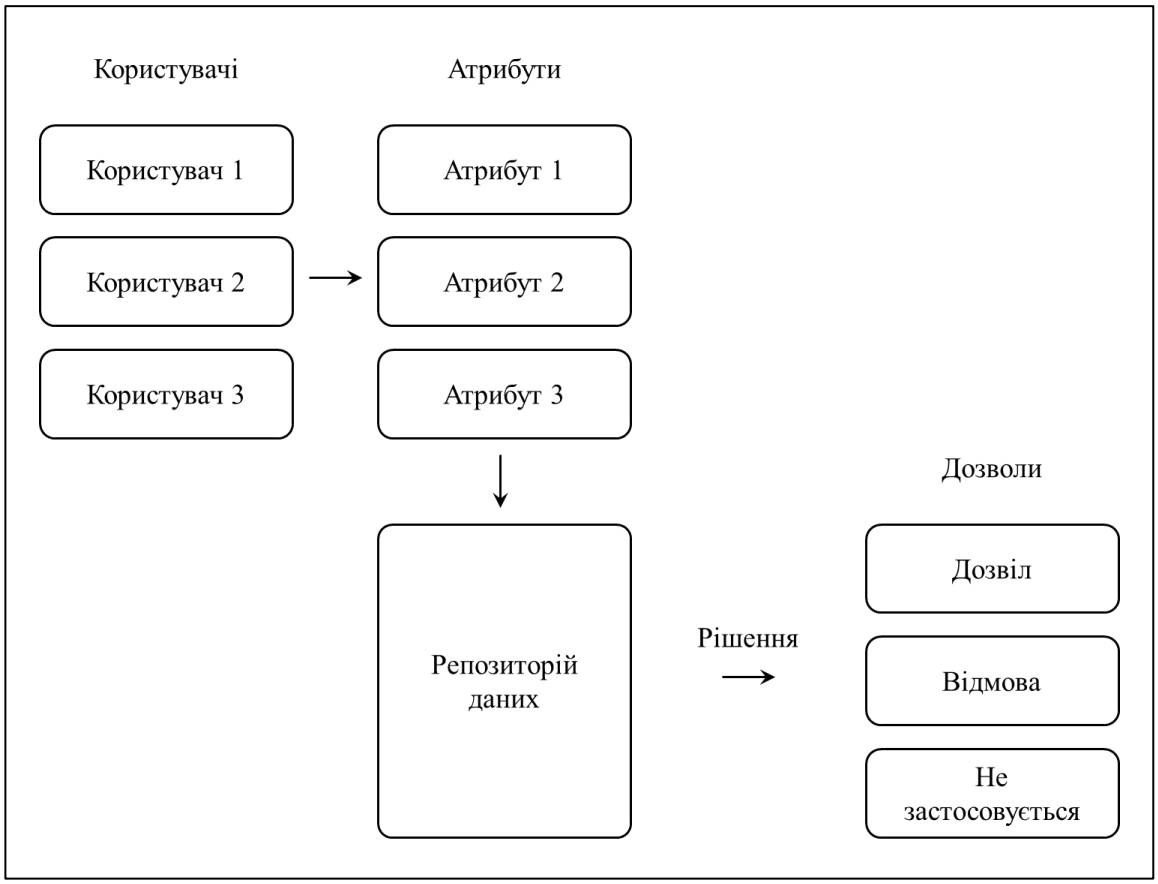

Рисунок 3.4 – Модель ABAC

Управління доступом на основі ролей (RBAC) надає доступ та авторизацію на основі ролей користувачів, що надає суб'єктам явні та неявні дозволи для певної ролі. Права доступу до ролей успадковуються через ієрархію ролей та визначають дозволи, необхідні для виконання певних операцій, як показано на рисунку 3.5. Конкретні ролі можуть бути надані одному або кільком користувачам. На відміну від інших рішень контролю доступу, RBAC може використовуватися для встановлення загальної політики безпеки компанії, що виходить за межі можливостей списків контролю доступу (ACL), визначаючи, як користувачі можуть змінювати файл.

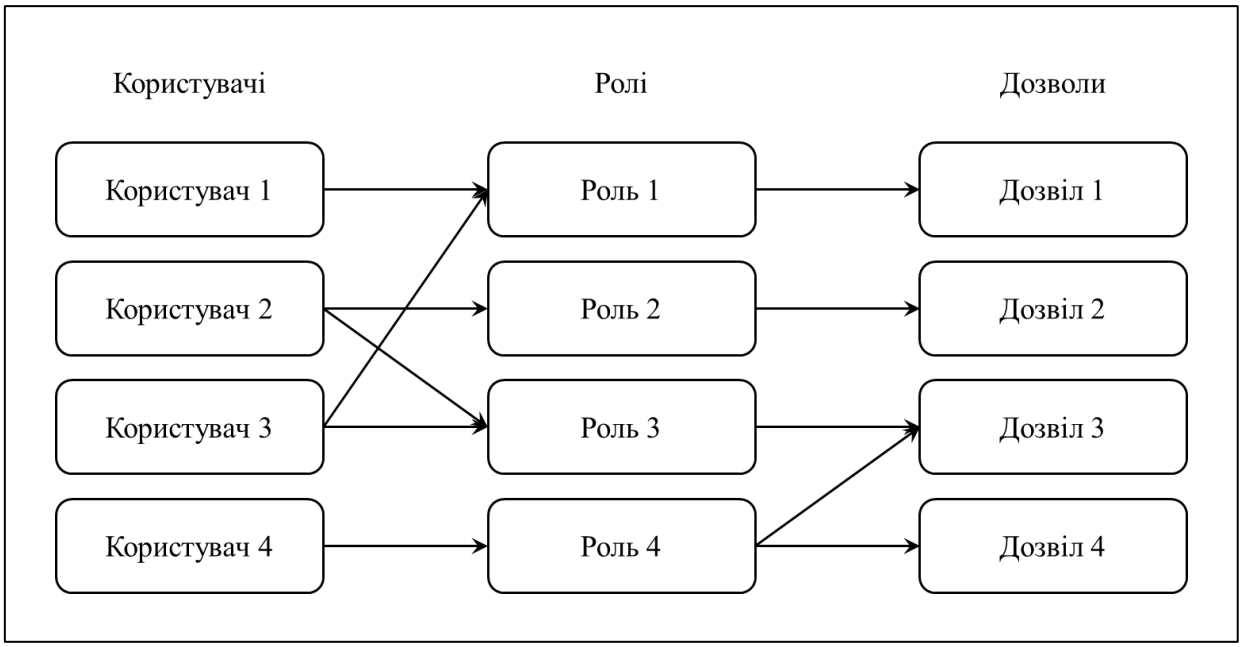

Рисунок 3.5 – Модель RBAC

Різні підходи до RBAC включають.

1. Плоский: ця модель використовує три основні правила RBAC. Система повинна підтримувати багато-багато призначень ролей і дозволів. Користувачам слід дозволяти використовувати дозволи декількох ролей одночасно.

2. Ієрархічний: ця модель використовує всі правила та можливості плоского RBAC та визначає старшинство між відносинами. Старші ролі включають в себе всі ролі, які нижчі за них.

3. Обмежений: ця модель використовує всі функції ієрархічного RBAC та додає підтримку розподілу обов'язків (SoD). Застосовується, коли для виконання завдання потрібно більше ніж одна людина [17].

4. Симетричний: це найвищий рівень впровадження RBAC і має всі вимоги обмеженого RBAC разом із функцією підтримки перегляду ролей дозволів [18].

5. Тимчасовий: ця модель розширює RBAC та підтримує увімкнення та вимкнення ролей.

Проблеми та обмеження RBAC включають вибух ролей, оскільки модель має труднощі з масштабуванням для задоволення складних вимог контролю доступу, пов'язаних із зростанням бізнесу та суворими кібербезпековими нормативами. RBAC також не має толерантності до ризиків безпеки, що вказує на рівень, до якого інформацію потрібно захищати від атак на конфіденційність або цілісність. Крім того, рішення не має масштабованості та динамізму через фокусування лише на ролях працівників та використання їх як засобу авторизації. Нарешті, впровадження цієї техніки у бізнесі може бути дорогим та складним, залежно від масштабу організації.

Архітектура RBAC є розподілом політики примусу та рішень з:

– точкою прийняття політики (PDP): яка надаватиме або відхилятиме запити, інтерпретуючи політику;

– точкою примусу політики (PEP): що зв'язується з PDP та забезпечує виконання рішень політики, зосереджуючись на привілейованих діях. PEP можуть бути розгорнуті по всьому коду, їх охоплення залежить від конкретних політик контролю доступу [19].

Сучасний стан RBAC можна оцінити із врахуванням його загальних обмежень та труднощів, які включають статичний дизайн та неефективність оновлення політик контролю доступу або обробки повторного шифрування при безпечному обміні файлами. Використовуючи криптосистему на основі ідентичності, можна створити виразну модель RBAC для хмарного середовища, особливо для хмарного зберігання. Рішення спрямоване на покращення RBAC, підвищення ефективності та гнучкості, додаючи механізм успадкування ролей, що робить призначення дозволів більш ефективним та точним. Функціональні тестування та аналіз продуктивності, демонструють, як система може виконувати ряд функцій, підтримувати динамічний контроль доступу до даних шифрованого тексту та зберігати час завершення операцій на прийнятному рівні [20].

Управління доступом на основі політик (Рисунок 3.6) забезпечує стратегічне рішення для управління доступом суб'єктів до кількох систем.

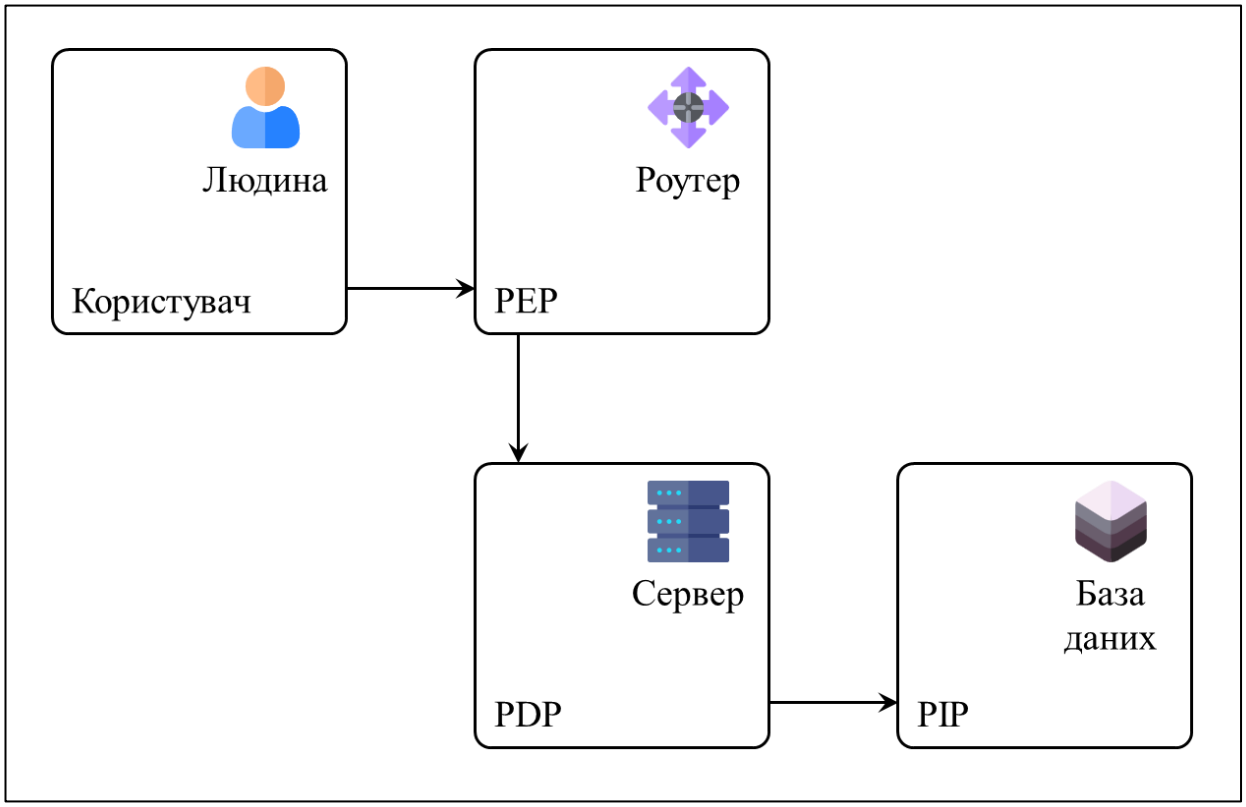

Рисунок 3.6 – Модель PBAC

Воно поєднує ролі для суб'єктів із політиками, які визначають привілеї доступу для певної ролі. Архітектура PBAC забезпечує детальне управління доступом для авторизованих суб'єктів до сервісів, одночасно захищаючи ресурси від несанкціонованого доступу. PBAC має певні недоліки, пов'язані зі складністю впровадження та часом і ресурсами, необхідними для розгортання багатьох політик і атрибутів під час встановлення правил.

PBAC можна використовувати для робототехнічних застосувань, щоб покращити аспекти безпеки операційних систем роботів, дозволяючи адміністратору динамічно відкликати дозволи. Модель розроблена для включення категорій дозволів, управління доступом на основі політик, ідентифікаційних токенів та токенів доступу. Політичний двигун (Policy Engine) розроблений для включення представлення політик, ідентифікації користувача та відкликання дозволів. Експерименти демонструють використання таких сценаріїв, як спроба неавторизованого оператора

виконати завдання, авторизований користувач, що виконує те саме завдання, і відкликання дозволів від авторизованої групи всіх користувачів, окрім адміністратора.

Гібридне рішення, що поєднує PBAC, ABAC та RBAC (PAR-AC), для ефективного управління та використання ресурсів, складається з трьох кроків: (1) реєстрація нового суб'єкта, (2) для поточних користувачів — вхід у систему (аутентифікація на основі політик), та (3) після аутентифікації механізм управління доступом надає користувачам певні привілеї залежно від їх рівня доступу.

3.2 Оцінка рішень контролю доступу

У цьому розділі здійснено оцінювання різних методів контролю доступу (Рисунок 3.7), розглядаючи такі аспекти: функціональність, алгоритми та структури даних, переваги, недоліки, можливості розгортання та відкриті проблеми.

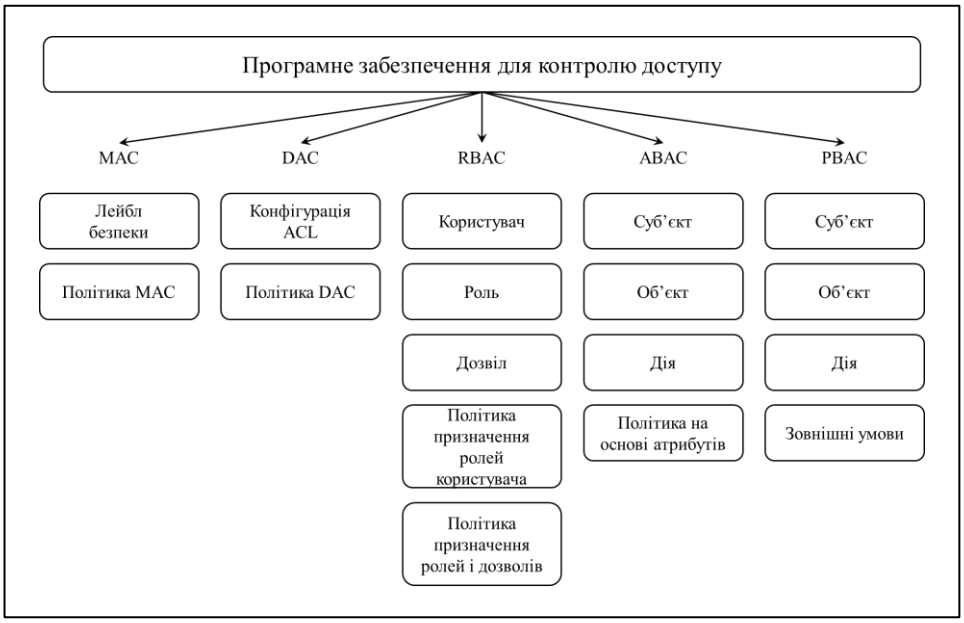

Рисунок 3.7 – Методи контролю доступу

У таблиці 3.2 підсумовано основні аспекти, що стосуються алгоритмів, структур даних та їх функціональності.

Таблиця 3.2 – Алгоритми контролю доступу та структури даних

Модель	Структура даних	Алгоритми	Можливості
ACL	Списки можливостей, списки доступу, реляційна база даних	Комбінування правил, видалення тіньових, покритих правил	Пошук правил, які можна безпечно видалити, в т.ч. тіньові та покриті правила. Перевпорядкування правил в ACL на основі фактичної, прогнозованої кількості хітів і затримки правил.
DAC	Деревоподібна структура, матриця доступу, список можливостей, таблиця авторизації	Виявлення критичних наборів (CSD)	Автоматичне скасування авторизації після закінчення інтервалу дійсності.
DAC (Bell-LaPadula) [21]		Дискреційна властивість безпеки	Дискреційні політики для виконання дій над ресурсами з використанням квитків можливостей.
MAC	Решітка	Цифровий підпис, властивість безпеки, простий аксіом інтеграції	Перевірка цифрового підпису. Заборона запису із нижчих рівнів, читання з вищих рівнів на нижчі та навпаки
ABAC	Політичні матриці, журнали	Витягування атрибутів, відносин, обрізка правил, покращення політики	Викачування алгоритмів, відносин і правил з БД, удосконалення політик для поліпшення обслуговування та дотримання політики.

Продовження таблиці 3.2

Модель	Структура даних	Алгоритми	Можливості
RBAC	Списки дозволів, матриця доступу, ієрархічне дерево	URA97, PRA97, RRA97	Призначення користувача, дозволів, ролі на роль,
PBAC	Політичні матриці	Витягування каталогу ресурсів даних	Диференціація привілеїв для користувачів і вмісту ресурсів

Списки контролю доступу (ACL) є важливим інструментом для обмеження доступу до ресурсів у мережі, забезпечуючи деталізований контроль над трафіком. Ця функціональність сприяє оптимізації використання ресурсів і захищає від несанкціонованого доступу. ACL працюють шляхом управління списками дозволів для користувачів, дозволяючи або забороняючи доступ до конкретних ресурсів. Основою для їх реалізації є списки можливостей, що обробляються за допомогою Active Directory або реляційних баз даних. Завдяки логарифмічному пошуку ACL ефективні навіть у великих мережах, хоча управління складними списками може бути проблематичним. Основною відкритою проблемою є обмежений контроль над тим, як користувачі модифікують файли, що може призвести до пошкодження даних. ACL ефективно розгортаються на маршрутизаторах, Windows, Linux, і дозволяють значно знизити обчислювальні витрати.

DAC дозволяє суб'єктам керувати власними даними та ефективно отримувати доступ до даних інших суб'єктів. Це дає можливість суб'єктам самостійно розробляти параметри доступу, а його обслуговування є відносно простим. Кожен фрагмент даних може мати індивідуальні обмеження доступу, а доступ до об'єктів обмежується на основі ідентичності суб'єктів. DAC зазвичай реалізується за допомогою списків контролю доступу (ACL) та централізовано контролюється.

У файлових системах дозволи можуть бути застосовані у структурі дерева папок. Кожен суб'єкт має Матрицю доступу, де кожен стовпець пов'язаний з об'єктом, а кожна клітинка містить набір прав доступу. Сховище для рядків у матриці відоме як Список можливостей. Алгоритм, що використовується в DAC, дозволяє тимчасову авторизацію з використанням часу початку та закінчення авторизації.

DAC пропонує кілька переваг, таких як можливість передачі власності на об'єкт іншим суб'єктам і визначення прав доступу для інших суб'єктів. Він також обмежує доступ суб'єктів після кількох невдалих спроб автентифікації, і несанкціоновані суб'єкти не мають доступу до властивостей об'єкта, таких як ім'я файлу, розмір і шлях до каталогу. Проте DAC має вбудовані вразливості, такі як неправильна конфігурація програмного забезпечення та атаки типу Trojan Horse. Його негативна авторизація обмежена, тобто він не може обмежити доступ до конкретних суб'єктів.

Відкритою проблемою є те, що DAC не може забезпечити всебічну безпеку, оскільки користувачі можуть ділитися своїми даними на свій розсуд. DAC може бути використаний для покращення відповідності та дозволяє організаціям моніторити мережеву активність.

Функціональність MAC полягає в тому, що адміністратор може детально визначити права доступу до об'єкта, і користувачі не можуть їх редагувати. Це захищає від атак типу Trojan Horse завдяки неспроможності знищити класифікацію даних або поділитися доступом до класифікованих даних. Операційна система або база даних обмежують права доступу: кожному суб'єкту та пристрою в системі присвоюється рівень класифікації та допуску. Це реалізується за допомогою ACL та контролюється централізовано.

Решітка розділяє доступ на різні відділи для визначення рівнів безпеки для користувачів і даних. Алгоритм обмежує модифікацію або зміни шляхом застосування правил. Файл або виконуваний файл можуть бути замінені лише на інший файл або виконуваний файл з такою ж цифровою підписю, що може

бути перевірена за допомогою будь-якого публічного ключа в бінарному файлі з таким же ім'ям.

MAC забезпечує надійне рішення для безпеки, оскільки лише системний адміністратор може отримати доступ або змінити контроль, що призводить до меншої кількості потенційних помилок безпеки. Централізований контроль під однією владою створює повністю централізовану систему. Однак ручна конфігурація рівнів безпеки та допуску потребує постійного моніторингу з боку адміністраторів, що веде до поганої підтримуваності. Крім того, цей метод контролю доступу не може масштабуватися автоматично, оскільки суб'єкти повинні запитувати доступ до всієї нової інформації і не можуть налаштовувати параметри доступу для своїх даних.

Основним викликом є складний процес налаштування та негнучкість.

MAC ефективно використовується там, де необхідний найвищий рівень захисту даних і наявне централізоване зберігання інформації.

Функціонал атрибутивного контролю доступу полягає в динамічному доступу до даних, який є можливим для гнучкості та масштабованості з низьким рівнем обслуговування. Атрибути конкретних суб'єктів детально обмежують мережевий доступ для забезпечення відповідності до вимог безпеки [21].

Матриці політик використовують заголовки стовпців як атрибути користувача для надання або відмови у правах доступу. Логи ABAC можна спостерігати для розуміння шаблонів навколо суб'єктів, ресурсів та умов навколишнього середовища. Алгоритми представляють матриці у моделі і автоматизують процес генерації політик через видобуток політик [23].

До переваг ABAC належить автоматичне оновлення дозволів з низькими витратами на адміністрування і детальний рівень безпеки. Серед недоліків – складна реалізація в порівнянні з іншими моделями контролю доступу.

Нагальною проблемою є складна реалізація, яка вимагає сотень тисяч атрибутів для встановлення правил і політик.

ABAC підходить для організацій, які вимагають точного й динамічного управління доступом та які надають перевагу вищому рівню безпеки, ніж той, що пропонують традиційні моделі контролю доступу.

RBAC дозволяє використовувати як прості, так і складні правила, обмежуючи доступ відповідно до ролей конкретних суб'єктів. Є три основні етапи в реалізації RBAC: призначення ролі, авторизація ролі та авторизація дозволів [24].

Алгоритми та структури даних RBAC використовують матрицю доступу як таблицю, де в рядках зазначені ролі, а в стовпцях — різні об'єкти та дії [25]. Список дозволів зберігає кожен об'єкт даних із деталями про те, хто може виконувати конкретні операції над цим об'єктом. Деревоподібна структура визначає ієрархію ролей у системі. Алгоритми надають і відкликають доступ користувача, дозволи та модифікації між відносинами однакових типів ролей.

RBAC покращує загальну відповідність вимогам безпеки, конфіденційність та приватність ресурсів, включаючи особисті дані або системи. Він також забезпечує диференційований доступ користувачам в залежності від їхніх ролей, з особливими дозволами для кожної ролі. Безпека вбудована в організаційну структуру та стратегію. RBAC підтримує розділення обов'язків (SoD) і є гнучким. Однак, може виникнути «вибух» ролей, коли дозволи є надто деталізованими, що ускладнює управління і може бути дорогим. Це робить RBAC складним і заплутаним. Рішення RBAC вимагає, щоб адміністратор мав глибоке розуміння безпекової карти організації та того, як дозволи були надані до розгортання. Після впровадження рішення реагувати на нові загрози безпеки та ризики стає складно. Визначення ролей може бути простим на початку впровадження RBAC у бізнесі, але з часом додавання більше ролей і персоналу може стати складним завданням. Розширене рішення RBAC може бути дорогим, що призводить до необхідності масштабування інфраструктури разом із ростом персоналу. Головним викликом є те, що користувачам надаються лише дозволи через ролі, а не через об'єкти чи операції.

RBAC добре підходить для середніх і великих організацій, що прагнуть стандартизувати контроль доступу, оскільки він покращує відповідність, конфіденційність і стандарти управління доступом для бізнесу.

PBAC використовує ролі користувачів у поєднанні з атрибутами для визначення детальних індивідуальних прав доступу. Правила видимі через PIPs, а процеси прийняття рішень і виконання чітко розділені [26].

Матриці політик використовують заголовки стовпців як атрибути користувача для надання або відмови у правах доступу. Алгоритм витягує збережені змінні контролю доступу, такі як користувач, ресурс та дозволи, які використовуються разом із точками політики [27].

Перевагами PBAC є гнучкість розвитку і інтеграції з іншими техніками. Підтримує масштабованість організації та відповідність. Недоліками є те, що розгортання може бути складним, як і управління великим обсягом запитів; складність технології, адміністрування та усунення несправностей також можуть бути проблемними.

Основним викликом є забезпечення відповідності п'яти основним критеріям: послідовність, релевантність, мінімальність, повнота і правильність є складним у розподілених політиках.

PBAC підходить для розподілених систем, де потрібна висока адаптивність і інтеграція.

3.3 Контроль доступу для хмарних середовищ

Хмарні обчислення використовуються для надання комп'ютерних ресурсів на вимогу, таких як зберігання даних або обчислювальна потужність, що працює без прямого управління користувачем (рисунок 3.8).

Рисунок 3.8 – Схема контролю доступу до хмари

Це можна спостерігати у великих хмарних середовищах, які включають кілька функціональностей, розподілених по різних локаціях. У таблиці 3.3 наведено деякі дослідження на тему контролю доступу (АС) для хмарних середовищ. Ці дослідження інноваційні в існуючих рішеннях і представляють нові підходи.

Таблиця 3.3 – Огляд рішень контролю доступу для хмари

Рішення	Тип	Характеристики	Інновації
C-CP-ARBE	ABAC	Обмежує мережевий доступ на основі атрибутів окремих користувачів	Високий рівень зручності, ефективне управління політикою
L-ABAC	ABAC	Ролі користувачів поєднуються з атрибутами для визначення індивідуальних прав доступу	Атака на сервер місцезнаходження впливає тільки на пов’язану інформацію. Інша залишається конфіденційною
Cloud ABAC	ABAC	Вводить концепцію груп, які асоціюються з рухомими ТЗ на основі специфічних атрибутів	Сповіщення, специфічні для місцезнаходження залежно від виконання політик в системі для інтелектуальних транспортних систем.

Продовження таблиці 3.3

Рішення	Тип	Характеристики	Інновації
L-BAC	ABAC	Ддвошаровий захист захищає від несанкціонованого доступу до даних у хмарі	Сильний засіб, що робить доступ до особистої інформації дуже складним для зловмисників.
T-RBAC	RBAC	Вбудована в ОС Microsoft Windows	Знижує ризики, покращує якість рішень, прийнятих операторами або власниками даних.
P-BAC	RBAC	Обмежує доступ до об'єктів на основі ідентичності суб'єкта	Використовує сховища Swift (OpenStack), що обмежує доступ до об'єктів за допомогою ACL.
Agent-based Framework	PBAC	Операційна система або БД обмежує рівень безпеки суб'єкта	Можливість зібрати поняття ролі, завдання, атрибуту, обмеження та сесії, комбінуючи рішення для авторизації, модель контролю доступу та аналіз поведінки користувача.
Product-lifestyle management	RBAC	Удосконалений RBAC для хмарного середовища з використанням патернів безпеки	Розширення RBAC з традиційних доменів застосування до хмарних середовищ.

Рішенням для великих даних у хмарних середовищах є колаборативне шифрування на основі атрибутів (C-CP-ARBE), яке включає криптографічний рівень, що забезпечує ефективну конфіденційність великих даних [23]. Оцінка техніки показує її ефективність для практичного впровадження АС у хмарній архітектурі. Майбутні дослідження зосереджені на великому експерименті для оцінки продуктивності одночасних доступів до великих наборів даних.

Схема контролю доступу на основі атрибутів з урахуванням місцезнаходження (L-ABAC) для хмарних середовищ включає власника даних, орган атрибутів, сервери місцезнаходження, датчики, споживачів даних (користувачів) і хмарний сервер [24]. Вони аналізують ефективність L-ABAC, демонструючи її низьку накладну для споживачів даних, органів атрибутів і хмари. Перевагою системи L-ABAC є те, що компрометація одного сервера вплине лише на інформацію, пов'язану з певним місцем, а інша інформація залишиться конфіденційною. Подальше дослідження стосується механізмів відновлення у випадку компрометації серверів місцезнаходження.

ABAC для промислових розумних транспортних засобів, які підтримують специфічні місця і повідомлення в реальному часі в розумному транспорті – це розумне рішення безпеки інтегрується з детальною ABAC-моделлю, що вводить групи як динамічно призначені елементи на основі властивостей рухомих транспортних засобів.

Доступ на основі решітки у хмарному середовищі для захисту інформації користувачів є новим рішенням з використанням гібридного алгоритму, де решітка формується за допомогою різних рівнів безпеки або значень [28]. Експерименти проводяться на симуляторі на основі хмари (CloudSim) з використанням подвійного шифрування AES та RSA. Рішення ефективно підвищує безпеку даних для користувачів у хмарних середовищах.

Модель оцінки на основі довіри впроваджує контроль доступу на основі ролей завдань (T-RBAC) у хмарному середовищі для зменшення ризиків і підвищення безпеки від атак Sybil, колюзій та атак включення/виключення [29]. Модель використовує критерії, такі як зниження довіри, довіру до завдання, важливість взаємодії, умовний трансфер і суб'єктивність, щоб зупинити завдання або роль у разі витоку даних.

Нове рішення контролю доступу на основі предикатів використовує RBAC та Open Stack Swift storage для хмарних середовищ і пропонує новий підхід для автоматизованого застосування безпекових предикатів до всіх запитів [30].

Фреймворк на основі агентів поєднує аутентифікацію, контроль доступу і аналіз поведінки суб'єкта [31]. Цей фреймворк захищає платформи постачальників від зовнішніх загроз і підтримує хмарні додатки для охорони здоров'я. Проведено експерименти для оцінки ефективності та тестування системи на вразливості до різних загроз, включаючи DoS, DNS-атаки, сканування TCP за допомогою NMAP та постійні бекдори Meterpreter.

RBAC і C-RBAC зазнали критики за їхню неспроможність забезпечити конфіденційність і цілісність, пропонуючи рішення з контекстним контролем доступу, яке використовує екологічний контекст, рівні дозволів та політики для адміністраторів і користувачів [22].

Удосконалена RBAC-модель для хмарних обчислень, засновану на принципах кібербезпеки: найменш привілеї, розділення обов'язків і абстракція даних. Модель тестувалась на SaaS, PaaS і IaaS, і SaaS виявилась найбільш підходящою для запропонованої системи RBAC [21].

3.4 Контроль доступу для середовищ на основі Blockchain

Blockchain є розподіленою і децентралізованою структурою даних, організованою як цифровий журнал, що зберігає транзакції в блоках на різних системах (Рисунок 3.9). Він може підвищити кібербезпеку, ускладнюючи підробку будь-якого блоку після його додавання до Blockchain. Механізм консенсусу забезпечує гарантії цілісності. Минулі транзакції зберігаються, розподіляються та дублюються по мережі комп'ютерних систем таким чином, що дозволяє учасникам індивідуально моніторити та перевіряти їх у спосіб, що економить обчислювальні ресурси. Перевірка поточних операцій може включати важкі обчислення, особливо для систем Proof of Work.

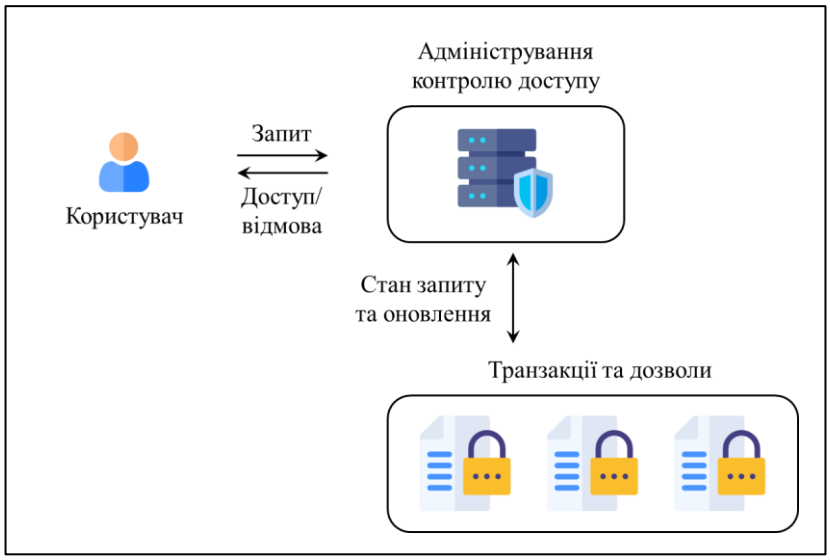

Рисунок 3.9 – Схема контролю доступу на основі блокчейна

У таблиці 3.4 представлено різні дослідження контролю доступу для середовищ на основі Blockchain.

Таблиця 3.4 – Огляд рішень контролю доступу для Blockchain

Рішення	Тип	Характеристики	Інновації
TBAC	ABAC	Транзакції як міст для інтеграції ABAC і блокчейну в нову платформу	Гнучке управління дозволами, прозорий процес авторизації доступу
BSeIn	ABAC	Працює з використанням криптографічних матеріалів (підписи на основі атрибутів, шифрування для кількох одержувачів	Кіберстійкість проти атаки підробки користувачів, атаки DoS/DDoS, модифікації трансляційних транзакцій або атак на відповіді повідомлень, і атаки MITM (людина посередині)
SBAC	ABAC	Надає постачальнику контенту можливість ділитися, перевіряти та скасовувати привілеї	Дає постачальнику контенту повний контроль над власним контентом, забезпечуючи високу ефективність і характеристики безпеки

Продовження таблиці 3.4

Рішення	Тип	Характеристики	Інновації
FADB	ABAC	Ця техніка поєднує блокчейн, розподілене сховище IPFS та шифрування CP-ABE	Нова схема шифрування, HECP-ABE поєднує традиційне шифрування CP-ABE з блокчейном
BDSS-FA	ABAC	Платформа обміну даними. Вводить новий алгоритм шифрування на основі атрибутів (HABE)	Використовує контракт для перевірки дозволів користувача
BacS	ABAC	Використовуючи адресу акаунта вузла в блокчейні як ідентифікатор для доступу до системи управління доменом, перевизначає правила управління доступом	Забезпечує шифрування всіх транзакцій управління доступом, які видаються сервером управління доменом. Контроль доступу є досяжним та безпечним для впровадження в розподілених середовищах (IoT)
SCBAC	ABAC	Рішення на основі IoT з використанням блокчейну	Використовуючи публічні атрибути, політики та дозволи на блокчейні, створює прозоре середовище конфіденційності даних
Blockchain -Based Delegatable AC	ABAC	Схема на основі атрибутів, яка інтегрується з можливостями контрольованого доступу	Забезпечує захист від підробки атрибутів, змови та псевдоанонімності

Дослідження інновують існуючі рішення та оригінальні підходи. ABAC у Blockchain впроваджується для управління цифровими активами за допомогою розподілених дозволів, представляючи нову платформу для

цифрового управління доступом (DAM-Chain), що використовує Контроль доступу на основі транзакцій (TBAC) [27]. Це забезпечує інтеграцію між моделлю розподілу ABAC і Blockchain, пропонуючи метод для організації легкого пошуку та доступу до цифрових активів, що складається з трьох компонентів: безпека активів, безпечна емісія активів та розподілені дозволи.

Нова структура для контролю доступу на основі Blockchain, відома як Blockchain-based Secure Mutual Authentication with Fine-Grained Access Control System for Industry (BSeIn), розроблена за допомогою криптографічних технік, таких як Attribute-Based Signatures (ABS) і Multi-Receiver Encryption (MRE) [28]. Метою є забезпечення кіберрезилієнтності проти атак підробки користувачів, атак типу "людина посередині" (MITM), модифікацій даних, атак відтворення, відмови в обслуговуванні (DoS) та розподілених атак DoS (DDoS). Оцінюється час виконання різних криптографічних алгоритмів на кількох конфігураціях серверів, а також вивчаються можливі оптимізації за допомогою апаратних або гібридних реалізацій.

Система Secure Blockchain-Based Access Control (SBAC) використовує механізм з токенами доступу на основі Blockchain для реалізації контентного контролю доступу на етапах розподілу, аудиту та відкликання [29]. Система забезпечує можливості для аудиту доступу до спільного контенту та рішень щодо доступу, а також тестується проти кібер-атак, таких як атаки на отруєння кешу, витягування даних з кешу, атаки DoS/DDoS і MITM-атаки.

Контроль доступу на основі смарт-контрактів (SCBAC) використовує ABAC для спрощення та покращення управління доступом, забезпечуючи динамічний метод тонко налаштованого контролю доступу. Реалізація систем контролю доступу за допомогою Blockchain через смарт-контракти демонструє ефективне вирішення проблем з одиночними точками відмови, досягаючи розподіленого контролю доступу та зберігаючи важливі дані в кількох місцях [32].

Рішення під назвою Fine-Grained Access Control Scheme for VANET Data Based on Blockchain (FADB) інтегрує Blockchain, розподілене зберігання IPFS

і шифрування на основі атрибутів (CP-ABE). Це рішення забезпечує безпеку даних, захист приватності та обмеження доступу в мережах Vehicle Ad Hoc Network (VANET) [30]. FADB використовує нову ефективну схему шифрування (HECP-ABE), поєднуючи традиційне шифрування CP-ABE з Blockchain для забезпечення розподілених послуг обміну даними. Система охоплює реєстрацію користувачів, завантаження даних та авторизацію доступу, а майбутні дослідження зосередяться на рівнях анонімності та безстатусному доступі.

Платформа для захищеного обміну даними на основі Blockchain з тонко налаштованим контролем доступу (BDSS-FA) включає ієрархічний алгоритм шифрування на основі атрибутів (HABE) [31]. Ця модель включає Центр генерації ключів, Власника даних, P2P-платформу розподілу даних, кластер IPFS, Blockchain Hyper-ledger Fabric і Споживача даних. Смарт-контракт дозволяє здійснювати довірені, відстежувані та незворотні транзакції без стороннього управління, а також використовується для перевірки дозволів суб’єкта та часткового декодування запитуваних даних.

Ще одне рішення, Blockchain-Based Access Control Scheme (BacS), спрямоване на захист від двох основних атак: крадіжки та модифікації даних і змін елементів у базі даних авторизації [33]. Це рішення усуває потребу в централізованій базі даних авторизації, але включає деякі обчислювальні витрати, необхідні для забезпечення високої пропускної здатності.

Інша робота пропонує схему контролю доступу, яка підтримує контрольовану делегацію доступу та забезпечує гнучкий і безпечний обмін даними за допомогою ABAC [34]. Основний акцент робиться на обміні медичною інформацією, що дозволяє надавати гнучкий доступ як зареєстрованим, так і незареєстрованим користувачам, де Blockchain управляє атрибутами, делегаціями та відкликаннями. Майбутні дослідження планують розширити підхід із впровадженням відповідної моделі довіри.

3.5 Контроль доступу для середовищ на основі IoT

Інтернет речей (IoT) – це концепція, яка об'єднує велику кількість фізичних пристроїв із вбудованими сенсорами, процесорами, програмним забезпеченням та іншими технологіями, що дозволяють їм збирати, обробляти і передавати дані. Основною ідеєю IoT є створення взаємопов’язаної екосистеми, де кожен пристрій, незалежно від його основної функції, може комунікувати з іншими пристроями та системами через інтернет або інші комунікаційні канали.

Такі пристрої можуть виконувати різноманітні завдання – від збору даних про навколишнє середовище (температура, вологість, рух, рівень освітлення) до виконання складних обчислень і прийняття рішень на основі аналізу отриманої інформації. Вони можуть бути як простими датчиками, так і повноцінними інтелектуальними системами.

Ключовими елементами IoT є:

Сенсори та виконавчі пристрої – вони забезпечують отримання даних із фізичного світу або виконують відповідні дії, наприклад, відкриття дверей чи вмикання освітлення.

Обчислювальні модулі – для обробки отриманих даних, проведення аналізу або виконання алгоритмів, які забезпечують автономність пристрою.

Комунікаційні технології – дозволяють пристроям обмінюватися інформацією між собою та з іншими системами. Це може бути Wi-Fi, Bluetooth, Zigbee, LTE, 5G або дротові з'єднання.

Програмне забезпечення – служить для координації роботи пристрою, управління даними, забезпечення їх передачі, зберігання та аналізу.

IoT дозволяє створювати мережі, що функціонують у реальному часі, інтегруючи дані з численних джерел і забезпечуючи комунікацію між пристроями. Наприклад, у розумному будинку пристрої, такі як термостати, освітлювальні системи, відеокамери та побутова техніка, можуть

синхронізуватись для підвищення комфорту, економії енергії або забезпечення безпеки.

Особливістю IoT є здатність формувати ad-hoc мережі — тимчасові мережі, які створюються для досягнення конкретних цілей. Наприклад, пристрої в автомобілі можуть об’єднуватися в окрему мережу для управління рухом, обміну інформацією з дорожньою інфраструктурою або інформування про аварійні ситуації. Розглянута система показана на рисунку 3.10, де демонструється, як пристрої IoT використовують інтернет і різні комунікаційні медіа для зв’язку між собою. Це наочно ілюструє, як фізичні об'єкти, оснащені сучасними технологіями, створюють єдине інформаційне середовище, що сприяє ефективнішому управлінню, прийняттю рішень і автоматизації процесів.

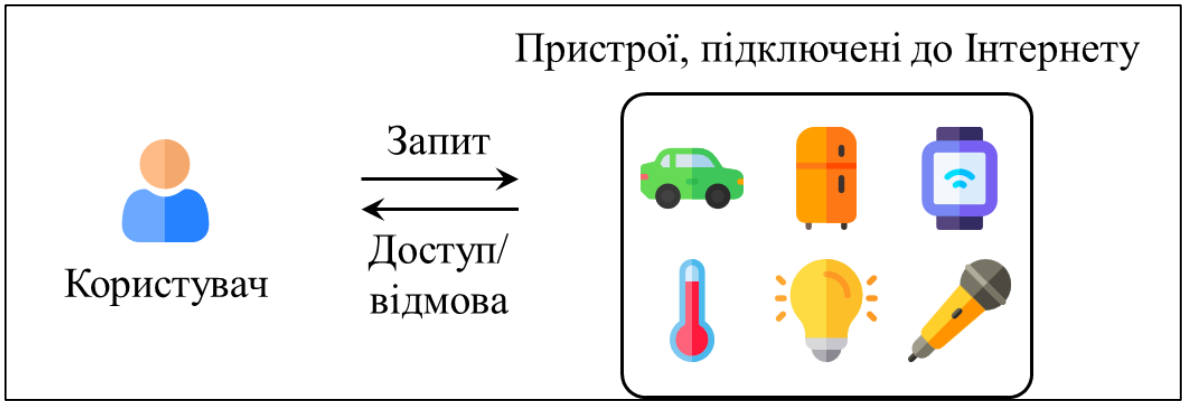

Рисунок 3.10 – Схема контролю доступу IoT

Огляд та аналіз досліджених робіт представлено у вигляді зведеної інформації, яка систематизована та узагальнена у таблиці 3.5.

У ній відображено ключові характеристики та інноваційний компонент досліджуваних моделей: CapBAC, CP-ABE, GCP-IoTAC, IACAC, SEM-ACSIT, BlendCAC, SEMAAC, LPAC.

Таблиця 3.5 – Огляд рішень контролю доступу для IoT

Рішення	Тип	Характеристики	Інновації
CapBAC	RBAC	Рядково-орієнтований список стилю, який асоціює кожен суб'єкт з парами об'єктів	Список можливостей зберігається у доступу, а не у ресурсів, до яких здійснюється доступ
CP-ABE [35]	ABAC	Підтримує кілька атрибутивних авторитетів, постійні ключі та розміри шифротексту	Спілкування та обчислення є економічно ефективними.
GCP-IoTAC	ABAC	Досліджує AC-рішення для Google Cloud IoT Platform	Безпечне спілкування для IoT-пристроївв. Захист від DoS/DDoS, MITM та Replay-атак
IACAC	RBAC	Легке, розподілене та стійке рішення безпеки	Захист від атак, наприклад, DoS/DDoS, MITM, Replay атак
SEM-ACSIT	ABAC	Гарантує безпеку при видаленні або оновленні атрибутів суб'єкта.	Значне зменшення накладних витрат на зберігання
BlendCAC	ABAC	Частково децентралізована та федеративна структура	Можливість використання смарт-контрактів та блокчейн-орієнтованого IoT-середовища
SEMAAC	RBAC	Базується на концепції спільноти для визначення прав	Нова спільнота-орієнтована структура для AC в розподілених IoT-контекстах
LPAC	ABAC	Акцент на захисті приватності атрибутів, легкі AC-політики.	Ефективно трансформує атрибути користувачів та політики доступу в компактний вектор атрибутів та вектор доступу

Основні підходи, застосовані до середовищ IoT, це ACL, контроль доступу на основі можливостей (CapBAC), RBAC, ABAC і контроль доступу на основі відносин (ReBAC). Ці технології порівнюються з урахуванням їхніх характеристик, застосованих до IoT, де пояснюються три особливі виклики: обмежені ресурси, гетерогенність і універсальність. Складність IoT потребує специфічного підходу до реалізації контролю доступу, включаючи легкість і масштабованість.

CP-ABE – це шифрування на основі політики атрибутів для контролю доступу користувачів у середовищах IoT. Це рішення підтримує тонко налаштований механізм контролю доступу з кількома Авторитетами атрибутів (AA), постійними розмірами ключів і шифротексту. Захищені дані отримуються шлюзовими вузлами з розумних пристроїв IoT, які зберігаються в часткових блоках і перетворюються в повні блоки хмарними серверами в P2P мережі. Даний аналіз також враховує витрати на комунікацію і обчислення, демонструючи ефективність рішення.

Google Cloud Platform IoT Access Control (GCP-IoTAC) – модель контролю доступу, експерименти з якою фокусуються на авторизаціях користувачів і ресурсів, розглядаючи реальні сценарії у випадках використання в охороні здоров'я та розумному домі з авторизаціями RBAC. Для майбутньої роботи запропоновано використання розширень на основі ABAC з рольовим методом для покращення взаємодії та досягнення тонко налаштованого контролю доступу. Існує підхід до аутентифікації особистості та контролю доступу на основі можливостей (IACAC) для середовищ IoT, що створює розподілене, легке і кіберрезилієнтне рішення. Було проведено експерименти і аналіз продуктивності, використовуючи потіковий шифр RC5 для шифрування, враховуючи атаки DoS/DDoS, атаки MITM і атаки відтворення. Новий метод контролю доступу – Secure and Efficient Multi-authority Access Control for IoT Cloud Storage (SEM-ACSIT). Система дозволяє значно зменшити накладні витрати на зберігання в системі. Крім того, рішення гарантує передову і зворотну безпеку при вилученні атрибутів користувача.

Експерименти та аналіз показують, що техніка вигідна для ефективності зберігання і обчислювальної ефективності з низькими накладними витратами, надаючи заходи кібербезпеки для надійного розподілу даних у середовищі хмарного зберігання в додатках IoT. Процедура управління доступом на основі можливостей з децентралізованою блокчейн-технологією (BlendCAC) для використання в середовищах Інтернету речей (IoT) використовує смарт-контракти та блокчейн-середовища. Експерименти включали створення прототипу концептуальної моделі, розгорнутої у фізичному середовищі IoT-мережі. Під час оцінки схеми вони розглядають дві інші техніки управління доступом, RBAC і ABAC, які були перекодовані для незалежних смарт-контрактів. Було виявлено, що RBAC і ABAC потребують локалізованого сховища даних для підтримки дозволів користувачів-ролей та обробки політик атрибутів-дозволів для завершення процесу авторизації та перевірки. Існує підхід під назвою Secure and Efficient Multi-Authority Access Control (SEMAAC) для сценарію використання в охороні здоров'я. У ньому фокус на підході управління доступом «спільноти» через те, що структура середовищ IoT рідко є повністю ізольованою. Рамкова модель складається з таких елементів: сервер авторизації, точка прийняття рішень політики (PDP), центр сертифікації (CA), «воротар» спільноти, точка виконання політики (PEP), спільнота (група сервісів, які мають спільні цілі) та можливість (структура даних, що містить набір прав доступу). Загалом, дослідження представляє позитивні кроки для системи управління доступом, в якій середовища демонструють адаптивну структуру, яку інші дослідники можуть використовувати для покращення заходів кібербезпеки. Техніка під назвою Lightweight Privacy-aware Access Control (LPAC) для сценарію використання в смарт-здоров'ї. LPAC забезпечує потужний захист конфіденційності атрибутів, детальне і легке управління доступом, процедури шифрування в офлайн та онлайн режимах, а також ефективні методи дешифрування. Порівнюючи зберігання і обчислювальних ресурсів та аналіз безпеки, можна зосередити увагу на здатності протистояти атакам.

3.6 Контроль доступу для середовищ на основі SDN

Програмно визначені мережі (SDN) є платформою управління мережею, яка пропонує динамічну, програмовану та ефективну конфігурацію мережі. Використання підходу SDN може покращити продуктивність та моніторинг мережі. На відміну від традиційних фізичних інфраструктур, він дозволяє мережевій інфраструктурі використовувати емуляцію, віртуалізацію та програмованість, а не фіксовані фізичні пристрої, як показано на рисунку 3.11.

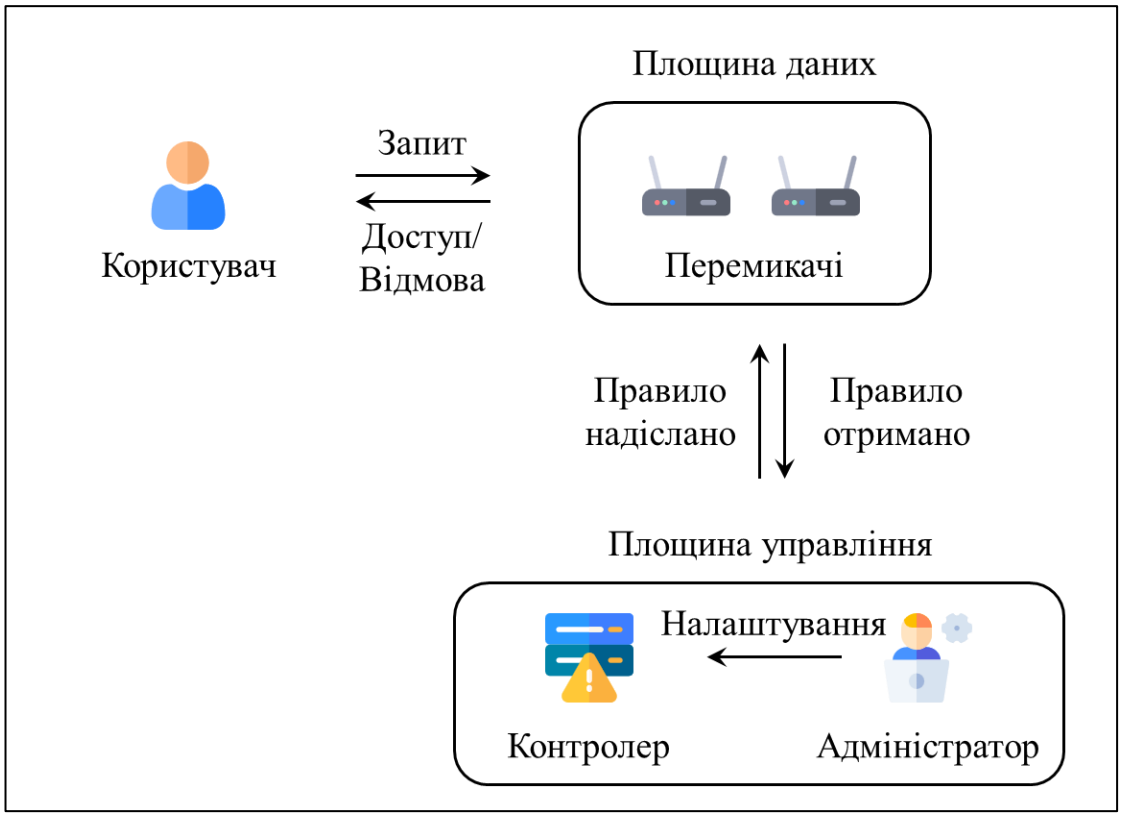

Рисунок 3.11 – Схема контролю доступу на основі SDN

У таблиці 3.6 детально описано техніки контролю доступу, застосовані до технології SDN, з підкресленими оригінальними підходами.

Таблиця 3.6 – Огляд рішень контролю доступу для SDN

AC	Тип	Технічні характеристики	Дослідницькі інновації
Flow Identity	RBAC	Високорівневі правила, засновані на інформації про роль та SDN-принципи, що динамічно застосовуються на мережевих кінцевих точках	Використання Policy Enforcement Point надає операторам мережі рішення щодо безпеки на підприємствах. Вирішує проблеми з мережевими постачальниками
SDN	ABAC	Доступу до ресурсів для SDN-інфраструктури з Network Access Control API	Виконання вимог доступу через конфіденційні компоненти
B-DAC [34]	RBAC	Децентралізована структура контролю доступу з прототипом реалізації, використовує Hyper-ledger Fabric Blockchain для захисту SDN-контролера	Рішення робить атаки на SDN-контролери марними для хакерів, оскільки стає неможливим створення помилкової сутності для запуску атак на канал додатків контролера SDN
FlowNAC	ABAC	Надає права доступу користувачам до мережі залежно від запитуваних сервісів	Контроль доступу до кількох сервісів одночасно, можливість відокремлення PEP на рівні плейн-дейта
AuthFlow	RBAC	Використовується як механізм автентифікації	Використовується у поєднанні з OpenFlow Software-Defined Networking для забезпечення контролю доступу до інфраструктури
Controller DAC	ABAC	Запропонована система, яка використовує Controller-Independent Security	Захищає SDN-контролер від атак на API та кібератак, використовуючи методи роботи з OpenDayLight з мінімальною складністю розгортання
SDN-RBAC	RBAC	Role-Based Access Control у середовищі SDN	Демонструє використання RBAC через SDN-контролер

Використання контролю доступу може відбуватися в середовищі SDN. RBAC застосовується шляхом визначення центральних ролей для пристроїв, точки прийняття рішень щодо політик (PDP) для визначення політики в центральному місці, точки реалізації політик (PEP) та точки інформації про політики (PIP) — яка функціонує шляхом об'єднання PEP і PIP в комутатор, що зберігає ідентичності користувачів, наприклад, сховище даних LDAP. Також використовується новий метод реалізації політики з використанням безстанового рольового брандмауера з компонентом FlowIdentity, який відповідає за функціональність брандмауера.

Масштабований контроль доступу може бути використаний для ресурсів SDN, представляючи модель, що обмежує доступ до ресурсів, використовуючи часткові системні види в залежності від топології ресурсів та видимості основної платформи виконання. Ця схема поєднує попередні підходи до контролю доступу, включаючи Capability Based Access (CBA), ABAC та PBAC. Вони стверджують, що, незважаючи на певні успіхи, ще потрібно провести значно більше досліджень і розробок для створення більш зручного і масштабованого механізму розгортання та конфігурації для SDN.

Також існує техніка контролю доступу в середовищі SDN у поєднанні з Blockchain. Модель, відома як Blockchain-based framework for Decentralized authentication and fine-grained Access Control (B-DAC), реалізує контроль доступу, залежного від контролера, прозорого для додатків, строгого та децентралізованого. Це забезпечує перевірку всіх комунікацій з усіх додатків до контролера перед їх транзитом у мережу.

Рішення Flow-based Network Access Control (FlowNAC) можна порівняняти зі стандартом IEEE 802.1X Port-based Access Control (PNAC). Це порівняння підкреслює вдосконалення, такі як контроль індивідуального доступу до багатьох служб одночасно (на відміну від обмеження до однієї, як у PNAC). Дизайн і розробка FlowNAC використовують принципи SDN, щоб дозволити сегрегацію PEP на рівні даних від процесу атрибута авторитету на

іншій сутності. Це розділення дозволяє модульне та незалежне масштабування кожного компонента за потреби.

AuthFlow є новою технікою, відомою як забезпечення контролю доступу в середовищах SDN. Вона використовує OpenFlow як механізм для аутентифікації та контролю доступу для SDN. Вона аутентифікує хости вище рівня MAC за допомогою стандарту IEEE 802.1X та сервера аутентифікації RADIUS. Механізм AuthFlow реалізується як аутентифікація RADIUS проти бази даних LDAP. Вони розробили та оцінили прототип, показуючи, що підхід може запобігти несанкціонованому доступу до мережевих ресурсів, особливо коли хости вже аутентифіковані. Після попередньо визначеного періоду вони можуть втратити свої привілеї, що означає, що рішення може бути чутливим до часу. AuthFlow забезпечує покращене управління в порівнянні з іншими рішеннями контролю доступу, вводячи більше контролю над інформацією та дозволяючи визначати політики для контролю доступу до потоків, пов'язаних з обліковими даними хоста.

Безпека, незалежна від контролера, яка покращує можливості DAC контролера системи, захищаючи контролер SDN від атак API за допомогою ефективного та гнучкого методу з динамічним контролем доступу. Існує прототип, який доповнює OpenDaylight і має низьку складність розгортання. Однак, незважаючи на значну роботу в цій галузі досліджень (використання наборів дозволів для захисту контролерів SDN), виявлення атаки API з статичним контролем дозволів ще не досягнуто.

SDN-RBAC – це система управління доступом для захисту додатків контролера SDN. Визначено різні підходи, де система може обробляти сесії додатків. Це допомагає застосовувати принцип найменших привілеїв на рівні додатків і їх сесій. Кількість записів у ACL може постійно зростати, щоб забезпечити актуальну безпеку в середовищі з величезною кількістю джерел атак. Пам'ять TCAM, що використовується для зберігання цих записів у мережевих комутаторах, є особливо дорогою, тому мінімізація обсягу пам'яті за допомогою технік стиснення правил є можливим рішенням. Розподіл

політики контролю доступу в менших таблицях правил також обговорювався у багатьох попередніх роботах. Щоб вирішити деякі з недоліків, таких як реплікація правил або модифікація структури пакетів, запропоновано підхід для розподілу та оновлення цих правил з акцентом на політику пріоритету Longest Prefix Match (LPM) [36]. Їхня стратегія застосовується до серійно-паралельних мережевих графів, з процесом скорочення від будь-якого двотермінального орієнтованого ациклічного графа до серійно-паралельного випадку.

ВИСНОВКИ

Отже, у процесі дослідження розроблено методику впровадження систем контролю та управління доступом (СКУД) із застосуванням сучасних технологій, таких як хмарні сервіси та біометричні ідентифікатори. Ця методика спрямована на забезпечення високого рівня безпеки підприємств за рахунок інтеграції інноваційних технологій, що відповідають сучасним вимогам до захисту даних і доступу.

Робота виконана згідно з поставленою метою та завданнями.

1. Проведено аналіз потреб підприємств щодо функціональності та специфікацій СКУД.
2. Здійснено порівняння основних методів контролю доступу з аналізом їх ефективності.
3. Обґрунтовано вибір хмарних технологій та біометричних ідентифікаторів як основи сучасних СКУД.

Методика впровадження СКУД враховує: аналіз потреб підприємства; визначення необхідних компонентів системи; вибір інноваційних технологій для інтеграції; створення алгоритму впровадження та налаштування. Запропоновані рішення базуються на системному підході до безпеки, інтеграції технологій та гнучкості масштабування.

Наукова новизна роботи полягає у комплексному аналізі використання хмарних сервісів для моніторингу та управління доступом у реальному часі; обґрунтуванні вибору біометричних технологій (сканування відбитків пальців, розпізнавання обличчя, аналіз сітківки ока) як засобів ідентифікації, що відповідають сучасним вимогам безпеки; розробці алгоритму адаптації СКУД до потреб підприємств різного масштабу, зокрема інтеграції з іншими системами безпеки.

Результати дослідження можуть бути використані:

- при проєктуванні СКУД для підприємств різного масштабу;

– у модернізації існуючих систем безпеки;

– для підвищення ефективності управління доступом до критичних об'єктів.

Методика враховує особливості функціонування підприємств у різних секторах економіки, включаючи промисловість, фінансову сферу, офісні центри та заклади охорони здоров'я.

У дослідженні виділено ключові фактори, що впливають на вибір СКУД, зокрема: розмір підприємства; характер його діяльності; потреби в зонуванні доступу; необхідність інтеграції з іншими системами.

Підприємства з великим числом співробітників і складною структурою вимагають багаторівневих систем з високою пропускною здатністю, тоді як для малих офісів оптимальними є автономні рішення.

Будо здійснено порівняння існуючих методів контролю доступу. Проаналізовано п’ять основних підходів: карткові системи; біометричні ідентифікатори; мобільні додатки; клавіатурні системи; гібридні рішення.

Визначено, що карткові системи забезпечують базовий рівень безпеки, але поступаються в точності ідентифікації біометричним системам. Останні, своєю чергою, мають високі витрати на впровадження, але гарантують персоніфікований підхід до управління доступом.

Надано обґрунтування вибору технологій. Хмарні сервіси рекомендовані для великих і середніх підприємств завдяки можливості віддаленого моніторингу, масштабування та зберігання великих обсягів даних. Біометричні ідентифікатори рекомендовані як основний засіб ідентифікації завдяки їх надійності, точності та неможливості передати ідентифікатор третій особі.

У роботі також сформульовано рекомендації впровадження СКУД, які включають такі кроки.

1. Провести детальний аналіз потреб підприємства, включаючи оцінку об'єкта, кількості співробітників та необхідного рівня безпеки.

2. Обрати відповідну технологію ідентифікації залежно від масштабу підприємства та фінансових можливостей.

3. Забезпечити інтеграцію СКУД з іншими системами, такими як відеоспостереження, пожежна безпека та системи обліку робочого часу.

4. Використовувати хмарні сервіси для віддаленого управління доступом, моніторингу подій та резервного копіювання даних.

Запровадження запропонованої методики дозволить: підвищити рівень безпеки підприємства; зменшити час та витрати на управління доступом; забезпечити ефективний контроль і облік доступу до об'єктів; створити гнучку систему, що адаптується до змін у структурі підприємства.

Робота не охоплює всіх можливих варіантів інтеграції СКУД, а також не враховує специфічних вимог окремих галузей. Подальші дослідження можуть бути спрямовані на аналіз новітніх технологій, таких як штучний інтелект та блокчейн, у контексті контролю доступу.

Розроблена методика є універсальною основою для створення сучасних СКУД, що відповідають викликам часу. Її впровадження забезпечить надійний захист підприємств, ефективний контроль доступу та можливість подальшого масштабування системи без втрати її продуктивності та надійності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методологія синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури: монографія / С. П. Євсеєв та ін., Харків: Новий Світ-2000, 2024. 300 с.

2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. 2-ге вид., стер. Львів : Новий Світ-2000, 2024. 678 с.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 16.01.2024, № 3549-IX ВВР, 2024, №18, ст. 76.

4. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Вид. офіц. Київ : ДСТСЗІ СБ України. 22 с.

5. ДСТУ EN 50134-7:2017. Системи тривожної сигналізації. Суспільні системи сигналізації. Частина 7. Правила застосування (EN 50134-7:2017, IDT) ; чинний від 2017-08-01. Вид. офіц. Київ : УкрНДНЦ, 2017.

6. ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. На заміну ISO/IEC 27001:2013; чинний від 2022-10-25. Вид. офіц. Женева: ISO, 2022. 32 с.

7. UL 294:2018 (7-е видання). Стандарт на обладнання системи контролю доступу. На заміну UL 294:2013 (6-е видання); чинний від 2018-08-30. Вид. офіц. Нортбрук: Underwriters Laboratories, 2018. 48 с.

8. Комплексні системи захисту інформації : навч. посіб. / Ю. Є. Яремчук та ін. Вінниця : ВНТУ, 2018. 118 с.

9. Богуш В. М. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Київ : Ліра-К, 2022. 286 с.

10. Хорошко В. О. Проектування комплексних систем захисту інформації. Львів : Львівська політехніка, 2020. 320с.

11. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / В. Д. Козюра та ін. Ніжин : ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. 144 с.

12. А. Аль-Амморі. Елементи теорії надійності та інформаційної безпеки комп'ютеризованих систем: навч. посіб. Київ: Ліра-К, 2024. 282 с.

13. Golightly L. et al. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. Cyber Security and Applications. 2023, №1. 20 p.

14. Huang Y.-T. et al. Lagrange interpolation-driven access control mechanism: towards secure and privacy-preserving fusion of personal health records. Knowledge-Based Systems. 2022. №236.

15. Kumar R., Tripathi R. Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–Lapadula model. Journal of Ambient Intelligence and Humanized Computing. 2021. №12 (2). P. 2321–2338.

16. Vijayalakshmi K., Jayalakshmi V. A similarity value measure of ABAC security rules. 5th International Conference on Trends in Electronics and Informatics. 2021. P. 565–571.

17. Sun W., Yuan X., Su H. Role-engineering optimization with user-oriented cardinality constraints in role-based access control. International Journal of Network Security. 2021. №23 (5). P. 845–855.

18. Johnson J.T. Recommendations for Distributed Energy Resource Access Control. New Mexico : Sandia National Laboratories. 2021. 50 p.

19. Laverdière M.-A., Julien K., Merlo E. RBAC protection-impacting changes identifi-cation: acase study of the security evolution of two php applications. Information and Software Technology. 2021. №139.

20. Xu J. et al. Role-based access control model for cloud storage using identity-based cryptosystem. Mobile Networks and Applications. 2021. №26 (4). P. 1475–1492.

21. Zhang R. et al. Improved Bell–La-padula model with break the glass mechanism. IEEE Transactions on Reliability. 2021. №70 (3). P. 1232–1241.

22. Vijayalakshmi K., Jayalakshmi V. A study on current research and challenges in at-tribute-based access control model. Intelligent Data Communication Technologies and Internet of Things. 2022. №101. P. 17–31.

23. Karimi L. et al. An automatic attribute-based access control policy extraction from access logs. IEEE Transactions on Dependable and Secure Computing. 2021. №19 (4). P. 2304–2317.

24. Sahani G.J., Thaker C.S., Shah S.M. Scalable RBAC model for large-scale applications with automatic user-role assignment. International Journal of Communication Networks and Distributed Systems. 2022. Vol. 28, iss. 1. P. 76–102.

25. Rai B.K., Solanki T. Access control mechanism in health care information system. CRC Press. 2021. P. 149–160.

26. Bhatt S., Alshehri A., Sandhu R. Access control models in cloud iot services / M. Gupta et al. Springer. 2022. P. 63–96.

27. Chen Z. et al. Policy-based access control system for delta lake. Tenth International Conference on Advanced Cloud and Big Data. 2022, P. 60–65.

28. Saravanan N., Umamakeswari A. Lattice based access control for protecting user data in cloud environments with hybrid security. Computer Security. 2021. Vol. 100.

29. Alshammari S.T., Albeshri A., Alsubhi K. Integrating a high-reliability multicrite-ria trust evaluation model with task role-based access control for cloud services. Symmetry. 2021. №13 (3). P. 492.

30. Anilkumar C., Subramanian S. A novel predicate based access control scheme for cloud environment using open stack swift storage, Peer-to-Peer Netw. Appl. 2021. №14 (4). P. 2372–2384.

31. Ennahbaoui M., Idrissi H., A new agent-based framework combining authentica-tion, access control and user behavior analysis for secure and flexible cloud-based healthcare environment. Concurrency and Computation. 2022. Vol. 34, iss. 5.

32. Song L. et al. A novel access control for internet of things based on blockchain smart contract. IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference, vol. 5, 2021. P. 111–117.

33. A blockchain-based access control scheme in distributed internet of things / N. Shi et al. Peer-to-Peer Networking and Applications. 2021. №14 (5). P. 2585–2599.

34. Duy P.T. et al. B-DAC: a decentralized access control framework on northbound interface for securing SDN using blockchain. Journal of Information Security and Applications. 2022. №64.

35. Saha S. et al. Consortium blockchain-enabled access control mechanism in edge computing based generic internet of things environment. Transactions on Emerging Telecommunications Technologies. 2021. №32 (6).

36. Abboud A. et al. Automatically distributing and updating in-network management rules for software defined networks. Network Operations and Management Symposium : Budapest, Hungary, April 25–29, 2022. P. 1–9.

ДОДАТОК А
ПРЕЗЕНТАЦІЯ ДЛЯ ЗАХИСТУ ПРОЄКТУ

Рисунок А.1 – Слайд 1

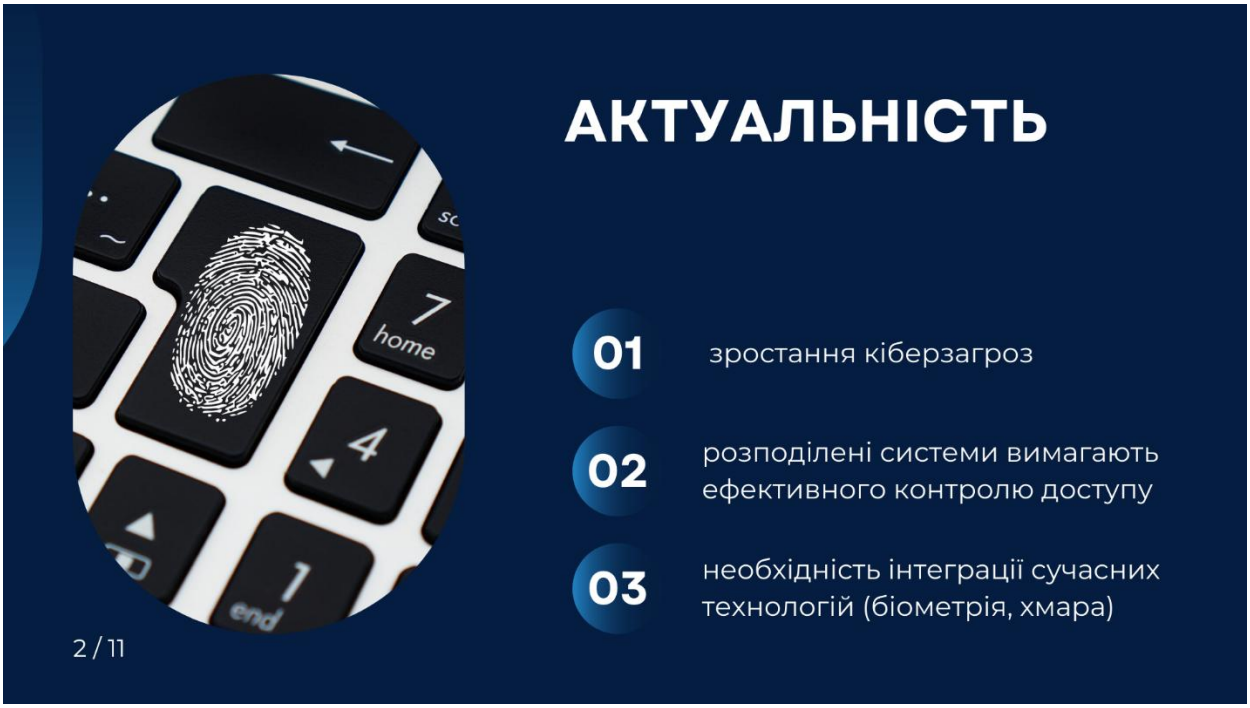

Рисунок А.2 – Слайд 2

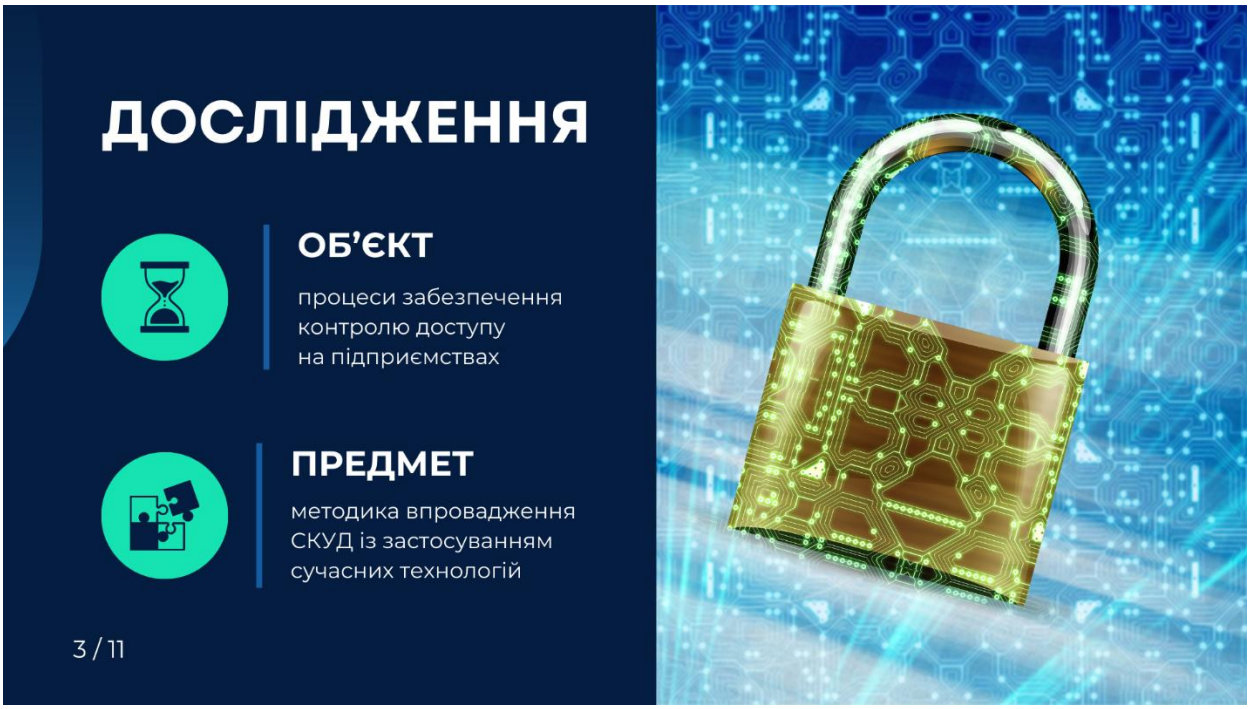

Рисунок А.3 – Слайд 3

Рисунок А.4 – Слайд 4

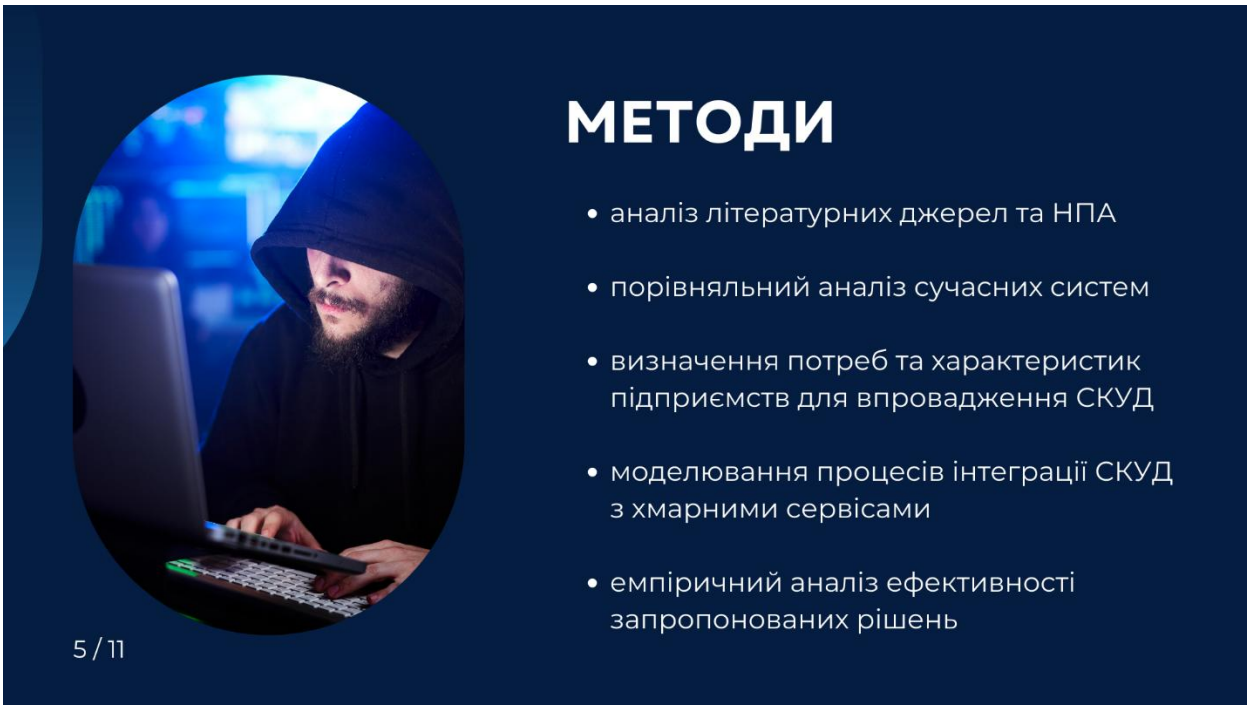

Рисунок А.5 – Слайд 5

Рисунок А.6 – Слайд 6

Рисунок А.7 – Слайд 7

Рисунок А.8 – Слайд 8

Рисунок А.9 – Слайд 9

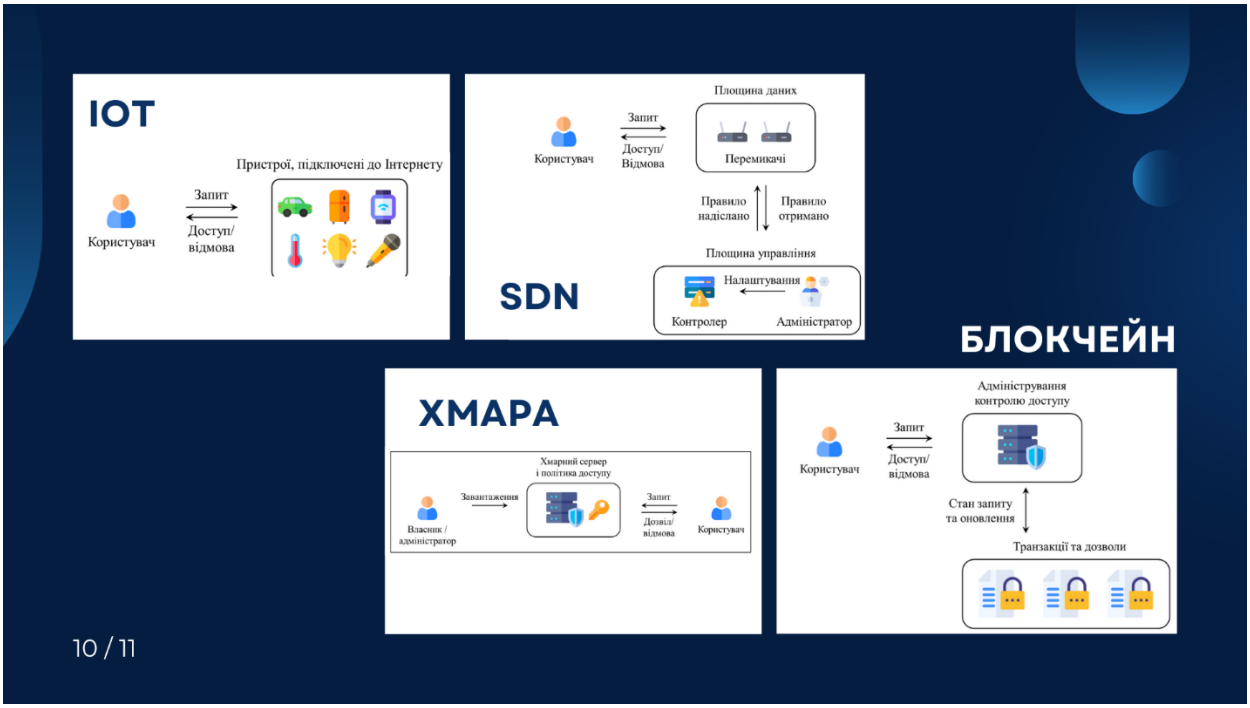

Рисунок А.10 – Слайд 10

Рисунок А.11 – Фінальний слайд