ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

на тему: «Захист інформації на об’єктах інформаційної діяльності шляхом використання сучасних систем контролю доступу»

на здобуття освітнього ступеня магістра
зі спеціальності __125 _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

_____ Євгеній ГЕРАСИМЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи СЗДМ-61
Євгеній ГЕРАСИМЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник:_____Андрій КОТЕНКО_____
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:_____
доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУРОБОТУ

_____Герасименко Євгенію Сергійовичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Захист інформації на об'єктах інформаційної діяльності шляхом використання сучасних систем контролю доступу»
керівник кваліфікаційної роботи _КОТЕНКО Андрій к.т.н., доцент_____
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Наукові джерела, стандарти (ISO/IEC 27001, NIST, GDPR) та аналітичні звіти (Gartner, Forrester).
2. Кейси впровадження систем Cisco ISE, Fortinet Access Management, Microsoft Azure AD.
3. Математичні моделі та інструменти аналізу FAR і FRR.
4. Дані тестування СКД та результати емпіричних досліджень.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд сучасних СКД та їх помилок (FAR, FRR).
2. Аналіз факторів, що впливають на точність систем.
3. Розрахунки, тестування і рекомендації для покращення СКД.
4. Висновки щодо результатів дослідження та перспектив впровадження.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання _____20.10.2024_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Євгеній ГЕРАСИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНККО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 95 стор., 3 рис., 3 табл., 30 джерел.

Об’єкт дослідження – процес забезпечення захисту інформації на об’єктах інформаційної діяльності.

Предмет дослідження – системи контролю доступу та їх вплив на захист інформації.

Мета роботи – підвищення ефективності систем контролю доступу для забезпечення надійного захисту інформації.

Методи дослідження – аналіз літератури, статистичний аналіз, математичне моделювання, емпіричний аналіз.

У роботі проведено аналіз сучасних систем контролю доступу, зокрема їхніх сильних сторін і недоліків, із акцентом на показниках помилок FAR (False Acceptance Rate) та FRR (False Rejection Rate). Використано математичні методи для оцінки ймовірності помилок у СКД. Розглянуто вплив організаційних та технічних факторів на точність систем. Ґрунтуючись на проведеному дослідженні, розроблено рекомендації щодо покращення роботи систем контролю доступу.

Апробація:

Є.С. Герасименко, Захист інформації на об’єктах інформаційної діяльності шляхом використання сучасних систем контролю доступу. *Всеукраїнської науково-практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.37 - 38.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Ключові слова: СИСТЕМИ КОНТРОЛЮ ДОСТУПУ, ЗАХИСТ ІНФОРМАЦІЇ, FALSE ACCEPTANCE RATE, FALSE REJECTION RATE, МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, БІОМЕТРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

The text of the master's qualification thesis: 95 pages, 3 figures, 3 tables, 30 references.

Object of the study – the process of ensuring information security at information activity objects.

Subject of the study – access control systems and their impact on information protection.

Purpose of the study – to enhance the efficiency of access control systems to ensure reliable information protection.

Methods of research – literature review, statistical analysis, mathematical modeling, empirical analysis.

The study analyzes modern access control systems, focusing on their strengths and weaknesses, with an emphasis on error indicators such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). Mathematical methods were used to evaluate the probability of errors in access control systems. The influence of organizational and technical factors on the accuracy of these systems was considered. Based on the conducted research, recommendations for improving the performance of access control systems were developed.

Field of application – information protection at information activity objects, including corporate offices, government institutions, and critical infrastructure facilities.

Approbation:

E.S. Gerasimenko, Information protection at information activity facilities through the use of modern access control systems. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.37 - 38.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Keywords: ACCESS CONTROL SYSTEMS, INFORMATION PROTECTION, FALSE ACCEPTANCE RATE, FALSE REJECTION RATE, MATHEMATICAL MODELING, MULTI-FACTOR AUTHENTICATION, BIOMETRICS, INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9

ВСТУП 10

РОЗДІЛ1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА СИСТЕМ КОНТРОЛЮ ДОСТУПУ 12

1.1. Визначення інформаційної безпеки 12

1.1.1. Історичний огляд розвитку інформаційної безпеки 13

1.1.2. Роль інформаційної безпеки у сучасному світі 14

1.2. Класифікація та функції систем контролю доступу 16

1.2.1. Основні функції систем контролю доступу 18

1.3 Сучасні технології в системах контролю доступу 19

1.4 Сучасні підходи до автентифікації 21

1.4.1 FAR і FRR у популярних системах 22

1.4.2 Інновації у методах автентифікації 23

1.4.3 Модель Zero Trust Security 24

1.5. Загрози інформаційній безпеці на об’єктах інформаційної діяльності 25

1.5.1. Уразливості систем контролю доступу 27

1.6. Висновок до першого розділу 28

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ 30

2.1. Огляд популярних рішень 30

2.1.1 Методологія відбору систем контролю доступу 31

2.1.2. Cisco ISE 32

2.1.3. Fortinet Access Management 33

2.1.4. Microsoft Azure AD Conditional Access 35

2.1.5. Практичне впровадження та аналіз у різних секторах 37

2.2. Недоліки сучасних рішень з урахуванням організаційних чинників 39
2.2.1. Ймовірність помилок FAR, FRR 40
2.2.2. Уразливості біометричних систем 42
2.2.3. Інфраструктурні проблеми..... 44
2.3. Математичний аналіз систем контролю доступу 46
2.3.1. Обчислення показників FAR та FRR 47
2.3.2 Методи зниження FAR/FRR 50
2.3.3 Приклади практичного застосування методів 52
2.3.4. Ймовірнісні моделі та розподіли даних..... 54
2.4. Прогноз ефективності та перспективи розвитку 56
2.4.1. Вплив інновацій ШІ, блокчейн, поведінковий аналіз. 58
2.4.2. Порівняння традиційних і сучасних СКД 60
2.4.3. IoT-рішення у фізичних СКД..... 62
2.5 Висновок до другого розділу 64
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗА ДОПОМОГОЮ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ 66
3.1 Аналіз і оптимізація системи контролю доступу для захисту інформації..... 66
3.2 Загальна характеристика об'єкта 67
3.1.1. Оцінка існуючої системи контролю доступу..... 69
3.1.2. Аналіз рівня захищеності інформації 70
3.2. Обґрунтування вибору сучасної системи контролю доступу 72
3.2.1. Вибір конкретної системи..... 73
3.2.2. Оцінка відповідності обраної системи міжнародним стандартам..... 75
3.2.3. Інтеграція системи в інфраструктуру організації..... 76

3.3. Математичний аналіз ризиків системи FAR, FRR 78
3.3.1. Визначення впливу FAR та FRR на захищеність об'єкта 78
3.4. Рекомендації щодо оптимізації системи контролю доступу 80
3.4.1. Розробка рекомендацій для зменшення FAR та FRR 80
3.4.2. Впровадження додаткових заходів безпеки 82
3.4.3. Прогноз ефективності після впровадження рекомендацій 84
3.5. Оцінка покращення захищеності даних після впровадження рекомендацій 85
3.5.1. Повторний розрахунок показників FAR та FRR 86
3.5.2. Порівняння результатів до та після впровадження 87
3.5.3. Висновки щодо ефективності запропонованих рішень 88
3.6 Висновок до третього розділу 90
ВИСНОВКИ 91
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 93

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СКД - Системи контролю доступу

MFA (Multi-Factor Authentication) - Багатофакторна автентифікація

FAR (False Acceptance Rate) - Ймовірність помилкового прийняття

FRR (False Rejection Rate) - Ймовірність помилкової відмови

FA (False Acceptance) - Помилкове прийняття

FR (False Rejection) - Помилкова відмова

RFID (Radio-Frequency Identification) - Ідентифікація за допомогою радіочастот

GDPR (General Data Protection Regulation) - Загальний регламент захисту даних

ML (Machine Learning) - Машинне навчання

AI (Artificial Intelligence) - Штучний інтелект

UBA (User Behavior Analytics) - Аналіз поведінки користувачів

IDS (Intrusion Detection System) - Система виявлення вторгнень

AES (Advanced Encryption Standard) - Передовий стандарт шифрування

RSA (Rivest-Shamir-Adleman) - Алгоритм криптографії RSA

BYOD (Bring Your Own Device) - Принеси свій власний пристрій

ISE (Identity Services Engine) - Платформа управління доступом Cisco

DDoS (Distributed Denial of Service) - Розподілена атака типу «відмова в обслуговуванні»

ZTS (Zero Trust Security) - Модель безпеки «нульової довіри»

ID (Identification) - Ідентифікація

IoT (Internet of Things) - Інтернет речей

RBAC (Role-Based Access Control) - Управління доступом на основі ролей

ABAC (Attribute-Based Access Control) - Управління доступом на основі атрибутів

SIEM (Security Information and Event Management) - Система управління інформацією та подіями безпеки

ВСТУП

Актуальність дослідження. Сучасне інформаційне суспільство характеризується швидким розвитком технологій, які впроваджуються у всі сфери життя: від бізнесу і медицини до державного управління. У цих умовах захист інформації, особливо на об’єктах інформаційної діяльності, стає одним із ключових аспектів забезпечення безпеки. За даними звіту IBM Security за 2023–2024 роки, середній збиток від витоку даних у світі перевищує 4,35 млн доларів, що підкреслює важливість впровадження надійних систем контролю доступу. Разом із зростанням кількості кіберзагроз та вимогами міжнародних стандартів, таких як ISO/IEC 27001, актуальність дослідження ефективності СКД є очевидною. Однак навіть найсучасніші рішення стикаються з проблемами, зокрема, із помилками доступу: хибним прийняттям FAR та хибним відмовленням FRR. В умовах України, з її специфічними викликами у сфері кібербезпеки, ця тема набуває особливого значення.

Об’єктом дослідження є системи контролю доступу, які використовуються для захисту інформації на об’єктах інформаційної діяльності.

Предметом дослідження є точність та надійність систем контролю доступу, їх вплив на захист інформації, а також методи зменшення помилок FAR і FRR.

Метою дослідження є аналіз ефективності сучасних систем контролю доступу, оцінка ймовірності виникнення помилок та розробка рекомендацій щодо їхньої оптимізації для забезпечення захисту інформації.

Наукові завдання. Для досягнення поставленої мети необхідно вирішити такі завдання:

- Провести огляд сучасних систем контролю доступу, які використовуються для захисту інформації на об’єктах інформаційної діяльності.
- Дослідити основні типи помилок у системах контролю доступу, зокрема:
- Помилки типу FAR — коли система пропускає неавторизованого користувача.

- Помилки типу FRR — коли система не пропускає авторизованого користувача.
- Оцінити ймовірність виникнення таких помилок за допомогою математичних методів.
- Проаналізувати фактори, що впливають на точність та надійність систем контролю доступу.
- Розробити рекомендації щодо покращення існуючих систем контролю доступу на основі проведеного аналізу.

Методи дослідження. Для досягнення поставленої мети та вирішення завдань у роботі використовуватимуться такі методи дослідження:

- **Аналіз літератури.** Проведення огляду наукових і технічних джерел для вивчення сучасного стану систем контролю доступу.
- **Статистичний аналіз.** Оцінка ефективності систем контролю доступу за допомогою статистичних показників, таких як FAR та FRR.
- **Математичне моделювання.** Використання математичних моделей для оцінки ймовірності виникнення помилок.
- **Емпіричний аналіз.** Тестування прототипу системи контролю доступу або існуючого рішення для збору даних про ефективність системи.

Практичне значення одержаних результатів полягає у можливості їх застосування для вдосконалення існуючих систем контролю доступу. Розроблені рекомендації можуть бути використані організаціями для оптимізації роботи СКД, зменшення кількості помилкових рішень і підвищення загальної надійності систем. Крім того, запропоновані методики дозволяють адаптувати СКД до нових умов, забезпечуючи відповідність міжнародним стандартам і зростаючим вимогам безпеки.

Таке дослідження є важливим не лише для приватного сектору, але й для державних установ, де захист інформації є критично важливим для національної безпеки. Результати роботи також можуть бути корисними для академічної спільноти, оскільки вони сприятимуть подальшому розвитку теоретичних і практичних аспектів інформаційної безпеки.

РОЗДІЛ1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1.1. Визначення інформаційної безпеки

Інформаційна безпека включає багато елементів, які захищають дані від несанкціонованого доступу, використання, розкриття, зміни або знищення. Конфіденційність, цілісність і доступність інформації є основними принципами інформаційної безпеки. [1][2].

Конфіденційність означає, що інформація може бути доступна лише уповноваженим особам чи системам. Сучасні системи контролю доступу використовують багатофакторну автентифікацію, яка перевіряє користувачів різними рівнями, такими як паролі, біометричні дані та SMS-коди. Наприклад, сучасні системи безпеки в офісі використовують комбінацію біометричних і RFID-карток для доступу до приміщень. [3].

Принцип цілісності означає, що інформація повинна бути захищена від несанкціонованих або випадкових змін. Цей принцип забезпечується в системах контролю доступу за допомогою використання криптографічних алгоритмів для захисту даних журналу подій, що унеможливлює зміну даних без авторизації. Наприклад, рішення Microsoft Azure Active Directory використовує хешування даних, щоб перевірити зміни та запобігти підробкам.

Для забезпечення доступності інформація повинна бути доступною для уповноважених користувачів у необхідний час. Це досягається системами захисту даних за допомогою резервного живлення та відмовостійких серверів, які забезпечують роботу навіть у разі перебоїв у мережі. Наприклад, системи контролю доступу Honeywell використовують два джерела живлення, щоб гарантувати безпеку роботи [2][3].

У сфері інформаційної безпеки стандарти є життєво важливими. Згідно з міжнародним стандартом ISO/IEC 27001, системи управління інформаційною безпекою повинні включати політику доступу, методи автентифікації та

моніторинг подій безпеки. Наприклад, цей стандарт зобов’язує компанії проводити регулярні оцінки ризиків інформаційної безпеки та впроваджувати відповідні заходи; це впливає на якість роботи СКД. [3][5].

Європейський регламент GDPR контролює обробку персональних даних і зобов’язує компанії захистити конфіденційні дані. У СКД це означає, що біометричні дані, такі як відбитки пальців або скани обличчя, які часто використовуються для автентифікації, повинні бути захищені. Згідно з GDPR, порушення правил безпеки може призвести до штрафів у розмірі до 20 мільйонів євро, що спонукає компанії ретельно дотримуватися їх. [4][21].

Таким чином, стандарти інформаційної безпеки лежать в основі захисту інформаційних систем. Сучасні стандарти, такі як ISO/IEC 27001 та GDPR, гарантують, що такі системи контролю доступу відповідають цим стандартам. [4][9].

1.1.1. Історичний огляд розвитку інформаційної безпеки

Утворення окремої галузі інформаційної безпеки демонструє поступовий розвиток методів захисту інформації. Перші методи захисту були виключно фізичними. Наприклад, під час середньовіччя використовувалися замки, сховища та обмеження доступу до архівів. Крім того, використовувалися прості методи шифрування, такі як поліалфавітне шифрування Віженера, які продовжують використовуватися до сучасної цифровізації. [1].

Коли під час Другої світової війни з’явилися нові електромеханічні пристрої для шифрування, такі як німецька «Енігма» та американська SIGABA, відбувся прорив у розвитку. Вони підкреслили важливість технічного та організаційного захисту даних і заклали основу для сучасної криптографії. Наприклад, протоколи передачі повідомлень, розроблені в цей період, стали основою сучасних протоколів кібербезпеки [2].

З початком цифрової ери в 60-х роках з’явилися електронні дані, що призвело до появи нових методів захисту, таких як паролі та обмеження доступу.

Розроблена в 1970-х роках модель Bell-LaPadula стала ключовою для захисту секретної інформації в системах з обмеженим доступом [1][2].

У 2000-х роках почався новий етап розвитку, коли збільшення обчислювальної потужності комп'ютерів дозволило впроваджувати складні криптографічні алгоритми, такі як AES і RSA. Основними інструментами безпеки стали багатофакторна автентифікація, системи виявлення вторгнень і аналіз поведінки користувачів. Наприклад, багатофакторна авторизація (MFA) підвищує захист, поєднуючи апаратні токени, біометричні дані та пароль для ідентифікації користувачів [10][24].

Особливу роль на сучасному етапі відіграють технології штучного інтелекту та машинного навчання. AI використовується для аналізу поведінкових аномалій у реальному часі, наприклад, для виявлення підозрілих спроб входу або несанкціонованого доступу. Системи на основі ML можуть прогнозувати атаки шляхом аналізу минулих даних, підвищуючи ефективність СКД. Блокчейн також активно інтегрується для захисту ланцюгів автентифікації, створюючи прозорі та незмінні журнали дій користувачів [2].

Таким чином, перехід від фізичних методів до високотехнологічних рішень, таких як штучний інтелект і блокчейн, спостерігається в розвитку інформаційної безпеки. Ця зміна гарантує ефективний захист від постійно зростаючих кіберзагроз.

1.1.2. Роль інформаційної безпеки у сучасному світі

У сучасному світі безпека інформації є важливою для бізнесу, медицини, держави та інших сфер. Усі ці галузі залежать від безпеки інформаційних систем, які обробляють, зберігають і передають життєво важливі дані. [1][2].

Для України виклики в галузі кібербезпеки стали особливо актуальними у зв'язку з військовою агресією Росії. Від 2014 року Україна стикається з масштабними кібератаками на державні та критично важливі об'єкти інфраструктури. Наприклад, атака на енергосистему України у 2015 році, відома як

"BlackEnergy", призвела до відключення електропостачання у трьох регіонах. Вона стала першим у світі випадком, коли кібератака безпосередньо вплинула на енергосистему. У 2017 році атака вірусу-здирника "NotPetya" завдала шкоди численним компаніям в Україні, викликавши фінансові втрати на сотні мільйонів доларів. Ці події підкреслюють критичну потребу в ефективних системах захисту, включаючи сучасні СКД [17][18].

У сфері бізнесу інформаційна безпека є ключовим елементом збереження конкурентоспроможності. Витік даних, зокрема клієнтських баз, може призвести до значних репутаційних і фінансових втрат. Наприклад, витік персональних даних клієнтів через вразливість у системі автентифікації платіжної платформи PayPal викликав резонанс у 2023 році, підкресливши необхідність багатофакторної автентифікації у фінансових системах [1][2].

Медицина також є однією з критично важливих галузей, де кібератаки мають серйозні наслідки. У 2021 році кібератака на ірландську систему охорони здоров'я HSE з використанням вірусу-здирника "Conti" паралізувала роботу лікарень, поставивши під загрозу життя пацієнтів. Такі атаки демонструють, наскільки важливо захищати медичні дані та забезпечувати доступність критичних систем [2][6].

У світі системи контролю доступу стають важливою ланкою захисту, але й вони піддаються атакам. Наприклад, у 2020 році атака на біометричну платформу Suprema Biostar, яка обслуговує об'єкти з доступом на основі відбитків пальців, спричинила витік 27,8 мільйонів записів. Це підкреслило важливість захисту біометричних даних і резервування даних.

Таким чином, сучасний світ стикається з дедалі складнішими викликами у сфері інформаційної безпеки, що вимагає впровадження багаторівневих заходів захисту. Особливо це актуально для України, яка перебуває на передовій глобальної кібервійни. Реалізація таких заходів, як інтеграція штучного інтелекту у системи контролю доступу, багатофакторна автентифікація та використання блокчейн-технологій, є ключовою для захисту критично важливих ресурсів [10].

1.2. Класифікація та функції систем контролю доступу

СКД є ключовим компонентом інформаційної безпеки, що дозволяє обмежувати доступ до ресурсів лише для уповноважених осіб або систем. Основна функція СКД полягає у встановленні та забезпеченні політики доступу, яка регулює права користувачів відповідно до їхніх повноважень. СКД базуються на трьох основних етапах: ідентифікації, автентифікації та авторизації [1].

СКД можна класифікувати залежно від сфери їх застосування та технологічної основи:

Фізичні системи контролю доступу: Ці системи використовуються для обмеження доступу до приміщень, будівель або територій. До них належать механічні замки, турнікети, ворота, сейфи тощо. Незважаючи на простоту використання, вони мають обмеження, зокрема неможливість адаптації до змін у правах доступу. Наприклад, механічні ключі можуть бути втрачені або скопійовані, що створює ризики безпеки.

Електронні системи контролю доступу: Включають RFID-картки, електронні замки, системи відеоспостереження, а також інтегровані рішення, які об'єднують кілька технологій. Наприклад, системи, які поєднують картковий доступ і розпізнавання обличчя, дедалі більше використовуються у корпоративних офісах. Водночас такі системи мають ризики, пов’язані з перехопленням сигналів або несанкціонованим копіюванням карток.

Логічні системи контролю доступу: Використовуються для захисту інформаційних ресурсів, таких як комп’ютери, сервери або бази даних. Логічні СКД забезпечують розмежування прав доступу, автентифікацію користувачів через паролі, токени або біометричні дані. Наприклад, Microsoft Azure Active Directory інтегрує багатофакторну автентифікацію для захисту корпоративних даних.

Гібридні системи контролю доступу: Поєднують фізичні та логічні методи захисту. Наприклад, система безпеки в сучасних дата-центрах використовує фізичний контроль доступу до серверних кімнат, а також логічний контроль

доступу до віртуальних машин. Такі рішення підвищують загальну ефективність захисту [1][2].

СКД виконують низку функцій, спрямованих на забезпечення безпеки об'єктів і ресурсів зображених на рисунку 1.1:

Рис. 1.1 - три концепції контролю доступу в кібербезпеці

Ідентифікація: визначення користувача або пристрою за унікальним ідентифікатором (наприклад, ID-картка, логін).

Автентифікація: підтвердження особи користувача за допомогою пароля, біометричних даних або апаратного токена.

Авторизація: перевірка прав доступу до конкретних ресурсів.

Аудит: ведення журналу подій для моніторингу та виявлення підозрілих дій.

Наприклад, сучасні системи з функцією штучного інтелекту аналізують журнали доступу в реальному часі, що дозволяє оперативно реагувати на можливі порушення [1].

Фізичні СКД забезпечують базовий рівень захисту, але не можуть адаптуватися до динамічних змін. Електронні СКД пропонують більшу гнучкість і функціональність, проте вони вразливі до кіберзагроз. Логічні та гібридні системи є найбільш ефективними, оскільки поєднують переваги обох підходів і дозволяють масштабувати рішення відповідно до потреб організації.

Навіть найбільш сучасні СКД стикаються з проблемами, зокрема:

- Помилки типу FAR, коли неавторизовані користувачі отримують доступ.
- Помилки типу FRR, коли авторизованим користувачам доступ блокується.

Загрози з боку внутрішніх зловмисників або інсайдерів, які мають легальний доступ до системи.

Таким чином, системи контролю доступу є важливим інструментом забезпечення інформаційної безпеки. Сучасні рішення спрямовані на інтеграцію новітніх технологій, таких як штучний інтелект та блокчейн, що дозволяє забезпечити як фізичний, так і цифровий захист ресурсів.

1.2.1. Основні функції систем контролю доступу

СКД виконують фундаментальну роль у забезпеченні інформаційної безпеки, забезпечуючи захист як фізичних, так і цифрових ресурсів. Вони регламентують доступ до ресурсів, виходячи з політик організації, мінімізуючи ризик несанкціонованого доступу та потенційних порушень безпеки. Основні функції СКД – ідентифікація, автентифікація, авторизація, моніторинг і аудит – працюють у взаємозв’язку, забезпечуючи цілісність системи захисту.

Ідентифікація передбачає встановлення того, хто саме намагається отримати доступ до ресурсу. Ідентифікатором може бути унікальний логін, карта доступу, серійний номер пристрою або біометричний зразок (відбиток пальця, райдужка ока). Цей етап є основою для всіх наступних дій у системі. Наприклад, ідентифікація за картковою системою з використанням RFID-міток дозволяє автоматично розпізнавати суб’єкта, при цьому знижуючи ризик помилкової ідентифікації через унікальність картки.

Автентифікація перевіряє справжність ідентифікатора, встановленого на попередньому етапі. У сучасних системах контролю доступу застосовується багатофакторна автентифікація, яка підвищує рівень захисту шляхом комбінації різних факторів: "те, що ви знаєте" (пароль або PIN-код), "те, чим ви володієте" (токен або смарт-картка), "те, ким ви є" (біометричні характеристики). Наприклад,

автентифікація через пароль у поєднанні зі сканером відбитків пальців значно ускладнює можливість злому системи.

Авторизація є процесом визначення рівня доступу користувача до ресурсів після успішної автентифікації. Вона базується на політиках доступу, які можуть реалізовуватися через моделі, такі як Role-Based Access Control або Attribute-Based Access Control. Наприклад, співробітник HR-відділу може мати доступ до бази даних співробітників, але не до фінансових документів організації. Авторизація дозволяє мінімізувати ризики, пов’язані з надмірними правами доступу, які можуть бути використані для зловживань.

Моніторинг здійснює постійний збір даних про всі дії, пов’язані з доступом до ресурсів. Це дозволяє виявляти аномалії, такі як багаторазові невдалі спроби автентифікації, які можуть свідчити про спробу злому. Наприклад, система моніторингу може виявити використання облікових даних працівника поза робочим часом, що є підозрілою активністю. Моніторинг також включає запис часу доступу, місця входу та інших параметрів [1][2].

Аудит дозволяє ретроспективно аналізувати дії, що здійснювалися в системі, виявляючи слабкі місця і вдосконалюючи політики безпеки. Наприклад, аудит логів доступу може показати, що певний користувач мав надмірні права доступу або що спроби автентифікації з певної IP-адреси часто завершувалися невдачею, що може свідчити про зловмисну активність. Результати аудиту є основою для поліпшення систем безпеки та забезпечення відповідності нормативним вимогам, таким як ISO/IEC 27001 або GDPR [3][9].

Реалізація всіх цих функцій у комплексі дозволяє системам контролю доступу мінімізувати ризики витоку даних та забезпечувати високий рівень інформаційної безпеки.

1.3 Сучасні технології в системах контролю доступу

Розвиток технологій суттєво змінив підхід до організації СКД. Традиційні методи, що базувалися на використанні паролів, фізичних ключів або карток, поступово замінюються або доповнюються інноваційними рішеннями. Сучасні технології не лише підвищують рівень безпеки, але й забезпечують зручність і гнучкість у використанні, що є ключовими факторами для їх впровадження у бізнесі, державних установах та інших сферах.

Однією з найбільш перспективних технологій у СКД є використання біометричних систем. Біометрія забезпечує ідентифікацію користувачів за їхніми унікальними фізіологічними або поведінковими характеристиками. Серед популярних методів розпізнавання виділяються: сканування відбитків пальців, розпізнавання обличчя, райдужної оболонки ока та навіть аналіз голосу. Наприклад, у банківській сфері активно впроваджуються системи, які дозволяють клієнтам здійснювати транзакції, використовуючи розпізнавання обличчя, що мінімізує ризики шахрайства. Однак біометричні системи мають певні недоліки, зокрема ризик компрометації біометричних даних. Наприклад, витік даних біометричної платформи Suprema Biostar у 2020 році спричинив загрозу для мільйонів користувачів. Такі випадки підкреслюють необхідність використання додаткових методів захисту, таких як шифрування біометричних даних та їхнє зберігання у децентралізованих базах [10][14].

Іншою важливою інновацією є багатофакторна автентифікація**,** яка передбачає використання комбінації кількох методів перевірки. Це можуть бути паролі, токени, біометричні дані або тимчасові коди. Наприклад, вхід до корпоративної системи може вимагати введення пароля, підтвердження через мобільний додаток і сканування відбитка пальця. Однак впровадження MFA потребує балансування між безпекою і зручністю для користувачів. Надмірно складні процедури автентифікації можуть призводити до незадоволення користувачів і помилок у роботі [10][24].

Ще однією тенденцією є використання штучного інтелекту для адаптивного управління доступом. Наприклад, система Amazon Rekognition інтегрує розпізнавання обличчя та аналіз поведінкових патернів, дозволяючи забезпечувати

доступ лише тим користувачам, чия поведінка не викликає підозр. Системи ШІ також аналізують поведінкові аномалії у реальному часі. Наприклад, якщо користувач намагається отримати доступ до ресурсів у нетиповий час або з незвичного місця, система може заблокувати його або вимагати додаткову автентифікацію. Недоліками ШІ в контексті СКД є можливість помилкового визначення загроз через недостатню якість навчальних даних, а також ризик упередженості алгоритмів.

Інтеграція блокчейн-технологій у СКД дозволяє створювати надійні журнали аудиту, які неможливо змінити або видалити. Наприклад, блокчейн може використовуватися для відстеження всіх дій користувачів у корпоративних системах. Це зменшує ризик внутрішніх загроз, оскільки кожна дія прозоро фіксується у незмінному реєстрі. Однак блокчейн-технології мають високу вартість впровадження та вимагають значних обчислювальних ресурсів, що обмежує їхнє використання у малих і середніх компаніях [27].

Ще однією технологією, яка стає популярною, є IoT-рішення для управління фізичним доступом. Наприклад, розумні замки дозволяють автоматично надавати доступ користувачам за допомогою мобільних пристроїв або носимих гаджетів. Хоча IoT-технології забезпечують високу гнучкість, вони також відкривають нові ризики. Зокрема, незахищені IoT-пристрої можуть стати об’єктами атак, як це сталося з інцидентами злому розумних замків через вразливості у мережах Wi-Fi [28].

Таким чином, сучасні технології значно підвищують ефективність СКД, але також вимагають вирішення нових викликів, таких як захист приватності, боротьба з уразливостями та забезпечення точності в роботі систем.

1.4 Сучасні підходи до автентифікації

Методологічна база, що використовується у побудові сучасних СКД, ґрунтується на міжнародних стандартах, таких як ISO/IEC 27001 та NIST SP 800-53. Ці стандарти визначають вимоги до забезпечення інформаційної безпеки, серед яких особливу увагу приділено автентифікації [3].

ISO/IEC 27001 підкреслює важливість політики управління доступом, яка охоплює розподіл ролей, ідентифікацію користувачів, автентифікацію та регулярний аудит дій користувачів. Стандарт NIST SP 800-53 акцентує увагу на використанні динамічних правил автентифікації, контролю доступу на основі ролей RBAC та криптографічних методів захисту облікових даних [4][26].

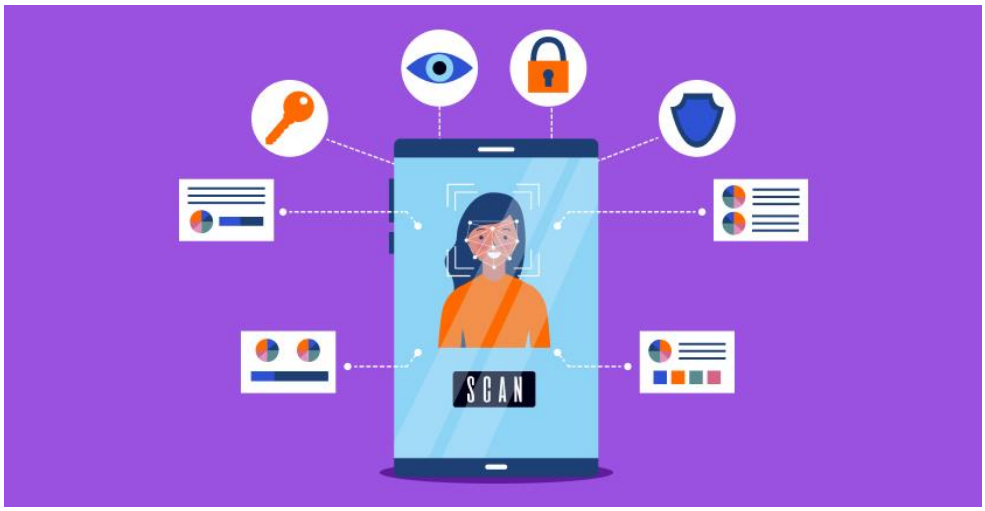


Рис. 1.2 - Основні методи автентифікації

На сьогоднішній день використовують такі методи автентифікації :

- Паролі**:** залишаються базовим методом, однак вимагають регулярного оновлення та складності.
- Токени: виступають фізичним носієм доступу, що додає додатковий рівень захисту.
- Біометрія: дозволяє ідентифікувати користувачів за унікальними характеристиками, такими як відбитки пальців або розпізнавання обличчя [10][14].
- Багатофакторна автентифікація**:** об'єднує кілька методів для підвищення надійності доступу [10][24].

1.4.1 FAR і FRR у популярних системах

Сучасні біометричні системи мають покращену точність, проте ще стикаються з помилками типу FAR — прийняття неавторизованих користувачів, та FRR — відмови у доступі авторизованим користувачам.

Для кількісної оцінки ефективності біометричних систем використовуються два основні показники: FAR та FRR. FAR визначає ймовірність помилкового прийняття неавторизованого користувача та обчислюється за формулою:

$$FAR = \frac{\text{Кількість помилкових приймань}}{\text{Загальна кількість авторизованих спроб}} \quad (1.1)$$

FRR, у свою чергу, показує ймовірність відмови у доступі авторизованому користувачу та обчислюється за формулою:

$$FRR = \frac{\text{Кількість помилкових відмов}}{\text{Загальна кількість авторизованих спроб}} \quad (1.2)$$

Баланс між показниками FAR та FRR є критично важливим для ефективності системи контролю доступу. Надто низький рівень FRR може призводити до підвищення FAR, що збільшує ймовірність несанкціонованого доступу. Водночас, жорсткі налаштування, спрямовані на мінімізацію FAR, можуть підвищити FRR, створюючи незручності для легітимних користувачів. Для візуалізації цього балансу часто будується ROC-крива, яка демонструє залежність між показниками FAR та FRR при різних порогових значеннях. Точка, у якій обидва показники мають однакове значення, визначається як Equal Error Rate і є важливим критерієм для оцінки загальної ефективності системи [10][11].

1.4.2 Інновації у методах автентифікації

Одним із найбільш перспективних підходів є поведінкова біометрія, яка аналізує унікальні патерни поведінки користувачів, такі як натискання клавіш, швидкість набору тексту, рухи миші та спосіб використання пристроїв. Наприклад:

- У банківській сфері поведінкова біометрія використовується для визначення аномальної активності в облікових записах клієнтів, дозволяючи оперативно виявляти шахрайство [10][14].

- У корпоративному середовищі такі системи інтегруються з Zero Trust Security, забезпечуючи динамічний контроль доступу залежно від поведінкових ризиків [13].

1.4.3 Модель Zero Trust Security

Zero Trust Security базується на постійній перевірці автентичності будь-якого запиту. Кожен запит аналізується з урахуванням контексту, такого як місце розташування, тип пристрою, час доби та поведінка користувача. Наприклад, доступ до корпоративних ресурсів може бути заблоковано, якщо запит надходить з невідомого пристрою, навіть якщо облікові дані були введені коректно [13].

Модель Zero Trust також активно впроваджує MFA і шифрування даних для мінімізації ризиків компрометації. За даними Gartner, до 2025 року понад 60% компаній перейдуть на ZTS як основну модель забезпечення безпеки [13].

Рис. 1.3 – Модель Zero Trust

Сучасні системи автентифікації стикаються з наступними викликами:

- Забезпечення точності біометричних систем без шкоди для зручності.

- Захист приватності користувачів, зокрема біометричних та поведінкових даних.
- Інтеграція нових технологій, таких як поведінкова біометрія, у вже існуючі системи безпеки.

Таким чином, сучасні підходи до автентифікації поєднують традиційні методи, такі як паролі, з інноваційними рішеннями, такими як поведінкова біометрія та Zero Trust Security. Ці підходи спрямовані на досягнення балансу між безпекою, зручністю та приватністю користувачів [10][14].

1.5. Загрози інформаційній безпеці на об’єктах інформаційної діяльності

Захист інформаційних об'єктів є однією з найважливіших задач у сучасному цифровому середовищі. Загрози інформаційній безпеці стають дедалі складнішими, що вимагає глибокого аналізу вразливостей та потенційних атак. Основними викликами у цій сфері є як зовнішні, так і внутрішні загрози, що негативно впливають на конфіденційність, цілісність та доступність інформації. До зовнішніх загроз належать різноманітні кібератаки, такі як фішинг, атаки типу «відмова в обслуговуванні» (DDoS) і шкідливе програмне забезпечення, зокрема програми-вимагачі. Яскравим прикладом є атака NotPetya у 2017 році, яка завдала значних збитків багатьом українським організаціям, повністю паралізувавши їхні інформаційні системи. Не менш небезпечною є експлуатація вразливостей систем контролю доступу, зокрема у біометричних рішеннях чи IoT-пристроях, що можуть стати точкою для несанкціонованого доступу. Соціальна інженерія також становить загрозу, оскільки зловмисники маніпулюють користувачами, отримуючи критично важливі облікові дані, як це часто трапляється через фішингові листи [3].

Внутрішні загрози включають інсайдерські атаки, коли співробітники або підрядники з легальним доступом до систем стають причиною витоку даних, як навмисно, так і випадково. Неправильна конфігурація систем контролю доступу є ще одним значним ризиком, адже надто широкі повноваження користувачів створюють додаткові можливості для потенційних атак. Системи контролю

доступу, попри свою критичну роль у забезпеченні безпеки об'єктів інформаційної діяльності, також мають свої вразливості. Біометричні системи часто стикаються з помилками ідентифікації, такими як показники FAR та FRR, що можуть призводити до прийняття неавторизованих користувачів або блокування легітимних. Окремою загрозою є компрометація біометричних даних, оскільки їх витік є незворотним через неможливість зміни фізіологічних характеристик. Подібний випадок стався під час злому платформи *Suprema Biostar* у 2020 році, що спричинив значні наслідки. Крім того, атаки на IoT-пристрої, як-от незахищені смарт-замки чи датчики, можуть стати вразливим місцем для несанкціонованого доступу [10][11].

Серед новітніх загроз особливе місце займають атаки, що використовують штучний інтелект. ШІ дозволяє зловмисникам автоматизувати атаки, генеруючи фішингові листи, які важко відрізнити від легітимних повідомлень, а також обходити автентифікаційні системи, аналізуючи поведінкові шаблони користувачів. Розширення масштабів кібершпигунства стало ще однією актуальною проблемою, оскільки системи контролю доступу можуть використовуватися для збору даних про переміщення осіб, особливо в урядових установах або на критично важливих об'єктах. Використання хмарних технологій для СКД також створює додаткові ризики, пов’язані із захистом даних, особливо за умови слабкого шифрування або відсутності регулярного аудиту безпеки.

Для мінімізації вказаних загроз необхідно впроваджувати комплексний підхід до безпеки, що включає регулярний аудит налаштувань систем контролю доступу для виявлення можливих слабких місць. Додатковим рівнем захисту є інтеграція багатофакторної автентифікації, яка забезпечує надійність доступу завдяки комбінації кількох рівнів перевірки. Важливо також проводити навчання персоналу для протидії методам соціальної інженерії та вдосконалювати їхні навички використання сучасних методів автентифікації. Використання блокчейн-технологій для створення прозорих та незмінних журналів доступу є перспективним рішенням, що підвищує рівень прозорості та захисту систем контролю доступу.

Таким чином, забезпечення захисту інформаційної діяльності в умовах сучасних кіберзагроз вимагає комплексного підходу, що поєднує технологічні інновації з дотриманням міжнародних стандартів безпеки. Реалізація запропонованих заходів дозволяє значно зменшити ризики компрометації систем, підвищити надійність захисту інформації та зберегти її конфіденційність, цілісність і доступність в умовах динамічного розвитку цифрового середовища [3].

1.5.1. Уразливості систем контролю доступу

Уразливості СКД становлять значний ризик для забезпечення інформаційної безпеки на об’єктах інформаційної діяльності. Вони можуть виникати через слабкі сторони фізичних, біометричних і технічних компонентів систем, що робить можливим їх експлуатацію зловмисниками. Усвідомлення таких уразливостей є важливим кроком для створення більш надійних систем захисту.

Фізичні механізми, які використовуються у СКД, часто є першою лінією захисту, але вони також можуть бути серйозним джерелом уразливостей. Наприклад, картки доступу, що базуються на RFID або магнітних стрічках, можуть бути легко дубльовані за допомогою спеціалізованих пристроїв. Зловмисники можуть створити дублікат картки доступу, який дозволить їм обійти систему безпеки. Також поширеним є обхід фізичних замків, зокрема за допомогою майстер-ключів або технічних інструментів для злому, що вказує на необхідність постійного вдосконалення конструкцій замків та використання багатофакторної автентифікації навіть для фізичних бар’єрів.

Біометричні системи, незважаючи на їхній високий потенціал щодо забезпечення безпеки, також мають низку вразливостей. Основною проблемою є помилки розпізнавання, які можуть призводити до відмови в доступі для законних користувачів або, навпаки, до помилкового надання доступу зловмисникам. Використання підроблених біометричних даних, таких як штучно створені відбитки пальців, відскановані зображення облич або підроблені голосові записи, становить серйозну загрозу для таких систем. Ці методи можуть бути особливо

ефективними в разі відсутності механізмів додаткової перевірки, таких як аналіз живого сигналу [21][29].

Мережеві системи контролю доступу також мають низку технічних уразливостей, пов’язаних із недостатнім рівнем шифрування або іншими недоліками у забезпеченні конфіденційності переданих даних. Якщо дані, які передаються між компонентами СКД, такими як контролери або сервери, не шифруються належним чином, вони можуть бути перехоплені зловмисниками. Це створює ризик несанкціонованого доступу до системи або маніпуляції її даними. Крім того, деякі системи можуть страждати від уразливостей програмного забезпечення, таких як помилки в прошивці або відсутність оновлень безпеки, які залишають їх відкритими для експлуатації.

Ці уразливості підкреслюють важливість багаторівневого підходу до проєктування та впровадження СКД. Поєднання надійних фізичних засобів, сучасних біометричних технологій з аналізом живого сигналу, а також забезпечення високого рівня шифрування і регулярного оновлення програмного забезпечення є ключовими для мінімізації ризиків [21].

1.6. Висновок до першого розділу

У першому розділі магістерської роботи "Теоретичні основи захисту інформації та систем контролю доступу" проведено комплексний аналіз ключових аспектів інформаційної безпеки, сучасних підходів до побудови СКД та технологій, які забезпечують захист об’єктів інформаційної діяльності.

Було визначено, що інформаційна безпека базується на трьох фундаментальних принципах: конфіденційність, цілісність і доступність інформації. Ці принципи є основою для побудови ефективних систем захисту, зокрема в контексті сучасних викликів, таких як глобальні кібератаки, зростання використання хмарних платформ і посилення вимог до захисту персональних даних (GDPR, ISO/IEC 27001) [1][2].

Розглянуто історичну еволюцію методів захисту інформації — від фізичних механізмів і шифрувальних машин до інтеграції штучного інтелекту, блокчейну та IoT у сучасні СКД. Акцент зроблено на значущості інноваційних технологій, таких як біометричні системи, MFA та аналіз поведінкових патернів, що дозволяють суттєво підвищити ефективність і точність захисту.

Особливу увагу приділено аналізу загроз інформаційній безпеці, серед яких кібератаки, соціальна інженерія, компрометація біометричних даних і уразливості IoT-пристроїв. Визначено, що впровадження багаторівневих механізмів захисту, таких як Zero Trust Security, здатне мінімізувати вплив зазначених загроз на інформаційні системи [13].

Проведено класифікацію систем контролю доступу за їхньою функціональністю та технологічною основою. Описано переваги та недоліки фізичних, електронних, логічних і гібридних СКД. У роботі наголошено на важливості аудиту, моніторингу подій і інтеграції СКД з іншими елементами системи інформаційної безпеки, такими як відеоспостереження та шифрування даних [1].

Таким чином, у цьому розділі закладено теоретичну основу для подальшого дослідження сучасних систем контролю доступу, їхньої ролі у забезпеченні інформаційної безпеки на об’єктах інформаційної діяльності, а також розробки рекомендацій для практичного впровадження цих технологій у різних галузях. Висновки, отримані у першому розділі, дозволяють перейти до глибшого аналізу практичних аспектів захисту інформації у наступних розділах роботи.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

2.1. Огляд популярних рішень

Сучасні СКД є невід’ємною частиною інформаційної безпеки, забезпечуючи управління доступом до фізичних і цифрових ресурсів. Основною метою таких систем є обмеження доступу до конфіденційних даних, критичних об'єктів і ресурсів лише для авторизованих осіб, що дозволяє мінімізувати ризики несанкціонованого доступу. У сучасному світі, де цифровізація охоплює практично всі галузі, важливість надійних СКД зростає, адже від їхньої ефективності залежить безпека даних, ресурсів і репутація організацій [28].

Розвиток інформаційних технологій значно змінив підхід до створення та функціонування СКД. Традиційні методи, які базувалися на використанні паролів або фізичних ключів, поступово доповнюються або замінюються більш інноваційними рішеннями. Серед сучасних тенденцій спостерігається стрімке впровадження біометричних технологій, MFA, штучного інтелекту, блокчейну та IoT-рішень. Ці технології дозволяють суттєво підвищити точність і адаптивність систем, роблячи їх більш ефективними навіть у складних і динамічних середовищах [28].

Важливо зазначити, що сучасні СКД є не лише засобом забезпечення доступу до ресурсів, але й інструментом управління безпекою в реальному часі. Завдяки інтеграції з іншими системами безпеки, такими як відеоспостереження, фаєрволи та системи моніторингу подій SIEM, вони забезпечують комплексний підхід до захисту, поєднуючи фізичний і цифровий контроль. Це особливо актуально для організацій, які працюють у режимі розподілених офісів або використовують гібридні інфраструктури.

До найбільш популярних платформ, які займають провідні позиції на ринку СКД, належать Cisco Identity Services Engine**,** Fortinet Access Management та Microsoft Azure AD Conditional Access. Кожна з цих платформ розроблена для задоволення потреб різних категорій організацій: від малих підприємств до

великих корпорацій та урядових установ. У наступних підрозділах детально розглянуто їхні функціональні можливості, виклики та приклади використання.

2.1.1 Методологія відбору систем контролю доступу

Відбір СКД є критично важливим етапом у забезпеченні інформаційної безпеки організацій. У сучасних умовах вибір СКД залежить не лише від технічних характеристик, але й від їхньої відповідності міжнародним стандартам, здатності інтегруватися в існуючу інфраструктуру, а також адаптації до швидкоплинних умов бізнесу. Методологія відбору базується на кількох ключових критеріях, які визначають ефективність, надійність і економічну доцільність впровадження систем.

Одним із головних критеріїв є відповідність систем міжнародним стандартам, таким як ISO/IEC 27001, NIST SP 800-53 або GDPR. Ці стандарти встановлюють чіткі вимоги до конфіденційності, цілісності та доступності інформації. СКД, що відповідають цим стандартам, дозволяють організаціям не лише підвищувати рівень безпеки, але й уникати штрафів за недотримання регуляторних вимог у різних юрисдикціях [4][9].

У світі, де все більше компаній переходять на хмарні сервіси, здатність СКД працювати в хмарних середовищах стає критичною. Системи, які інтегруються з хмарними платформами (наприклад, Microsoft Azure або Amazon Web Services), дозволяють забезпечити захист даних у географічно розподілених структурах. Підтримка хмарних рішень також сприяє підвищенню доступності даних і зниженню витрат на інфраструктуру.

Сучасні організації мають змогу швидко зростати, тому масштабованість системи є важливим аспектом. СКД повинна дозволяти додавання нових користувачів, пристроїв або ресурсів без необхідності заміни існуючого обладнання чи системного програмного забезпечення. Масштабовані системи можуть адаптуватися до потреб малих підприємств і великих корпорацій, забезпечуючи однаково високий рівень безпеки.

Економічна ефективність є важливим критерієм при виборі СКД. Оцінка вартості володіння (Total Cost of Ownership) включає витрати на впровадження, ліцензії, обслуговування та оновлення. Організації прагнуть знайти баланс між високим рівнем безпеки та мінімізацією фінансових витрат. Системи, що пропонують гнучкі моделі ліцензування (наприклад, на основі підписок), стають все більш популярними.

Сумісність із існуючими інфраструктурами. Інтеграція з існуючими інфраструктурами є ще одним ключовим фактором. СКД має бути сумісною з поточними мережами, програмним забезпеченням і апаратними рішеннями, такими як фаєрволи, SIEM-системи та платформи автентифікації. Це забезпечує мінімізацію часу та витрат на інтеграцію, а також спрощує управління.

2.1.2. Cisco ISE

Cisco ISE є комплексним рішенням для управління доступом до мережі, яке поєднує функціональність автентифікації, авторизації та моніторингу дій користувачів. Основна перевага Cisco ISE полягає у впровадженні контекстуальних політик доступу, що враховують ідентифікацію користувача, характеристики пристрою, місце розташування та рівень ризику запиту. Наприклад, доступ до ресурсів може бути дозволений лише з корпоративних пристроїв, які відповідають стандартам безпеки. Завдяки використанню профілювання пристроїв, система може автоматично визначати тип підключеного обладнання, його конфігурацію та стан безпеки [6].

Система дозволяє автоматично перевіряти пристрої на відповідність вимогам безпеки, зокрема щодо оновлення антивірусного програмного забезпечення, наявності шифрування даних або встановлення актуальних патчів. У разі виявлення невідповідностей Cisco ISE здатна автоматично ізолювати пристрій, обмежуючи його доступ до мережі до моменту усунення проблем. Завдяки цьому мінімізуються ризики, пов’язані з використанням незахищених або вразливих пристроїв [6].

Cisco ISE інтегрується з іншими рішеннями Cisco та сторонніми продуктами, такими як SIEM-системи для аналізу подій безпеки, NGFW (Next-Generation Firewall) для посиленого контролю мережевого трафіку, а також системами NAC (Network Access Control) для повноцінного управління доступом. Особливістю платформи є її можливість інтеграції з технологіями хмарного захисту та управління трафіком.

Концепція BYOD (Bring Your Own Device), підтримувана Cisco ISE, особливо корисна для сучасних організацій, які дозволяють співробітникам використовувати власні пристрої для робочих завдань. Система здатна розділяти корпоративний і особистий трафік, обмежуючи доступ до критично важливих даних лише авторизованим користувачам і пристроям, які відповідають встановленим вимогам. У секторі охорони здоров’я Cisco ISE забезпечує захист медичних даних, контролюючи підключення пристроїв лікарів та медичного обладнання, а також обмежує доступ до чутливої інформації відповідно до рівня прав користувача [6].

Додатково Cisco ISE підтримує функціональність динамічного контролю доступу на основі політик, що дозволяє автоматично змінювати рівень доступу в залежності від поведінкових патернів користувача чи виявлення потенційних загроз. Наприклад, при спробі входу з невідомого місця або в неробочий час система може вимагати додаткову автентифікацію або обмежити доступ лише базовими привілеями. Це робить Cisco ISE ефективним рішенням для організацій, які впроваджують Zero Trust Security, де кожен запит до мережі розглядається як потенційно небезпечний та проходить багатоетапну перевірку [6].

Таким чином, Cisco ISE є гнучким і потужним інструментом для організації комплексного захисту мережі, забезпечуючи високий рівень контролю, автоматизації та відповідності сучасним стандартам кібербезпеки.

2.1.3. Fortinet Access Management

Fortinet Access Management є ключовою складовою екосистеми Fortinet Security Fabric, що забезпечує інтеграцію фізичного та цифрового контролю

доступу. Основним підходом системи є динамічний контроль доступу, що змінюється залежно від контексту запиту. Платформа аналізує параметри запиту, такі як місце розташування користувача, тип пристрою, час доступу та рівень ризику. Наприклад, система може заблокувати запит, якщо він надходить із пристрою, що не відповідає політикам безпеки, або з регіону, що має підвищений рівень загроз. Додатково Fortinet Access Management підтримує механізм **адаптивного контролю доступу**, що дозволяє автоматично коригувати права користувача на основі його дій або змін у мережевому середовищі [7].

Fortinet активно використовує MFA, що комбінує паролі, апаратні токени та біометричні дані, для мінімізації ризиків несанкціонованого доступу. Зокрема, токени FortiToken забезпечують генерацію одноразових паролів, що підвищує рівень безпеки, особливо для критичних інфраструктур, таких як банківські системи. У банківському секторі рішення Fortinet надає можливість багаторівневого контролю доступу, інтегруючи захищені VPN-з'єднання, що дозволяє безпечно підключатися до корпоративних ресурсів з віддалених локацій, а також запобігає атакам з боку неавторизованих користувачів.

Особливістю системи є її тісна інтеграція з іншими продуктами Fortinet, такими як NGFW, FortiGate VPN та FortiAnalyzer. Завдяки цьому створюється єдина централізована захищена інфраструктура, яка забезпечує комплексне управління мережею, моніторинг трафіку та аналіз інцидентів безпеки у режимі реального часу. Наприклад, у разі виявлення підозрілої активності в одному із сегментів мережі, система може автоматично відключити пристрій від мережі або обмежити його доступ.

Fortinet Access Management також підтримує технології сегментації мережі, які дозволяють розділяти внутрішню інфраструктуру на ізольовані зони для мінімізації ризику поширення загроз. У поєднанні з функцією FortiNAC (Network Access Control), система забезпечує контроль і управління підключеннями, включно з IoT-пристроями, які часто стають вразливими точками мережі. Також платформа використовує функціонал поведінкового аналізу, який дозволяє

виявляти аномалії у діях користувачів і реагувати на потенційні загрози до їх повної реалізації [7][28].

Таким чином, Fortinet Access Management є комплексним рішенням, що забезпечує динамічний та адаптивний контроль доступу, високий рівень інтеграції з іншими системами безпеки та можливість побудови надійної захищеної інфраструктури. Завдяки впровадженню сучасних методів автентифікації, глибокої сегментації мережі та поведінкового аналізу, ця система відповідає вимогам сучасної кібербезпеки і є ефективним інструментом для організацій, які прагнуть мінімізувати ризики несанкціонованого доступу та захистити свої ресурси від складних загроз.

2.1.4. Microsoft Azure AD Conditional Access

Microsoft Azure AD Conditional Access — це хмарне рішення, яке забезпечує динамічний контроль доступу на основі умовних правил і політик безпеки. Основна функціональність платформи полягає у використанні контекстуальних даних для прийняття рішень щодо надання чи обмеження доступу до ресурсів. Політики платформи враховують широкий спектр параметрів, таких як місце розташування користувача, тип пристрою, стан пристрою, рівень ризику і навіть поведінкові патерни. Наприклад, доступ до конфіденційних даних може вимагати додаткової автентифікації, якщо запит надходить із невідомого пристрою, або може бути заблокований, якщо спроба входу виявлена з регіону з високим рівнем загроз [8].

Azure AD Conditional Access підтримує MFA, що дозволяє значно підвищити безпеку облікових записів, вимагаючи додаткове підтвердження особи через SMS, мобільні додатки або біометричні дані. У разі виявлення потенційного ризику, як-от незвичний вхід або спроба доступу з небезпечного IP-адресу, система автоматично застосовує поглиблені заходи безпеки, такі як блокування облікового запису або вимога негайного оновлення пароля. Однією з ключових переваг платформи є її адаптивність, оскільки вона може в реальному часі змінювати політики доступу залежно від поточних загроз і поведінки користувача.

Платформа широко застосовується не лише в урядових установах, а й у корпоративному секторі для захисту критично важливих ресурсів та даних. Наприклад, у Великобританії Azure AD Conditional Access використовується для забезпечення безпеки державних службовців під час доступу до хмарних ресурсів, що дозволяє ефективно обмежувати несанкціоновані спроби входу з підозрілих регіонів або пристроїв, які не відповідають вимогам політик. У корпоративному середовищі платформа дозволяє організаціям впроваджувати політики відповідності для пристроїв, які підключаються до хмарних систем. Наприклад, якщо пристрій не відповідає вимогам щодо шифрування даних або не має встановленого антивірусного програмного забезпечення, доступ до ресурсів може бути обмежений [8].

Особливістю Azure AD Conditional Access є можливість інтеграції з іншими інструментами Microsoft, такими як Microsoft Defender for Cloud, Azure Sentinel і Microsoft Intune, що забезпечує комплексний підхід до кібербезпеки. Така інтеграція дозволяє не лише контролювати доступ, але й моніторити активність користувачів, аналізувати ризики та оперативно реагувати на загрози. Завдяки функціоналу Risk-Based Conditional Access, платформа автоматично аналізує ризик запитів на доступ за допомогою алгоритмів машинного навчання, що дозволяє виявляти аномальну активність і забезпечувати додаткові рівні перевірки у разі виявлення загрози [8].

Таким чином, Microsoft Azure AD Conditional Access є потужним інструментом для забезпечення безпеки доступу до хмарних ресурсів, що враховує контекст і ризики запиту для мінімізації ймовірності несанкціонованого доступу. Завдяки високій гнучкості, інтеграції з іншими рішеннями Microsoft і підтримці адаптивних політик безпеки, платформа є ефективним рішенням для державних установ та корпоративного сектору, які прагнуть забезпечити високий рівень захисту інформаційних ресурсів у сучасному цифровому середовищі .

2.1.5. Практичне впровадження та аналіз у різних секторах

Практичне впровадження СКД у різних секторах демонструє їхню здатність забезпечувати високий рівень захисту даних та ресурсів у різних галузях. Сучасні СКД завдяки своїй адаптивності та функціональності стали невід'ємною частиною інформаційної безпеки організацій різного масштабу — від медичних установ до урядових структур і критично важливих об'єктів. Нижче наведено аналіз використання Cisco ISE, Fortinet Access Management та Microsoft Azure AD Conditional Access у конкретних секторах, з акцентом на їхні переваги, виклики та відповідність стандартам.

1) До корпоративних секторів використовується:

- **Cisco ISE:** У корпоративному середовищі Cisco ISE забезпечує безпечний доступ до мережі завдяки підтримці адаптивних політик доступу. Одним із ключових сценаріїв є впровадження концепції BYOD, що дозволяє співробітникам використовувати особисті пристрої. Наприклад, у багатонаціональних компаніях Cisco ISE автоматично перевіряє відповідність пристроїв стандартам безпеки, таким як оновлення антивірусного програмного забезпечення або встановлення актуальних патчів. Це відповідає стандартам ISO/IEC 27001 та допомагає уникнути ризиків витоку даних через небезпечні пристрої [3][26].

- **Fortinet Access Management:** Ця система широко застосовується у фінансових установах для забезпечення багаторівневого захисту. У банківському секторі система дозволяє реалізувати MFA, яка включає використання одноразових паролів або біометричних даних. Наприклад, великий банк інтегрував Fortinet для контролю доступу до серверів із конфіденційною клієнтською інформацією, дотримуючись стандартів PCI DSS.

- **Microsoft Azure AD Conditional Access:** Ця система ідеально підходить для хмарно-орієнтованих компаній. Microsoft Azure AD Conditional Access дозволяє встановлювати політики доступу на основі контексту, таких як геолокація чи тип пристрою. Наприклад, IT-компанія, яка використовує Microsoft 365, може

обмежити доступ до конфіденційних даних із незнайомих пристроїв, що забезпечує відповідність стандартам SOC 2.

2) До урядових установ відноситься:

- **Cisco ISE:** Активно використовується у державних установах для забезпечення безпеки критичних даних. Наприклад, у Міністерстві оборони система дозволяє сегментувати мережу, розмежовуючи доступ до військових і адміністративних ресурсів. Це відповідає стандартам NIST SP 800-53 і гарантує, що тільки авторизовані користувачі мають доступ до чутливих даних [4].
- **Fortinet Access Management:** У будівлях урядових установ Fortinet забезпечує як фізичний, так і цифровий контроль доступу. Наприклад, доступ до серверних кімнат контролюється за допомогою біометричних даних, що відповідає вимогам GDPR. Це дозволяє захистити персональні дані державних службовців і запобігти несанкціонованому доступу до критичних об’єктів [4][9].
- **Microsoft Azure AD Conditional Access:** Забезпечує надійний захист хмарних сервісів для урядових установ. Наприклад, у Великобританії ця система дозволяє встановлювати умовні політики доступу до державних баз даних, використовуючи багатофакторну автентифікацію та обмежуючи доступ із небезпечних географічних регіонів.

3) До критично важливих об’єктів:

- **Cisco ISE:** Для критично важливих об’єктів, таких як енергетичні станції чи транспортні хаби, Cisco ISE забезпечує захист операційних мереж. Наприклад, система використовується для сегментації мережі SCADA, що дозволяє обмежити доступ лише для авторизованих користувачів. Це відповідає стандартам IEC 62443, які регулюють безпеку інфраструктури [6].
- **Fortinet Access Management:** Fortinet застосовується для захисту об’єктів підвищеного ризику, таких як транспортна інфраструктура. Наприклад, система контролює доступ до операційних центрів аеропортів, використовуючи біометричні методи автентифікації, що дозволяє дотримуватися стандартів Transported Asset Protection Association [7].

- **Microsoft Azure AD Conditional Access:** Широко застосовується на об’єктах, що використовують хмарні технології. Наприклад, міжнародні аеропорти інтегрують платформу для захисту баз даних польотів та централізованих серверів, впроваджуючи умовні політики доступу, які враховують роль користувача та тип пристрою [8].

Однією з ключових переваг обраних платформ є їхня здатність інтегруватися в гібридних середовищах, де поєднуються локальні та хмарні інфраструктури. Наприклад, у великих корпораціях Cisco ISE використовується для контролю доступу до локальних серверів, тоді як Microsoft Azure AD Conditional Access захищає хмарні ресурси. Це дозволяє створити багаторівневу систему безпеки, яка відповідає вимогам сучасних організацій із розподіленими командами.

2.2. Недоліки сучасних рішень з урахуванням організаційних чинників

СКД часто стикаються з фундаментальними проблемами оцінки точності ідентифікації користувачів, які описуються показниками FAR і FRR.

1) FAR — це відсоток випадків, коли система помилково надає доступ неавторизованим користувачам. Високий FAR становить загрозу для безпеки організації, оскільки зловмисники можуть отримати доступ до захищених ресурсів.

2) FRR — це відсоток випадків, коли система помилково відмовляє у доступі авторизованим користувачам. Високий FRR може знижувати продуктивність роботи, викликати невдоволення серед персоналу та збільшувати операційні витрати [10][11].

Обидва показники є критичними для забезпечення балансу між безпекою та зручністю користування СКД [3]. Вплив організаційних чинників, таких як кадрова політика, навчання персоналу та внутрішні регламенти, відіграє ключову роль у зниженні цих помилок [3].

СКД є фундаментальним елементом забезпечення інформаційної безпеки в організаціях. Вони дозволяють ефективно обмежувати доступ до критичних ресурсів та забезпечують захист від кіберзагроз. Однак навіть найбільш інноваційні

рішення мають певні недоліки, які проявляються не лише в технічному, але й у організаційному контексті. Успішне впровадження та експлуатація СКД залежать не лише від технологій, що використовуються, але й від людського фактора, внутрішніх процесів і процедур, які регламентують їхню роботу.

В організаційній площині недоліки сучасних СКД проявляються через такі фактори, як недостатнє навчання персоналу, відсутність регламентованих процесів моніторингу та реагування, а також низький рівень адаптації системи до специфіки організації. Відсутність уваги до цих аспектів може призводити до зростання ймовірності помилок, таких як FAR і FRR, що знижує загальну ефективність системи [10][11].

Крім того, уразливості біометричних систем та технічна складність налаштування інфраструктури СКД додають викликів, особливо в умовах обмежених ресурсів і низької кваліфікації персоналу. Таким чином, аналіз недоліків сучасних рішень потребує комплексного підходу, який охоплює як технічні, так і організаційні аспекти їхньої експлуатації.

2.2.1. Ймовірність помилок FAR, FRR

Однією з найбільш значущих проблем сучасних СКД є наявність помилок ідентифікації, які виражаються у вигляді показників FAR і FRR. FAR характеризує частку випадків, коли система помилково ідентифікує неавторизованого користувача як авторизованого, що створює прямий ризик компрометації даних і ресурсів. FRR, у свою чергу, показує частку ситуацій, коли система блокує доступ легітимним користувачам, негативно впливаючи на продуктивність організації [10][11].

Помилки цього типу мають багатофакторну природу. З одного боку, вони можуть бути зумовлені технічними недоліками обладнання або алгоритмів автентифікації. З іншого боку, важливу роль у формуванні цих помилок відіграють організаційні чинники, які визначають, наскільки ефективно впроваджена і керується система. Наприклад, недостатнє навчання персоналу, який відповідає за

налаштування СКД, може призвести до неправильного визначення порогових значень автентифікації, що є ключовим параметром для балансу між FAR і FRR. У багатьох випадках організації не враховують особливості роботи свого персоналу, що також впливає на точність і ефективність СКД.

Навчання користувачів є ще одним критичним фактором. Наприклад, у біометричних системах персонал має розуміти, як правильно користуватися обладнанням, таким як сканери відбитків пальців або розпізнавачі обличчя. Невірне розташування пальця на сенсорі або недотримання стандартних процедур сканування може спричиняти значне збільшення показника FRR. Це особливо актуально для сфер із високими вимогами до точності, таких як медицина або банківська справа [10][11].

Внутрішні регламенти організації також мають значний вплив на рівень помилок. Наприклад, відсутність чітко встановлених процедур моніторингу й аналізу роботи СКД ускладнює виявлення причин підвищеного FAR чи FRR. Регулярний аудит системи, включаючи перевірку її налаштувань і аналіз журналів доступу, є необхідною умовою для мінімізації помилок. Більш того, організації повинні враховувати, що навіть невеликі зміни у складі персоналу або умовах експлуатації можуть вимагати переналаштування системи.

Практичний аналіз роботи СКД у різних галузях демонструє специфічні виклики. Наприклад, у корпоративному секторі використання біометричних систем із низьким рівнем навчання користувачів часто призводить до помилкових відмов, що уповільнює бізнес-процеси. У медичних установах, де обробляються чутливі дані, навіть одиничний випадок FAR може призвести до серйозних порушень конфіденційності та відповідальності перед законом. У таких випадках важливим є впровадження багаторівневого захисту, який зменшує ймовірність помилок, використовуючи додаткові методи автентифікації [10][11].

Таким чином, зниження FAR і FRR вимагає комплексного підходу, що охоплює як технічні, так і організаційні аспекти роботи СКД. Регулярний аудит, навчання персоналу та впровадження ефективних внутрішніх регламентів є

ключовими заходами для забезпечення точності і надійності сучасних систем контролю доступу.

2.2.2. Уразливості біометричних систем

Біометричні системи автентифікації, що ґрунтуються на унікальних фізіологічних або поведінкових характеристиках користувачів, є одними з найсучасніших засобів забезпечення доступу до ресурсів. Висока точність таких систем, їхній зручний функціонал і здатність автоматично адаптуватися до умов експлуатації зробили їх популярними в різних галузях. Однак ця технологія має ряд вразливих місць, що обумовлено як технічними недоліками, так і організаційними проблемами, що часто виникають через неналежне управління та підтримку.

Однією з головних загроз є можливість витоку або компрометації біометричних даних. Унікальність таких даних, як відбитки пальців, зображення обличчя або зразки голосу, ускладнює їхнє відновлення у випадку компрометації, що робить проблему захисту цих даних критично важливою. Додатково, складність впровадження стандартів захисту, недостатнє навчання персоналу та відсутність чітких регламентів щодо аудиту таких систем створюють значні ризики для організацій.

Ефективне використання біометричних систем значною мірою залежить від рівня організаційної підтримки. Для мінімізації ризиків необхідно інтегрувати комплекс заходів, що включають підготовку персоналу, регулярний аудит систем і дотримання сучасних стандартів безпеки.

Навчання персоналу відіграє ключову роль у мінімізації помилок і зниженні ризиків, пов’язаних із неправильним використанням біометричних пристроїв. Персонал повинен бути обізнаний із технічними особливостями обладнання, такими як сканери відбитків пальців або сенсори розпізнавання обличчя, та навчений розпізнавати спроби зловмисників обійти систему. Регулярні тренінги допомагають забезпечити належний рівень компетенції працівників і підвищують загальний рівень безпеки.

Регулярний аудит є важливим інструментом для моніторингу роботи біометричних систем. Перевірка налаштувань, аналіз журналів доступу та тестування на стійкість до атак допомагають виявити слабкі місця системи. Наприклад, аудит може виявити некоректно встановлені порогові значення, які можуть спричиняти високий рівень хибних прийняттів або відмов. Такі заходи є особливо актуальними в умовах стрімкого розвитку кіберзагроз.

Дотримання міжнародних стандартів також має вирішальне значення. Такі стандарти, як ISO/IEC 27018, регламентують принципи безпечного зберігання та обробки біометричних даних, що включає шифрування інформації, обмеження доступу до неї та впровадження механізмів моніторингу. Рекомендації NIST визначають застосування криптографічних алгоритмів, таких як AES-256, для забезпечення захисту даних, а також закликають до мінімізації обсягу зібраної інформації [3][26].

Останні роки ознаменувалися кількома масштабними інцидентами, що продемонстрували вразливість біометричних систем. Серед них найбільш резонансним став витік даних Suprema Biostar у 2019 році, коли було розкрито понад 27,8 мільйонів записів. Відсутність шифрування даних і неналежна конфігурація доступу стали основними причинами цього інциденту.

У 2023 році також було зафіксовано кілька серйозних витоків. Один із найбільших інцидентів пов’язаний із уразливістю у програмному забезпеченні MOVEit, що призвело до компрометації інформації понад 2 393 організаці. Хоча основна частина даних стосувалася особистої інформації, цей випадок підкреслив ризики для платформ, які обробляють біометричні дані.

Інший помітний випадок стосується компанії 23andMe, яка спеціалізується на генетичних тестах. У результаті атаки було скомпрометовано дані клієнтів, що ще раз акцентувало увагу на важливості безпеки для систем, які працюють із біометричними і генетичними даними.

Уразливості біометричних систем підкреслюють необхідність впровадження комплексних організаційних заходів, зокрема навчання персоналу, регулярного аудиту та дотримання міжнародних стандартів захисту даних.

2.2.3. Інфраструктурні проблеми

Інфраструктурні проблеми є однією з найбільших перешкод для ефективного функціонування СКД, оскільки вони впливають на стабільність, безпеку та надійність роботи цих систем. СКД як багатокомпонентні системи залежать від злагодженої роботи програмного забезпечення, апаратних засобів і мережевої інфраструктури. Проблеми, пов’язані з інфраструктурою, можуть бути спричинені як технічними аспектами, так і управлінськими помилками, що знижує ефективність захисту і створює додаткові ризики для організацій.

Однією з ключових проблем є відсутність резервних каналів зв’язку, які забезпечують стабільність роботи СКД у разі збою основного каналу. Резервні канали потрібні для захисту від можливих порушень у роботі системи, які можуть бути спричинені кібератаками, технічними несправностями або перебоями в електропостачанні. Наприклад, у великих організаціях, які використовують централізовані системи автентифікації, збій основного каналу зв’язку може повністю заблокувати доступ до ресурсів, що вплине на операційну діяльність і навіть спричинить значні фінансові втрати. У разі відсутності резервування працівники можуть втратити доступ до критичних об’єктів, а СКД стають вразливими до зловмисних дій. Для вирішення цієї проблеми необхідно впроваджувати стратегії резервування, які включають дублювання каналів передачі даних, створення автономних точок доступу та використання систем моніторингу мережевої інфраструктури для раннього виявлення збоїв [17][18].

Ще одним важливим викликом є недостатній рівень кваліфікації IT-персоналу, який відповідає за впровадження, налаштування та обслуговування СКД. Сучасні системи є високотехнологічними рішеннями, що вимагають від спеціалістів глибоких знань і навичок для забезпечення їхньої стабільної роботи. Неправильне налаштування СКД, зокрема параметрів автентифікації або мережевих з’єднань, може призводити до збільшення ймовірності FAR або відмов FRR. Наприклад, недостатньо підготовлений персонал може не помітити спроб зловмисників обійти систему або неправильно відреагувати на сповіщення про

підозрілу активність. Важливою складовою вирішення цієї проблеми є впровадження програм навчання та сертифікації IT-фахівців, орієнтованих на сучасні стандарти кібербезпеки, такі як ISO/IEC 27001 або NIST SP 800-53. Навчання має включати моделювання реальних інцидентів і впровадження найкращих практик реагування на загрози [3][26].

Недоліки в процедурах оновлення є ще одним критичним фактором, який впливає на безпеку та стабільність роботи СКД. Застаріле програмне забезпечення, яке не отримує регулярних оновлень, стає вразливим до новітніх атак, а відсутність чітких регламентів оновлення створює додаткові ризики для організацій. Наприклад, уразливості в прошивках біометричних сканерів можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи або викрадення біометричних даних. Для забезпечення захисту від таких загроз організації повинні впроваджувати політики управління оновленнями, що включають регулярне тестування нових версій програмного забезпечення на сумісність із наявною інфраструктурою, а також планування безпечного впровадження оновлень без ризику для функціонування системи. Крім того, використання автоматизованих систем моніторингу, які повідомляють про необхідність оновлення, дозволяє знизити ризик пропуску критичних патчів [3].

Наслідки інфраструктурних проблем часто мають серйозний вплив на операційну діяльність організацій. Наприклад, збій у роботі серверів, які відповідають за автентифікацію користувачів, може спричинити повне припинення роботи підприємства. У медичних установах збої в системах доступу можуть становити загрозу життю пацієнтів, оскільки персонал не матиме доступу до необхідних даних або обладнання. У промислових компаніях подібні збої можуть зупинити виробничі процеси, що спричинить значні фінансові збитки. Наприклад, у 2023 році збій в енергетичній компанії через відсутність резервного каналу зв’язку призвів до втрат понад 5 мільйонів доларів. Такі приклади підкреслюють важливість резервування інфраструктури та впровадження чітких процедур управління системами.

Таким чином, інфраструктурні проблеми є серйозним викликом для організацій, які використовують системи контролю доступу. Відсутність резервних каналів, низька кваліфікація IT-персоналу та недоліки в процедурах оновлення значно знижують ефективність роботи СКД та збільшують ризики для організацій. Для їх вирішення необхідно впроваджувати комплексний підхід, який включає резервування ресурсів, навчання персоналу та автоматизацію процесів управління інфраструктурою. Лише за умови дотримання цих заходів можна забезпечити стабільну та безпечну роботу систем контролю доступу.

2.3. Математичний аналіз систем контролю доступу

Математичний аналіз є ключовим інструментом для оцінки ефективності СКД. Він дозволяє формалізувати процеси автентифікації та ідентифікації, визначати основні показники ефективності системи, такі як FAR і FRR, і знаходити оптимальний баланс між безпекою та зручністю використання. Завдяки цьому аналізу можна здійснити порівняння різних технологій, визначити слабкі місця системи та запропонувати методи їхнього усунення [10][11].

СКД базуються на використанні складних алгоритмів автентифікації, які вимагають точного налаштування порогових значень для розпізнавання користувачів. Наприклад, у біометричних системах параметри алгоритмів розпізнавання обличчя чи відбитків пальців повинні бути оптимізовані для досягнення мінімальних значень FAR і FRR. Якщо порогові значення занадто низькі, це збільшує ризик помилкового прийняття неавторизованих користувачів, що створює потенційну загрозу для інформаційної безпеки. Навпаки, високі порогові значення можуть призводити до відмови в доступі легітимним користувачам, що знижує продуктивність організації [11].

Ключовою метою математичного аналізу є не лише оцінка поточного стану системи, але й прогнозування її поведінки в різних сценаріях. Наприклад, можна моделювати, як зміниться ефективність системи за умов підвищення навантаження, зміни кількості користувачів чи введення нових методів автентифікації. Крім того,

математичні моделі дозволяють оцінювати взаємозв’язок між показниками безпеки та економічними витратами на впровадження і підтримку СКД.

Особливе значення має побудова ROC-кривих, які демонструють залежність між рівнем помилкових прийняттів і відмов у системі за різних налаштувань порогових значень. Аналіз цих кривих дозволяє визначити оптимальні параметри роботи системи залежно від її призначення. Наприклад, у банківських установах важливіше мінімізувати FAR, навіть якщо це призведе до підвищення FRR, тоді як у медичних установах необхідно знайти баланс між цими показниками, щоб забезпечити швидкий доступ до критично важливих ресурсів [10].

Математичний аналіз також дозволяє інтегрувати статистичні методи для обробки великих масивів даних, зібраних під час роботи СКД. Використання розподілів імовірностей і методів регресійного аналізу допомагає прогнозувати ймовірність виникнення помилок у залежності від часу доби, місця доступу або інших контекстних факторів. Такий підхід забезпечує адаптивність СКД до реальних умов експлуатації.

Загалом, математичний аналіз є фундаментальним етапом в оптимізації роботи СКД. Він дозволяє не лише оцінити точність і надійність існуючих рішень, але й розробити нові методи, які забезпечать вищий рівень безпеки та зручності для користувачів. У наступних підрозділах буде розглянуто практичне застосування математичних моделей для аналізу показників ефективності СКД, моделювання їхньої роботи за різних умов і прогнозування впливу змін на систему [11].

2.3.1. Обчислення показників FAR та FRR

Обчислення показників FAR та FRR є важливим етапом математичного аналізу, що використовується для оцінки ефективності роботи СКД. FAR визначає ймовірність того, що система помилково надасть доступ неавторизованому користувачу. Цей показник критично важливий у системах, де безпека є головним пріоритетом, наприклад у банківській або урядовій сфері. FRR, у свою чергу, характеризує ймовірність відмови у доступі легітимному користувачу, що може

спричиняти операційні проблеми, такі як затримки в роботі або зниження ефективності бізнес-процесів. Розрахунок цих показників дозволяє встановити баланс між безпекою та зручністю використання системи.

Формули для обчислення FAR і FRR базуються на результатах експлуатації або тестування системи. Для FAR застосовується формула 2.1:

$$\mathrm{F}AR = \frac{N_{FA}}{N_T} \tag{2.1}$$

де N_{FA} — кількість помилкових рішень, а N_T— загальна кількість спроб автентифікації. Для FRR формула 2.2 виглядає так:

$$FRR = \frac{N_{FR}}{N_A} \tag{2.2}$$

де N_{FR} — кількість помилкових відмов, а N_A — кількість спроб доступу авторизованими користувачами. Ці формули забезпечують універсальний підхід до оцінки роботи СКД та використовуються як стандарт у галузі кібербезпеки [10].

Показники FAR і FRR взаємозалежні, тому зміна параметрів системи, наприклад порогових значень для ідентифікації користувачів, безпосередньо впливає на ці показники. Наприклад, зменшення порогового значення може знижувати FRR, але водночас підвищувати FAR, і навпаки. Тому для кожної системи контролю доступу важливо знайти оптимальний баланс між цими показниками, залежно від її призначення [11].

Загальну ефективність системи контролю доступу можна оцінити через сумарну ймовірність помилки, яка враховує як FAR, так і FRR. Формула для обчислення загальної ймовірності помилки виглядає наступним чином:

$$P_{error} = P_{(FAR)} + P_{(FRR)}, \tag{2.3}$$

де $P_{(FAR)}$ — ймовірність помилкового прийняття неавторизованого користувача, а $P_{(FRR)}$— ймовірність помилкового відхилення авторизованого користувача.

Ця формула дозволяє оцінити сукупний ризик помилок, який є критичним для систем з високими вимогами до точності, таких як біометричні системи або багатофакторна автентифікація. Зменшення P_{error} можливе за рахунок оптимізації порогового значення системи, що визначає чутливість до прийняття або відхилення

запиту. Графічно цей баланс можна продемонструвати через ROC-криву, де залежність між FAR і FRR дозволяє обрати оптимальний поріг, що мінімізує сумарний ризик помилок. Важливо зазначити, що для критичних систем пріоритет часто віддається мінімізації FAR, навіть якщо це трохи підвищує значення FRR [10][24].

Щоб продемонструвати практичне застосування, розглянемо кейс для корпоративного підприємства з 500 співробітниками, кожен з яких здійснює в середньому 5 спроб автентифікації на день. Це становить загалом 2500 спроб на день і 75000 на місяць. Якщо система реєструє 15 помилкових прийняттів і 60 помилкових відмов на місяць, то FAR обчислюється за формулою 2.1:

$$FAR = \frac{15}{7500} = 0.0002 = 0.02\% \quad (2.4)$$

а FRR обчислюється за формулою 2.2:

$$FRR = \frac{60}{500 \times 30} = \frac{60}{15000} = 0.004 = 0.4\% \quad (2.5)$$

Ці результати показують, що система має низький рівень помилкових прийняттів, що є прийнятним для більшості організацій. Однак значення FRR вказує на можливість певних операційних затримок через відмови авторизованим користувачам, що може вимагати налаштування системи.

Показники FAR і FRR також можна використовувати для моделювання поведінки системи у змінних умовах, таких як збільшення кількості користувачів або підвищення навантаження на систему. Для цього застосовуються статистичні методи, які дозволяють прогнозувати ймовірність помилок залежно від різних факторів, наприклад часу доби, місця доступу або типу пристрою автентифікації. Це дозволяє організаціям адаптувати свої системи до реальних умов експлуатації, зберігаючи високу точність та ефективність.

Обчислення FAR і FRR також має важливе значення при інтеграції різних методів автентифікації, таких як біометричні сканери, PIN-коди або смарт-картки. Кожен метод має свої показники ефективності, які повинні бути враховані при розробці багатофакторних систем контролю доступу. Наприклад, біометричні

системи зазвичай мають нижчий рівень FRR, але підвищений ризик FAR у разі неправильного налаштування або поганої якості обладнання [10].

Таким чином, математичний аналіз FAR і FRR є ключовим інструментом для забезпечення балансу між безпекою та зручністю роботи СКД. Він дозволяє оцінити ефективність системи, знайти її слабкі місця та розробити рекомендації щодо оптимізації налаштувань для досягнення найкращих результатів у конкретних умовах. Цей аналіз також допомагає прогнозувати поведінку системи у різних сценаріях, що робить його незамінним інструментом для організацій, які прагнуть підвищити рівень своєї інформаційної безпеки [11].

2.3.2 Методи зниження FAR/FRR

Зниження показників FAR і FRR є важливим завданням для оптимізації роботи СКД. FAR, що відображає ймовірність помилкового прийняття неавторизованого користувача, і FRR, який характеризує ймовірність відмови легітимному користувачу, є взаємозалежними показниками. Для їх зменшення використовується комплексний підхід, який включає технічні вдосконалення, організаційні заходи та впровадження інновацій [10].

Одним із ключових методів є оптимізація порогових значень, що визначають рівень чутливості системи. Порогові значення впливають на точність автентифікації: надто низький поріг знижує FRR, але збільшує FAR, тоді як високий поріг зменшує FAR, але підвищує FRR. Для пошуку оптимального порогу використовуються математичні моделі, зокрема ROC-криві, які дозволяють візуалізувати співвідношення FAR і FRR та обрати налаштування залежно від потреб системи. Наприклад, у високоризикових середовищах, таких як банки, пріоритетним є мінімізація FAR, навіть якщо це призводить до підвищення FRR, тоді як у корпоративних офісах важливо забезпечити зручність для користувачів і мінімізувати FRR [11].

Іншим ефективним методом є впровадження багатофакторної MFA, яка об’єднує декілька рівнів перевірки, таких як біометричні дані, паролі або смарт-

картки. Наприклад, у разі сумнівів щодо автентичності біометричних даних система може запросити додатковий фактор, наприклад, одноразовий пароль. Такий підхід дозволяє зменшити ризик помилкових прийняттів і підвищує надійність системи. Використання адаптивних алгоритмів автентифікації, що базуються на машинному навчанні, також сприяє зниженню FAR і FRR. Ці алгоритми аналізують контекстні фактори, такі як час, місце доступу чи тип пристрою, і автоматично коригують параметри системи в реальному часі, підвищуючи її точність.

Технічні вдосконалення, такі як використання високоякісних сенсорів, також є критичними. Сучасні сканери відбитків пальців чи камери розпізнавання облич із високою роздільною здатністю забезпечують точніше зчитування даних, що знижує кількість помилок. Додатково, технології «аналізу живого сигналу» дозволяють розрізняти реальні біометричні дані від підроблених. Наприклад, системи можуть аналізувати рухи очей чи реакцію зіниць, що робить неможливим обхід системи за допомогою фотографій або відео [10].

Організаційні заходи також відіграють важливу роль у зниженні показників FAR і FRR. Навчання персоналу правильному використанню СКД допомагає зменшити помилки, пов’язані з людським фактором. Наприклад, співробітники можуть дізнатися, як правильно розташовувати пальці на сканері чи уникати надмірного натискання. Регулярний аудит систем дозволяє виявляти слабкі місця та вчасно коригувати налаштування. Крім того, стандартизовані політики та процедури, що регламентують оновлення програмного забезпечення та моніторинг роботи системи, сприяють її стабільності та ефективності [10][11].

Інноваційні підходи, такі як використання криптографії для захисту біометричних даних і впровадження поведінкових методів автентифікації, також сприяють зниженню FAR і FRR. Наприклад, аналіз шаблонів набору тексту або рухів курсора додає додатковий рівень перевірки, що зменшує залежність від окремих методів автентифікації та підвищує загальну точність системи.

Таким чином, зниження показників FAR і FRR є багатогранним завданням, яке вимагає інтеграції технічних рішень, організаційних заходів і новітніх

технологій. Лише комплексний підхід дозволяє досягти високої ефективності систем контролю доступу, забезпечуючи баланс між безпекою та зручністю для користувачів.

2.3.3 Приклади практичного застосування методів

Практичне застосування методів зниження FAR і FRR демонструє їхню ефективність у реальних умовах експлуатації СКД. Нижче наведено приклади, які ілюструють впровадження технічних, організаційних та інноваційних підходів у різних секторах [10].

1) Корпоративний сектор: великі міжнародні компанії, такі як Google або Microsoft, впроваджують MFA для захисту доступу до корпоративних мереж. У таких системах основний рівень автентифікації, наприклад, біометричні дані співробітників, доповнюється одноразовими паролями або фізичними токенами, такими як YubiKey. Це знижує ризик FAR, адже навіть у разі помилкового прийняття біометричних даних система вимагатиме додаткової перевірки. Так, компанія Microsoft повідомила про зменшення кількості зловмисних спроб доступу до корпоративних облікових записів на 85% після інтеграції MFA.

2) Банківська справа: у банківському секторі критично важливо мінімізувати FAR, оскільки навіть одна помилка може призвести до значних фінансових втрат. Наприклад, банк HSBC використовує технологію розпізнавання голосу для автентифікації клієнтів у кол-центрах. Щоб знизити FAR, система аналізує понад 100 параметрів голосу, включаючи тональність, частоту та паузи, а також використовує «аналіз живого сигналу» для перевірки автентичності голосу. Такий підхід значно зменшує ймовірність обману системи за допомогою записів голосу.

3) Медичні установи: У лікарнях та медичних центрах мінімізація FRR є пріоритетом, адже відмови в доступі можуть призводити до затримок у наданні медичної допомоги. Наприклад, система управління доступом у лікарнях Mayo Clinic використовує біометричні сканери відбитків пальців для швидкого входу

медичного персоналу до баз даних пацієнтів. Щоб уникнути помилкових відмов, система регулярно оновлює свої алгоритми автентифікації та забезпечує навчання персоналу щодо правильного використання обладнання. Це дозволяє підтримувати високий рівень FRR на рівні менш ніж 0.1%, що є критично важливим для роботи в екстрених умовах.

4) Державні установи: в органах державної влади, таких як митниці чи імміграційні служби, впровадження адаптивних алгоритмів автентифікації допомагає знизити обидва показники — FAR і FRR. Наприклад, служба прикордонного контролю в Сінгапурі використовує систему розпізнавання обличчя із вбудованими адаптивними алгоритмами. Система враховує контекстні фактори, такі як якість освітлення та положення обличчя, що дозволяє знизити помилки під час ідентифікації пасажирів. Крім того, використання резервних методів автентифікації, таких як QR-коди або RFID-картки, допомагає уникнути проблем із відмовою у доступі.

5) Промислові об'єкти: на об'єктах критичної інфраструктури, таких як атомні електростанції або нафтопереробні заводи, впроваджуються технології криптографічного захисту біометричних даних. Наприклад, на одній із атомних станцій в Японії використовується система, що комбінує біометричну автентифікацію (сканування райдужної оболонки ока) з шифруванням даних за допомогою AES-256. У разі FAR система блокує доступ до збережених даних і повідомляє адміністратора, що забезпечує додатковий рівень захисту. Такий підхід дозволив знизити FAR до 0.005% і одночасно підтримувати низький рівень FRR.

6) Освітні заклади: в університетах і коледжах інтеграція поведінкових методів автентифікації дозволяє знизити FRR без значного впливу на FAR. Наприклад, система управління доступом у бібліотеках Кембриджського університету аналізує шаблони набору тексту користувачами для ідентифікації. У поєднанні зі стандартною автентифікацією за допомогою пароля це дозволяє уникнути проблем із доступом для студентів під час навчального процесу. Такі інновації забезпечують точність і зручність для користувачів, зменшуючи кількість помилкових відмов.

7) Аеропорти: вони часто стикаються з високим навантаженням на системи контролю доступу. Наприклад, система розпізнавання обличчя у міжнародному аеропорту в Дубаї використовує технологію «аналізу живого сигналу» для верифікації пасажирів. Це знижує ймовірність обходу системи, одночасно забезпечуючи швидке проходження контролю. Додатково, у разі невідповідності біометричних даних, система автоматично переходить до резервного сценарію з використанням електронних паспортів, що мінімізує затримки та забезпечує низький FRR.

Ці приклади ілюструють, як різні організації впроваджують методи зниження FAR і FRR залежно від своїх потреб. Використання багатофакторної автентифікації, адаптивних алгоритмів, поведінкових методів і криптографічного захисту дозволяє досягти високої ефективності та точності в реальних умовах експлуатації. Кожен із наведених прикладів демонструє значення комплексного підходу, який включає як технічні, так і організаційні заходи для підвищення безпеки та зручності використання СКД [10][11].

2.3.4. Ймовірнісні моделі та розподіли даних

Застосування ймовірнісних моделей є важливим інструментом для аналізу точності СКД у реальних умовах експлуатації. Такі моделі дозволяють враховувати неоднорідну структуру персоналу, яка включає різні рівні підготовки, частоту використання системи, а також індивідуальні особливості фізіологічних і поведінкових характеристик користувачів. Вивчення цих факторів забезпечує глибше розуміння роботи СКД та дозволяє створювати більш ефективні та адаптивні системи.

Персонал будь-якої організації складається з груп людей, які мають різний рівень доступу, навичок і досвіду роботи із СКД. Наприклад, у виробничих компаніях частина працівників може рідко користуватися системами автентифікації, тоді як адміністративний персонал робить це регулярно. Така нерівномірність використання впливає на точність системи: працівники, які рідко

користуються СКД, можуть мати вищі показники False Rejection Rate (FRR) через нестачу досвіду або помилки під час взаємодії із системою.

Додатково, фізіологічні особливості користувачів (наприклад, різна якість сканування відбитків пальців через грубу шкіру в працівників фізичної праці) також впливають на показники помилок. У біометричних системах це може спричинити підвищення як FRR, так і FAR, особливо якщо система недостатньо адаптована до таких особливостей.

Для моделювання цих впливів використовуються ймовірнісні моделі, які базуються на розподілах даних. Наприклад, розподіл Гауса (нормальний розподіл) може бути використаний для опису розподілу біометричних параметрів серед працівників, тоді як розподіл Пуассона підходить для моделювання частоти помилкових спроб доступу.

Розглянемо приклад підприємства з 500 працівниками, розподіленими на три основні групи:

- **Адміністративний персонал (200 осіб):** здійснює близько 10 спроб доступу на день.
- **Технічний персонал (250 осіб):** використовує СКД приблизно 5 разів на день.
- **Сезонні працівники (50 осіб):** взаємодіють із системою нечасто, у середньому 2 рази на день.

Якщо враховувати нормальний розподіл точності біометричних систем (наприклад, розпізнавання відбитків пальців), для кожної групи можна оцінити ймовірність помилкових прийняттів і відмов. Використовуючи статистичні дані про FAR і FRR, можна побудувати модель, яка оцінює, як зміни у структурі персоналу впливають на загальну ефективність системи [10][11].

Національний інститут стандартів і технологій (NIST) розробив рекомендації щодо калібрування систем контролю доступу для забезпечення їх точності в умовах неоднорідної структури персоналу. Основними рекомендаціями є:

Регулярне тестування на відповідність системи умовам експлуатації. Це включає перевірку точності роботи системи для різних груп користувачів і сценаріїв доступу [4].

- **Налаштування порогових значень для різних груп користувачів.** Наприклад, для працівників, які часто взаємодіють із системою, можна встановити більш суворі порогові значення, тоді як для сезонних працівників — знижені, але з додатковим фактором автентифікації.
- **Використання адаптивних алгоритмів.** Це дозволяє системі змінювати параметри залежно від історичних даних про користувачів, таких як частота доступу або попередні показники помилок.
- **Аналіз статистичних даних.** NIST рекомендує використовувати великий обсяг зібраних даних для побудови ймовірнісних моделей і прогнозування можливих помилок у роботі СКД [4].

Одним із практичних прикладів реалізації таких рекомендацій є використання модульних систем контролю доступу в міжнародних корпораціях. Наприклад, компанії, що працюють у сфері енергетики, інтегрують адаптивні алгоритми, які базуються на ймовірнісному аналізі. Ці алгоритми використовують інформацію про графік роботи, роль користувача та частоту доступу для налаштування параметрів автентифікації. Додатково, системи автоматично адаптуються до нових умов, наприклад, під час зміни складу персоналу або впровадження нових технологій.

2.4. Прогноз ефективності та перспективи розвитку

СКД є невід’ємною складовою забезпечення інформаційної безпеки в умовах цифрової трансформації. Вони перебувають у постійному розвитку, адаптуючись до нових викликів, таких як зростання обсягів даних, збільшення кількості користувачів і появи нових загроз. Оцінка ефективності СКД та аналіз перспектив їх розвитку є критично важливими для визначення вектору впровадження інновацій, які зможуть відповідати сучасним і майбутнім вимогам.

Ефективність сучасних СКД залежить від балансу між безпекою, зручністю користування і вартістю впровадження та підтримки. Прогноз ефективності ґрунтується на аналізі поточних показників системи, таких як FAR, FRR та середній час обробки запитів. Наприклад, у сучасних багатофакторних СКД використання біометричних даних і адаптивних алгоритмів значно підвищує точність і надійність систем, але водночас збільшує їхню вартість і потребує високої кваліфікації персоналу.

Однак ключовим фактором у прогнозі ефективності є впровадження новітніх технологій. Використання ШІ для аналізу поведінкових патернів користувачів дозволяє створювати адаптивні системи, що автоматично коригують свої параметри залежно від контексту. Наприклад, розпізнавання аномальної поведінки користувача у реальному часі може забезпечити додатковий рівень захисту без зниження зручності для авторизованих користувачів. Подібні підходи мають перспективу не лише в корпоративному секторі, але й у державних установах, системах критичної інфраструктури та IoT [28].

Перспективи розвитку СКД також пов’язані із впровадженням нових стандартів безпеки та технологій. Наприклад, технології блокчейн можуть забезпечити незмінність і захист журналів доступу, що особливо актуально для об’єктів критичної інфраструктури. Крім того, інтеграція з IoT відкриває нові можливості для управління доступом до пристроїв, однак водночас створює нові виклики, такі як захист розподілених систем і безпека в умовах масштабування.

Особливо важливим є питання впровадження технологій захисту персональних даних у системах, що використовують біометричні дані. Зростаючий обсяг регуляторних вимог, таких як GDPR, вимагає не лише високого рівня шифрування, але й прозорості у використанні даних. У майбутньому можна очікувати появу більш досконалих стандартів, таких як оновлення ISO/IEC 27001, які охоплюватимуть новітні методи захисту ідентифікаційних даних [4][9].

У подальших підрозділах буде детально розглянуто, як саме технологічні вдосконалення, такі як штучний інтелект, блокчейн і поведінковий аналіз, впливатимуть на ефективність СКД. Також буде проведено порівняння

традиційних та сучасних систем, що дозволить оцінити переваги нових підходів з урахуванням організаційних і технологічних аспектів. Особлива увага буде приділена IoT-рішенням і їхній інтеграції у фізичні системи контролю доступу, а також прогнозу їхнього впливу на безпеку й управління у майбутньому.

2.4.1. Вплив інновацій ШІ, блокчейн, поведінковий аналіз.

Інноваційні технології, такі як ШІ, блокчейн і поведінковий аналіз, стають рушійною силою розвитку СКД. Їх впровадження дозволяє підвищити точність, зменшити вразливості та забезпечити відповідність сучасним вимогам безпеки. Застосування цих технологій дає змогу організаціям не лише реагувати на загрози, але й проактивно запобігати їм. Прогноз розвитку базується на аналітичних даних провідних дослідницьких агентств, таких як Gartner та Forrester.

Штучний інтелект є основою багатьох сучасних рішень у сфері СКД. Його використання дозволяє створювати адаптивні системи, які автоматично коригують налаштування залежно від контексту. Наприклад, ШІ аналізує великі обсяги даних, включаючи історію входів, поведінкові шаблони користувачів, а також зовнішні фактори, такі як час доби чи геолокація. Завдяки цьому система може знизити FAR і FRR, забезпечуючи при цьому зручність для легітимних користувачів.

Прогноз Gartner на 2025 рік передбачає, що понад 70% компаній будуть використовувати ШІ у своїх СКД, що дозволить підвищити точність і зменшити час обробки запитів на доступ на 40%. Такі результати досягаються завдяки впровадженню алгоритмів розпізнавання аномалій та поведінкової аналітики, які автоматично блокують підозрілі дії або запити.

Блокчейн стає ключовою технологією для захисту даних у розподілених системах контролю доступу. Його основна перевага полягає у забезпеченні незмінності даних і прозорості процесів автентифікації. Використання блокчейну дозволяє зберігати журнали доступу у децентралізованій мережі, що унеможливлює їх підробку.

Наприклад, у системах IoT, які часто є частиною СКД, блокчейн забезпечує захист даних, що передаються між пристроями, і гарантує цілісність інформації. За прогнозами Forrester, до 2026 року понад 30% рішень у сфері СКД будуть інтегровані з блокчейном, що дозволить знизити ризики несанкціонованого доступу до розподілених мереж на 25% [3][5].

Поведінковий аналіз стає невід'ємною частиною СКД, забезпечуючи додатковий рівень безпеки. Система використовує дані про звички користувачів, такі як шаблони набору тексту, рухи курсора або частота взаємодії з певними ресурсами. Це дозволяє не лише підтвердити особу користувача, але й визначити аномалії, які можуть свідчити про спробу компрометації облікового запису.

Сучасні рішення інтегрують поведінкову аналітику з адаптивними алгоритмами ШІ, що забезпечує проактивне виявлення загроз. Наприклад, якщо користувач починає виконувати незвичні для нього дії (наприклад, намагається отримати доступ до закритих ресурсів), система автоматично підвищує рівень автентифікації або блокує доступ. Gartner прогнозує, що до 2027 року поведінковий аналіз буде використовуватися у 85% систем корпоративного рівня, що зменшить кількість внутрішніх загроз на 30%.

Інтеграція ШІ, блокчейну та поведінкового аналізу створює можливості для підвищення точності систем контролю доступу на 50–70% залежно від сценаріїв використання. Завдяки автоматизації процесів автентифікації та моніторингу системи стають більш стійкими до зовнішніх і внутрішніх загроз. Крім того, впровадження інновацій дозволяє знизити операційні витрати на управління системами безпеки завдяки їхній здатності самостійно адаптуватися до нових умов. За даними Forrester, організації, які впровадили системи на основі ШІ, заощаджують до 30% бюджету на інформаційну безпеку через зниження кількості інцидентів і прискорення процесів обробки запитів. Водночас використання блокчейну забезпечує додатковий рівень прозорості та надійності, що важливо для регульованих галузей, таких як фінанси або медицина.

Інновації, такі як штучний інтелект, блокчейн і поведінковий аналіз, мають значний вплив на розвиток систем контролю доступу. Вони забезпечують нові

можливості для підвищення точності, зниження вразливостей і забезпечення відповідності сучасним вимогам безпеки. Прогнозоване поширення цих технологій у найближчі роки свідчить про їхній критично важливий внесок у розвиток інформаційної безпеки в цифрову епоху. У подальших підрозділах буде розглянуто детальні приклади впровадження цих інновацій у різних галузях.

2.4.2. Порівняння традиційних і сучасних СКД

СКД пройшли довгий шлях від традиційних рішень, заснованих на простих фізичних та цифрових методах, до сучасних високотехнологічних систем, що використовують штучний інтелект, багатофакторну автентифікацію, блокчейн і біометричні технології. Порівняння цих двох типів систем дозволяє зрозуміти, як еволюція технологій змінила підходи до забезпечення безпеки, підвищила точність роботи СКД та вплинула на організаційні фактори, такі як навчання персоналу й інвестиції в інфраструктуру.

Традиційні СКД базуються на використанні фізичних ключів, магнітних карток, PIN-кодів або інших статичних методів автентифікації. Їхня головна перевага полягає у простоті експлуатації та низькій вартості впровадження. Для більшості користувачів такі системи не вимагають складних знань чи спеціальної підготовки. Однак ці переваги мають зворотний бік: низький рівень захисту, висока ймовірність компрометації ключів або паролів і відсутність гнучкості в адаптації до нових викликів. Наприклад, втрачений фізичний ключ або скомпрометований пароль може забезпечити несанкціонований доступ до об’єктів або ресурсів, що робить такі системи неприйнятними для об’єктів із високими вимогами до безпеки.

Сучасні СКД пропонують значно вищий рівень безпеки завдяки впровадженню інноваційних технологій. Використання біометрії, як-от розпізнавання обличчя, відбитків пальців чи райдужної оболонки ока, забезпечує точну ідентифікацію користувачів, яка практично не піддається компрометації. Наприклад, у міжнародному аеропорту Дубая реалізовано систему контролю доступу на основі розпізнавання облич із використанням штучного інтелекту. Ця

система дозволяє миттєво перевіряти ідентичність пасажирів, знижуючи ризик несанкціонованого доступу до критичних зон. Крім того, сучасні системи інтегрують MFA, що комбінує біометричні дані, паролі та фізичні токени. Це забезпечує додатковий рівень захисту навіть у разі компрометації одного з факторів [14].

Важливим аспектом порівняння є організаційні фактори. Для традиційних СКД навчання персоналу є мінімальним, оскільки користувачам достатньо знати, як користуватися ключами чи вводити PIN-коди. У сучасних системах потреба в навчанні значно вища. Наприклад, при впровадженні біометричних систем працівники повинні розуміти, як правильно використовувати обладнання, наприклад, сканери відбитків пальців чи пристрої розпізнавання облич. Недостатня підготовка може призводити до підвищення FRR, що викликає затримки у роботі та знижує продуктивність. Для технічного персоналу навчання включає розуміння роботи адаптивних алгоритмів, моніторинг підозрілої активності та управління інцидентами [13].

Ще одним важливим організаційним фактором є інвестиції в інфраструктуру. Традиційні системи потребують мінімальних вкладень, оскільки їхнє впровадження обмежується встановленням карткових рідерів, замків чи інших базових пристроїв. Натомість сучасні СКД вимагають серйозних інвестицій у спеціалізоване обладнання, як-от біометричні сенсори, сервери для обробки даних, а також у розробку або впровадження програмного забезпечення на основі штучного інтелекту. Наприклад, інтеграція блокчейну для зберігання даних про доступ вимагає високопродуктивної мережевої інфраструктури, яка забезпечує надійний обмін даними між вузлами.

Реальні приклади демонструють значення цих інвестицій. У компанії Siemens, наприклад, впровадження адаптивної системи контролю доступу на основі ШІ дозволило знизити витрати на управління безпекою на 25% завдяки автоматизації моніторингу та зменшенню кількості інцидентів. У медичному центрі Mayo Clinic навчання персоналу правильному використанню біометричних

систем допомогло зменшити FRR на 15%, що позитивно вплинуло на оперативність роботи медичного персоналу.

Таким чином, традиційні та сучасні СКД значно відрізняються за рівнем безпеки, функціональними можливостями та організаційними вимогами. Хоча традиційні системи залишаються актуальними для середовищ із низькими вимогами до захисту через їхню простоту та низьку вартість, сучасні СКД є більш ефективними для забезпечення безпеки в умовах високих ризиків. Врахування організаційних факторів, таких як навчання персоналу та інвестиції в інфраструктуру, є вирішальним для успішного переходу на нові системи, які забезпечують високу точність, надійність і адаптивність до сучасних загроз.

2.4.3. IoT-рішення у фізичних СКД

IoT суттєво змінює підхід до фізичних СКД, інтегруючи інтелектуальні пристрої, сенсори та хмарні платформи. Завдяки цим технологіям СКД стають більш гнучкими, адаптивними та інтерактивними, що відкриває нові можливості їх використання в різних галузях: від побутових потреб до управління складними інфраструктурними об’єктами. Інноваційні IoT-рішення, як-от смарт-замки та інтегровані датчики, не лише підвищують ефективність контролю доступу, але й змінюють спосіб взаємодії користувачів із цими системами. Водночас зростання кількості IoT-пристроїв створює нові ризики, що вимагає впровадження комплексних організаційних заходів для їх мінімізації [17][28].

Одним із найпоширеніших IoT-рішень у фізичних СКД є смарт-замки. Вони дозволяють управляти доступом через мобільні додатки, біометричні дані, RFID-картки чи одноразові паролі, що значно підвищує зручність для користувачів. Смарт-замки забезпечують можливість динамічного управління: доступ можна надавати чи скасовувати в реальному часі з будь-якого місця, що особливо важливо для готелів, орендованого житла (наприклад, Airbnb) та корпоративних офісів із високою ротацією персоналу. Наприклад, в офісах сучасних компаній користувачі можуть отримувати доступ до приміщень після верифікації за допомогою

мобільного пристрою чи біометричних даних, що виключає потребу у фізичних ключах і знижує ризик їхньої втрати.

Інша важлива технологія — IoT-датчики, які забезпечують додатковий рівень контролю в СКД. Вони здатні моніторити широкий спектр параметрів, таких як рух, температура, вологість або відкриття дверей. Інтеграція таких датчиків із центральними системами управління дозволяє автоматично реагувати на аномалії чи незвичну активність. Наприклад, якщо датчик виявляє рух у забороненій зоні під час неробочого часу, система автоматично блокує доступ, вмикає сигналізацію або надсилає сповіщення адміністратору. У промислових умовах IoT-датчики активно використовуються для моніторингу доступу до зон завантаження в логістичних центрах або для контролю доступу до критичних зон у виробництві [3][28].

Основними перевагами IoT-рішень є їхня гнучкість, адаптивність і можливість збору й аналізу великих обсягів даних. Завдяки хмарним платформам доступ можна віддалено регулювати, а інтеграція з іншими системами, такими як відеоспостереження чи автоматизовані бар’єри, забезпечує всебічний контроль. Крім того, IoT-пристрої генерують значний обсяг даних, які можна аналізувати для оптимізації роботи систем і прогнозування потенційних загроз. Наприклад, у логістичних компаніях дані про частоту використання зон доступу допомагають покращити розподіл ресурсів і уникнути перевантажень.

Попри значні переваги IoT-рішень, вони також відкривають нові вразливості. Підключення великої кількості пристроїв до мережі збільшує ризик кібератак, компрометації даних та збоїв у роботі систем. Для мінімізації цих ризиків організації мають впроваджувати комплексний підхід, який включає захист даних і комунікацій, регулярне оновлення прошивки, сегментацію мережі, моніторинг і навчання персоналу. Наприклад, шифрування даних за допомогою протоколів TLS/SSL забезпечує захист комунікацій між пристроями, знижуючи ризик їхнього перехоплення. Сегментація мережі, яка розділяє IoT-пристрої на окремий сегмент, запобігає розповсюдженню загроз на критичні системи. Оновлення програмного

забезпечення IoT-пристроїв допомагає уникнути експлуатації відомих вразливостей.

Крім того, важливо навчати персонал базовим принципам безпеки IoT-пристроїв, зокрема правильному використанню мобільних додатків для управління доступом. Наприклад, співробітники повинні знати, як налаштовувати унікальні паролі для своїх облікових записів або реагувати на підозрілі повідомлення від системи.

IoT-рішення у фізичних СКД мають величезний потенціал для підвищення ефективності, зручності та безпеки. Смарт-замки, інтегровані датчики та інші IoT-пристрої дозволяють автоматизувати багато процесів і знижують потребу у втручанні людини. Однак їхнє впровадження потребує ретельного планування, дотримання заходів безпеки та постійного моніторингу. Завдяки поєднанню технологічних і організаційних рішень організації можуть повною мірою використовувати переваги IoT, зберігаючи високий рівень захисту в умовах сучасних кіберзагроз.

2.5 Висновок до другого розділу

У ході аналізу сучасних СКД, представленого в цьому розділі, було продемонстровано широкий спектр підходів та технологій, покликаних підвищити рівень безпеки на об’єктах інформаційної діяльності. Проведений огляд підтвердив, що ефективні СКД не обмежуються використанням лише статичних методів (наприклад, паролів чи фізичних ключів), а дедалі частіше впроваджують багатофакторну автентифікацію, біометричні системи, засоби ШІ, блокчейну, а також інтегруються з хмарними сервісами та IoT-рішеннями.

Одним із ключових висновків стало розуміння, що сучасні СКД – це складні багатокомпонентні системи, які повинні забезпечувати не тільки надійну ідентифікацію користувачів, але й динамічне управління доступом на підставі контексту (місцезнаходження, тип пристрою, роль користувача, оцінка ризику запиту). Огляд популярних платформ, таких як Cisco ISE, Fortinet Access

Management та Microsoft Azure AD Conditional Access, засвідчив здатність цих рішень ефективно контролювати доступ до критичних ресурсів, забезпечуючи високий рівень захисту інформації.

Не менш важливою складовою виявилися організаційні чинники: навчання персоналу, розробка внутрішніх регламентів, регулярний аудит, оптимізація інфраструктурних процесів та чітке управління оновленнями. Розглянуті проблеми, пов’язані з імовірнісними помилками, уразливостями біометричних технологій та інфраструктурними недоліками, підкреслюють необхідність комплексного підходу до впровадження СКД: не лише технологічного, але й організаційного та методологічного.

Математичний аналіз показав, що точність СКД можна покращувати за допомогою адаптивних алгоритмів, поведінкового аналізу та оптимізації порогових значень. Впровадження інноваційних технологій, зокрема ШІ, блокчейну та інтеграція з IoT, має перспективу суттєво підвищити точність, стійкість і гнучкість систем, а також сприятиме ефективному масштабуванню рішень у мінливих умовах.

Таким чином, результати розділу свідчать, що сучасні СКД є не просто технічним інструментом, а стратегічним елементом кібербезпеки. Вони здатні динамічно адаптуватися до нових загроз, інтегруватися з іншим програмно-апаратним забезпеченням і відповідати міжнародним стандартам, водночас забезпечуючи високий рівень захисту інформаційних ресурсів.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗА ДОПОМОГОЮ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

3.1 Аналіз і оптимізація системи контролю доступу для захисту інформації

Сучасний стан інформаційної безпеки вимагає впровадження комплексних рішень для захисту даних на об’єктах інформаційної діяльності. У зв’язку зі швидким розвитком технологій, збільшенням обсягу оброблюваної інформації та зростанням кількості кіберзагроз, особливого значення набувають СКД, що є ключовим інструментом у забезпеченні конфіденційності, цілісності та доступності інформації.

У цьому розділі розглянуто практичну реалізацію сучасної системи контролю доступу для підвищення рівня захищеності інформації на конкретному об’єкті інформаційної діяльності. Основний акцент зроблено на аналізі інфраструктури об’єкта, виявленні його слабких місць, а також обґрунтуванні вибору сучасної системи контролю доступу, що відповідає міжнародним стандартам безпеки.

Особливу увагу буде приділено математичному аналізу ризиків, пов’язаних із помилками системи контролю доступу, а саме FAR та FRR. Визначення та розрахунок цих показників дозволить оцінити ефективність обраної системи у реальних умовах і запропонувати рекомендації щодо мінімізації помилок.

Кінцевою метою цього розділу є розробка технічних та організаційних рекомендацій для оптимізації роботи системи контролю доступу, що забезпечить максимальну точність автентифікації, мінімізацію помилок FAR та FRR і, як наслідок, підвищення загального рівня захищеності об’єкта.

Враховуючи важливість об’єкта для інформаційної діяльності, практичне впровадження таких рішень дозволить не лише посилити контроль за доступом, а й створити надійну та гнучку систему захисту, здатну адаптуватися до сучасних загроз і викликів.

3.2 Загальна характеристика об'єкта

Диспетчерська служба екстреної медичної допомоги 103 є центральною ланкою системи реагування на медичні виклики. Основна функція установи полягає у прийомі та оперативній обробці запитів громадян на надання невідкладної медичної допомоги, що потребує не лише бездоганного виконання функціональних завдань, але й забезпечення надійного захисту конфіденційних даних. До таких даних належать персональна інформація пацієнтів, маршрути руху медичних бригад, а також координаційна інформація, необхідна для ефективного управління ресурсами служби.

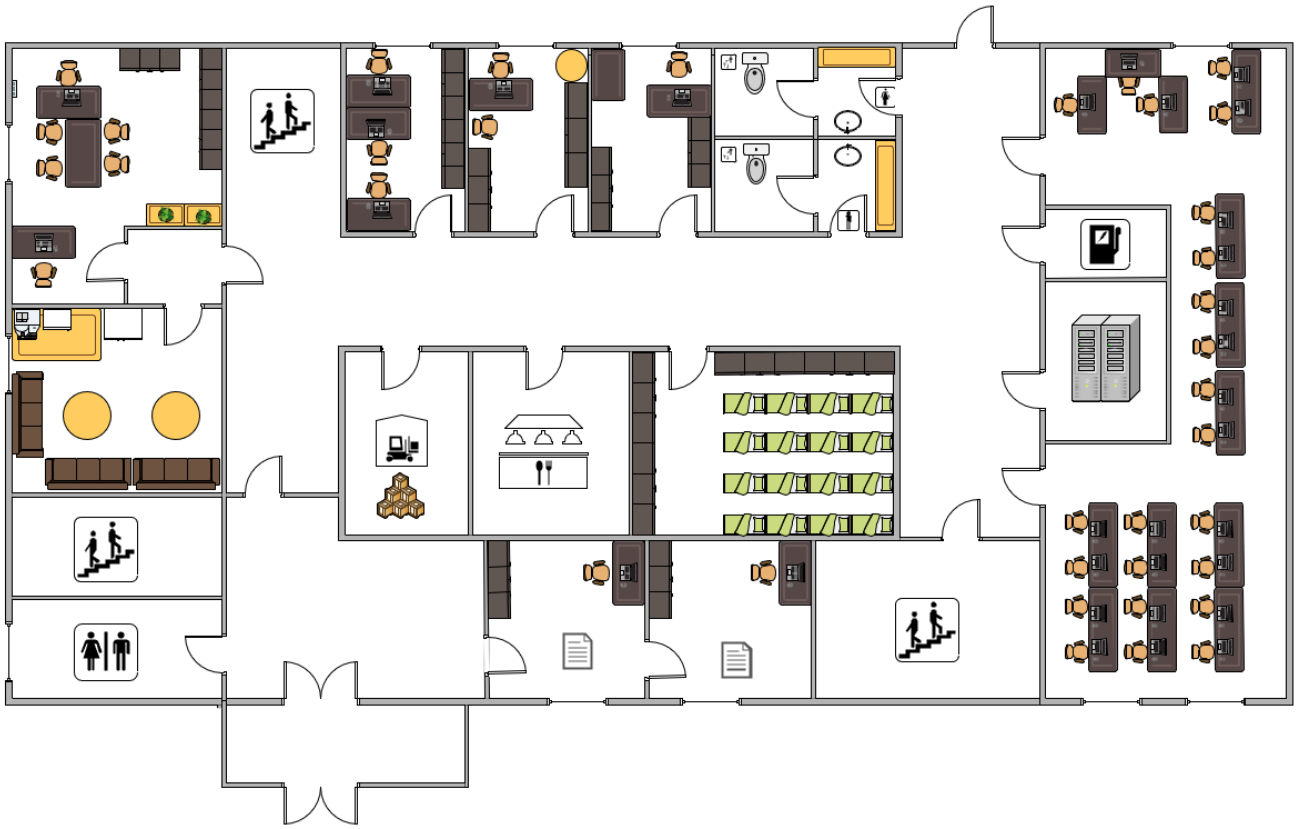


Рис 3.4 — Схема планування диспетчерської служби викликів 103.

Будівля диспетчерської служби спроєктована з урахуванням оптимізації робочих процесів та забезпечення контролю доступу до критично важливих зон. Просторове планування передбачає наявність кількох функціональних зон, кожна з яких виконує свою специфічну роль. При вході до будівлі розташована зона прийому та очікування, що є першим рубежем контакту для відвідувачів та

обслуговуючого персоналу. Основний робочий простір організовано у вигляді диспетчерської зали, де знаходяться робочі місця операторів, які цілодобово здійснюють прийом та обробку викликів. Кількість робочих місць відповідає масштабу роботи служби, забезпечуючи ефективну координацію викликів у режимі реального часу.

Особливе значення для установи мають технічні та архівні приміщення. Технічна зона, що включає серверну кімнату, є критичною частиною будівлі, де зберігаються та обробляються важливі дані. Це приміщення вимагає особливих умов захисту як від несанкціонованого доступу, так і від фізичного пошкодження обладнання. Архівна зона, своєю чергою, призначена для зберігання документації, що містить історію викликів, звіти та інші важливі дані, які потребують належного контролю доступу.

Окрім робочих приміщень, у будівлі передбачені адміністративні та допоміжні зони, до яких відносяться кабінети керівництва, кімнати відпочинку для персоналу, санітарні вузли та технічні приміщення. Чітке зонування простору дозволяє організувати логічне розмежування функціональних завдань та забезпечити зручність роботи для персоналу.

З огляду на характер оброблюваної інформації, питання контролю доступу до різних зон будівлі є особливо актуальним. Приміщення, такі як серверна кімната та диспетчерська зала, повинні мати обмежений доступ і потребують впровадження сучасних систем контролю доступу з використанням багатофакторної автентифікації. Це дозволить мінімізувати ризик проникнення сторонніх осіб та забезпечити належний рівень конфіденційності даних.

Таким чином, будівля диспетчерської служби викликів 103 має добре продуману архітектуру, що відповідає функціональним вимогам організації. Завдяки раціональному плануванню, зонуванню приміщень та застосуванню заходів контролю доступу, забезпечується як ефективність робочих процесів, так і надійний захист критичної інформації. Подальший аналіз буде спрямований на оцінку існуючих ризиків і розробку рекомендацій щодо вдосконалення систем контролю доступу.

3.1.1. Оцінка існуючої системи контролю доступу

Існуюча система контролю доступу в диспетчерській службі екстреної медичної допомоги 103 по Київській області поєднує як фізичні, так і логічні засоби захисту, забезпечуючи базовий рівень безпеки для об’єкта.

Фізичний захист на об'єкті реалізовано через традиційні механічні замки, які встановлені на всіх дверях приміщень, включаючи серверну кімнату, диспетчерську залу, архівні приміщення та кабінети адміністрації. Крім того, для підвищення рівня безпеки доступ до диспетчерської зони контролюється за допомогою системи RFID-карток, що дозволяє регулювати потік співробітників. Проте система має недолік — можливість копіювання RFID-карток, оскільки мітки доступні кожному працівнику. Для зовнішнього контролю об'єкта впроваджено систему відеоспостереження, однак її функціонал обмежується лише зовнішнім периметром, що створює прогалини у внутрішньому моніторингу. Турнікети або інші механізми обмеження входу не використовуються.

Логічні засоби захисту організовані на більш високому рівні. Кожен співробітник працює з унікальним обліковим записом, захищеним надійним паролем. Програма, що використовується для обробки даних, підтримує шифрування під час передачі інформації, що забезпечує захист від несанкціонованого доступу під час обміну даними. Додатковим елементом захисту є ведення журналів доступу та журналів безпеки, які дозволяють відстежувати активність користувачів та виявляти потенційні загрози.

Незважаючи на надійність існуючих заходів та регулярний контроль їх працездатності, система має кілька недоліків. Одним із ключових є відсутність MFA, що підвищує ризик несанкціонованого доступу у разі компрометації облікових даних.

Позитивним є те, що доступ до серверної кімнати та архіву строго контролюється, оскільки ключі від цих приміщень є лише у системного адміністратора або технічного персоналу. Для нових співробітників оперативно створюються нові облікові записи, а для звільнених працівників їхні профілі

архівуються та переводяться до неактивного режиму, що мінімізує ризики внутрішніх загроз.

Таким чином, наявна система контролю доступу забезпечує певний рівень безпеки завдяки поєднанню механічних та цифрових засобів захисту, однак її ефективність обмежується відсутністю сучасних технологій автентифікації та внутрішнього моніторингу. Подальший аналіз буде спрямовано на визначення конкретних загроз та розробку рекомендацій щодо вдосконалення системи з метою підвищення рівня захисту об'єкта.

3.1.2. Аналіз рівня захищеності інформації

На основі наявної системи контролю доступу та характеру оброблюваної інформації в диспетчерській службі викликів 103, можна виділити кілька ключових загроз, які впливають на рівень захищеності даних. Аналіз цих загроз проводився з урахуванням поточного стану фізичних та логічних засобів безпеки, а також вразливостей, що були виявлені у попередньому розділі. Для оцінки рівня ризику застосовувалась стандартна методологія, за якою ризик визначається як добуток ймовірності настання загрози на величину її впливу, що оцінюється за шкалою від 1 до 5.

Джерелами числових оцінок слугують наявні недоліки інфраструктури, практичні випадки з досвіду роботи аналогічних установ та загальні рекомендації у сфері інформаційної безпеки.

Таблиця 3.1 містить результати розрахунків для основних загроз, характерних для диспетчерської служби, та дозволяє оцінити їх значущість.

Таблиця 3.1

Розрахунок ризиків для основних загроз

Загроза	Ймовірність (P)	Вплив (I)	Ризик (R = P × I)	Коментар
Фізичне проникнення	0.6	4	2.4	Механічні замки та RFID легко обійти.
Кібератаки (взлом акаунтів)	0.5	5	2.5	Відсутність MFA підвищує ймовірність атак.

Продовження таблиці 3.1

Компрометація RFID-карток	0.7	3	2.1	Можливість копіювання карток є реальною.
Внутрішні загрози	0.4	4	1.6	Недостатній внутрішній моніторинг.

Фізичне проникнення до приміщення, що можливе через уразливість механічних замків та RFID-карток, є однією з найбільш імовірних загроз. Її ймовірність оцінено у 0.6, а потенційний вплив на роботу об'єкта становить **4** через ризик витоку або пошкодження критично важливих даних. Загальний рівень ризику для цієї загрози складає 2.4.

Кібератаки, спрямовані на компрометацію облікових записів через відсутність багатофакторної автентифікації, мають значний потенційний вплив — 5, оскільки успішна атака може призвести до повного витоку конфіденційних даних. Ймовірність реалізації такої загрози оцінено у 0.5, що зумовлює ризик на рівні 2.5 — найвищий показник серед проаналізованих загроз.

Компрометація RFID-карток, викликана можливістю їх копіювання, є більш імовірною загрозою з ймовірністю 0.7. Однак вплив обмежується локальними наслідками для певних зон, що дозволяє оцінити його у 3. Таким чином, рівень ризику становить 2.1.

Внутрішні загрози, які можуть бути спричинені як ненавмисними діями співробітників, так і умисними спробами компрометації даних, мають ймовірність 0.4 та потенційний вплив 4 через можливість витоку або зміни критичної інформації. Загальний рівень ризику оцінено у 1.6.

Значення ризику, наведені у таблиці 3.1, дозволяють класифікувати загрози за рівнем пріоритетності:

- 2.5 (кібератаки) вказує на критичний рівень ризику, що потребує термінових заходів через високу ймовірність та максимальні наслідки для даних.
- 2.4 (фізичне проникнення) також належить до високих ризиків і потребує модернізації фізичних засобів контролю доступу.

- 2.1 (компрометація RFID-карток) є значущим ризиком через простоту реалізації загрози, але обмежений вплив локалізує його наслідки.
- 1.6 (внутрішні загрози) вказує на середній рівень ризику, який може бути зменшено шляхом впровадження додаткових механізмів моніторингу.

3.2. Обґрунтування вибору сучасної системи контролю доступу

На основі проведеного аналізу існуючої системи контролю доступу та оцінки основних загроз, виявлено низку критичних недоліків, які потребують модернізації. Найбільші загрози, такі як компрометація облікових записів**,** вразливість RFID-карток та фізичне проникнення, вказують на необхідність впровадження більш надійної та функціональної системи контролю доступу (СКД). Це дозволить підвищити рівень безпеки об’єкта, забезпечити захист конфіденційних даних та ефективний контроль доступу до критичних зон.

Вибір сучасної СКД обумовлений наступними факторами:

- Забезпечення багаторівневого контролю доступу: Сучасні системи повинні інтегрувати як фізичні, так і логічні методи захисту, включаючи багатофакторну автентифікацію (MFA) та захищені технології для карток доступу.
- Захист від несанкціонованого доступу: Системи мають забезпечувати високий рівень захисту від компрометації карток і облікових записів, а також можливість виявлення несанкціонованих спроб доступу.
- Інтеграція з іншими системами безпеки: Сучасні СКД дозволяють легко інтегруватися з системами відеоспостереження, моніторингу активності користувачів і сигналізацією для забезпечення комплексної безпеки.
- Відповідність міжнародним стандартам: Обрана система повинна відповідати вимогам ISO/IEC 27001 та іншим стандартам у сфері інформаційної безпеки, що забезпечує високий рівень захисту даних.

Цей підрозділ детально розгляне вибір конкретної сучасної системи контролю доступу, її відповідність міжнародним стандартам та можливості інтеграції у наявну інфраструктуру об’єкта. Результатом стане обґрунтований

вибір рішення, що дозволить усунути наявні вразливості та значно підвищити рівень безпеки диспетчерської служби викликів 103.

3.2.1. Вибір конкретної системи

З огляду на виявлені вразливості в існуючій системі контролю доступу, для диспетчерської служби викликів 103 по Київській області було проведено аналіз трьох сучасних рішень: Cisco ISE**,** Fortinet та Microsoft Azure AD Conditional Access. Основна увага приділялася можливостям цих систем щодо підтримки MFA, інтеграції з хмарними платформами, використання біометричних методів та загальної гнучкості їх налаштування для потреб організації.

Таблиця 3.2

Порівняльний аналіз сучасних систем контролю доступу

Критерій	Cisco ISE	Fortinet	Microsoft Azure AD Conditional Access
Багатофакторна автентифікація (MFA)	Підтримка MFA на основі токенів, SMS	Підтримка MFA із широкими методами	Повна підтримка MFA з інтеграцією з Azure
Інтеграція з хмарними платформами	Обмежена інтеграція	Інтеграція з AWS, Google Cloud	Глибока інтеграція з Microsoft Azure
Використання біометрії	Опціональна, інтегрується через сторонні рішення	Підтримка біометрії через FortiAuth	Підтримка біометрії у складі Azure AD
Гнучкість налаштувань	Високий рівень гнучкості для локальних мереж	Оптимальна для мережевої безпеки	Висока гнучкість для хмарних середовищ
Моніторинг активності	Розширені функції з аналітикою	Моніторинг доступу на основі політик	Автоматизований моніторинг з аналітикою
Відповідність стандартам	ISO/IEC 27001, NIST	ISO/IEC 27001, GDPR	ISO/IEC 27001, GDPR, NIST
Вартість впровадження	Висока	Середня	Відносно низька

На основі результатів порівняння найбільш оптимальною системою для диспетчерської служби викликів 103 є Microsoft Azure AD Conditional Access. Вибір обумовлено кількома ключовими факторами: система забезпечує повну підтримку

MFA, що є критично важливим для захисту облікових записів співробітників від несанкціонованого доступу. Крім того, глибока інтеграція з хмарною платформою Microsoft Azure дозволяє централізовано управляти доступом та забезпечувати гнучку масштабованість у межах організації. Серед переваг також варто відзначити вбудовану підтримку біометричної автентифікації, що дозволяє усунути ризик компрометації RFID-карток, та автоматизований моніторинг активності користувачів, який допомагає виявляти потенційні загрози у режимі реального часу.

Для ефективного функціонування Microsoft Azure AD Conditional Access пропонується встановити її елементи відповідно до особливостей об’єкта. Впровадження MFA повинно бути реалізоване на всіх робочих місцях операторів у диспетчерській залі, забезпечуючи додатковий рівень захисту під час входу до програмного середовища. У критичних зонах, таких як серверна кімната та архіви, доцільно впровадити біометричні сканери для ідентифікації осіб з правом доступу. Біометрія може застосовуватися у поєднанні з оновленими RFID-картками, що мають захист від копіювання.

Моніторинг активності користувачів та аналітика буде реалізована на всіх робочих станціях з автоматичним збором даних про спроби входу та зміни у політиках доступу. Аналіз отриманих даних відбуватиметься у хмарному середовищі Microsoft Azure, що забезпечить оперативне виявлення аномальної поведінки та спроб несанкціонованого доступу.

Таким чином, вибір системи Microsoft Azure AD Conditional Access дозволяє вирішити ключові вразливості поточної системи контролю доступу. Її впровадження не лише мінімізує ризики компрометації облікових записів та фізичного доступу, але й забезпечує комплексний захист інформації завдяки інтеграції сучасних методів автентифікації та автоматизованого моніторингу.

3.2.2. Оцінка відповідності обраної системи міжнародним стандартам

Вибір Microsoft Azure AD Conditional Access як сучасної системи контролю доступу для диспетчерської служби викликів 103 обґрунтовано її відповідністю основним міжнародним стандартам інформаційної безпеки, що є ключовою вимогою для захисту конфіденційних даних і мінімізації вразливостей системи.

Одним із найважливіших стандартів у сфері безпеки є ISO/IEC 27001, який регламентує вимоги до побудови системи управління інформаційною безпекою. Відповідність цьому стандарту забезпечується завдяки використанню багатофакторної автентифікації, централізованого управління політиками доступу та шифруванню даних як у процесі передачі, так і під час зберігання. Ці функціональні можливості дозволяють створити контрольований та захищений доступ до критичної інформації, знижуючи ймовірність несанкціонованого проникнення у систему.

Окрім цього, обрана система відповідає вимогам GDPR, що є особливо актуальним для диспетчерської служби, де обробляється значний обсяг персональних даних пацієнтів. Підтримка політик мінімізації прав доступу забезпечує відповідність принципу «мінімально необхідних привілеїв», а функція моніторингу активності користувачів дозволяє відстежувати дії з даними та виявляти потенційні загрози. Це дає змогу гарантувати дотримання вимог конфіденційності та забезпечити контроль за обробкою персональних даних відповідно до регламенту GDPR.

Додатково система відповідає вимогам NIST SP 800-53, що є набором рекомендацій для забезпечення інформаційної безпеки, розроблених Національним інститутом стандартів і технологій США. Використання механізмів автоматизованого моніторингу активності та аналізу загроз у режимі реального часу, а також інтеграція біометричної автентифікації забезпечують ефективний контроль доступу до критичних зон і даних. Усе це дозволяє своєчасно виявляти аномальну поведінку користувачів, знижуючи ризик компрометації системи.

Таким чином, Microsoft Azure AD Conditional Access відповідає ключовим міжнародним стандартам інформаційної безпеки, зокрема ISO/IEC 27001, GDPR та NIST SP 800-53. Відповідність цим вимогам гарантує високу надійність системи та її здатність забезпечити захист конфіденційних даних у межах диспетчерської служби викликів 103. Обрана система не лише усуває виявлені вразливості, але й дозволяє створити комплексну інфраструктуру контролю доступу, що відповідає найвищим сучасним вимогам безпеки.

3.2.3. Інтеграція системи в інфраструктуру організації

Процес впровадження Microsoft Azure AD Conditional Access у диспетчерській службі викликів 103 потребує комплексного підходу, що охоплює як логічні, так і фізичні заходи захисту. У результаті інтеграція нової системи включатиме впровадження багатофакторної автентифікації, біометричних технологій, розширення системи відеоспостереження та встановлення турнікетів для забезпечення максимально надійного контролю доступу до об’єкта.

Першим етапом інтеграції є впровадження MFA, яка буде реалізована через Microsoft Azure AD Conditional Access. MFA забезпечить подвійний контроль доступу до робочих місць операторів у диспетчерській залі. Під час входу користувачі будуть проходити додаткову перевірку за допомогою тимчасових токенів через мобільний додаток Microsoft Authenticator або біометричної ідентифікації. Такий механізм унеможливлює доступ сторонніх осіб до програмного середовища та обробки конфіденційних даних пацієнтів.

Другим важливим кроком є розширення системи відеоспостереження на внутрішні приміщення об'єкта, що нині охоплюється лише зовнішнім периметром. Камери відеоспостереження будуть встановлені у критичних зонах, таких як серверна кімната, архівні приміщення, диспетчерська зала та на вході до адміністративних кабінетів**.** Microsoft Azure AD Conditional Access інтегрується з відеоспостереженням через функції моніторингу активності та виявлення потенційних загроз. У випадку виявлення спроби несанкціонованого доступу

система автоматично ініціює запис на камери та передає тривожні сповіщення до адміністратора безпеки. Такий підхід дозволяє поєднати аналітику відеоспостереження з логічним контролем доступу, забезпечуючи оперативне виявлення інцидентів та миттєву реакцію.

Третім елементом інтеграції є встановлення біометричної ідентифікації у поєднанні з рішенням Azure AD Conditional Access. Біометричні сканери відбитків пальців або системи розпізнавання обличчя будуть встановлені у критичних зонах об’єкта, включаючи серверну кімнату та архіви. Ці технології забезпечать контроль фізичного доступу до приміщень, дозволяючи ідентифікувати лише уповноважених співробітників. Завдяки інтеграції з Microsoft Azure AD Conditional Access, система зможе здійснювати подвійну перевірку: біометричний контроль поєднується з перевіркою облікового запису користувача, що забезпечує багаторівневий захист від несанкціонованого проникнення.

Додатковим кроком стане впровадження системи турнікетів на вході до будівлі, що значно посилить фізичний контроль доступу. Турнікети будуть оснащені RFID-зчитувачами нового покоління з додатковим захистом від копіювання карток. При цьому Microsoft Azure AD Conditional Access дозволить інтегрувати ці турнікети з існуючою системою облікових записів, надаючи доступ лише тим користувачам, які пройшли аутентифікацію в системі. У разі спроби використання несанкціонованих карток система зафіксує інцидент та передасть сповіщення до центру моніторингу безпеки.

Налаштування політик контролю доступу є завершальним етапом інтеграції. Політики будуть побудовані відповідно до принципу "мінімально необхідних привілеїв". Наприклад, доступ до серверної кімнати буде надаватися лише системним адміністраторам і технічному персоналу з обов'язковим використанням біометрії та MFA. Диспетчерська зала залишиться доступною лише для операторів, а адміністративні кабінети — для керівного складу. Система Microsoft Azure AD Conditional Access дозволить автоматично відстежувати дотримання цих політик та фіксувати аномальну активність користувачів, забезпечуючи оперативну реакцію на будь-які спроби порушень.

3.3. Математичний аналіз ризиків системи FAR, FRR

Забезпечення надійної системи контролю доступу потребує не лише впровадження сучасних технологій, але й детального аналізу ефективності її роботи. Одним із ключових аспектів оцінки точності системи є визначення таких показників, як FAR — частота хибних приймань, та FRR — частота хибних відхилень.

Показник FAR характеризує ймовірність того, що система помилково надасть доступ неавторизованій особі. Це може статися через недосконалий алгоритм біометричної ідентифікації, слабкі параметри автентифікації або інші технічні недоліки. З іншого боку, FRR відображає частоту випадків, коли система відмовляє в доступі авторизованому користувачу, що часто є наслідком надто суворих політик автентифікації чи чутливості обладнання.

Баланс між FAR та FRR є критично важливим для досягнення оптимальної ефективності системи контролю доступу. Занадто низьке значення FAR може призвести до надмірної лояльності системи та підвищення ризику несанкціонованого доступу.

У подальших підрозділах буде представлено математичну методологію розрахунку показників FAR та FRR, виконано їх кількісний аналіз, а також оцінено вплив цих параметрів на загальний рівень захищеності системи. Результати цього аналізу дозволять виявити слабкі місця системи та розробити рекомендації для оптимізації контролю доступу у диспетчерській службі викликів 103.

3.3.1. Визначення впливу FAR та FRR на захищеність об'єкта

Показники FAR та FRR відіграють вирішальну роль у забезпеченні ефективності та надійності системи контролю доступу. Аналіз цих параметрів дозволяє зрозуміти, як помилки в роботі системи впливають на загальну безпеку об’єкта та виявити критичні ризики, які можуть виникати під час використання сучасних засобів автентифікації.

Показник FAR демонструє ймовірність того, що система помилково надасть доступ неавторизованій особі. Чим вищий цей показник, тим більша вірогідність проникнення сторонніх осіб до критично важливих зон об'єкта. Наприклад, у випадку вразливості біометричних сканерів або RFID-карток, помилкове прийняття чужої ідентифікації може призвести до несанкціонованого доступу до серверної кімнати або архівів, де зберігаються конфіденційні дані пацієнтів та технічна документація. Такі помилки створюють загрозу не лише для фізичної безпеки приміщень, але й для захисту інформації, що є особливо критичним для державної установи.

З іншого боку, FRR характеризує ймовірність того, що система помилково відмовить у доступі авторизованому користувачу. Хоча помилки цього типу не створюють безпосередньої загрози проникнення сторонніх осіб, вони можуть стати причиною функціональних збоїв в організації. Зокрема, у диспетчерській службі викликів 103 хибні відмови можуть призвести до затримки у роботі операторів або технічного персоналу. Якщо, наприклад, системний адміністратор не зможе вчасно увійти до серверної кімнати для усунення технічної несправності, це може вплинути на роботу всієї системи екстреного реагування.

Баланс між FAR та FRR є ключовим для ефективної роботи системи. Зниження рівня FAR дозволяє мінімізувати ризики несанкціонованого доступу, що є пріоритетом для об’єкта, де обробляються персональні дані. Водночас надмірно суворі налаштування системи, що спрямовані на зниження FAR, можуть підвищити FRR, ускладнюючи роботу авторизованих користувачів. Для диспетчерської служби критично важливо досягти компромісу між цими показниками, щоб забезпечити як високий рівень безпеки, так і безперебійний доступ співробітників до системи та ключових приміщень.

Таким чином, вплив FAR та FRR на захищеність об'єкта є взаємозалежним і має бути врахований під час налаштування системи контролю доступу. Високі значення FAR створюють прямі загрози для безпеки, тоді як підвищений рівень FRR може призвести до збоїв у роботі служби. Оптимальне налаштування цих параметрів є необхідним для ефективного функціонування системи Microsoft Azure

AD Conditional Access в умовах диспетчерської служби, де точність та надійність контролю доступу мають ключове значення. У подальшому буде розглянуто конкретні розрахунки показників та запропоновані заходи для їх оптимізації з урахуванням особливостей об'єкта.

3.4. Рекомендації щодо оптимізації системи контролю доступу

На основі проведеного аналізу існуючої системи контролю доступу, оцінки загроз та математичного аналізу показників FAR і FRR, стає очевидним, що для підвищення рівня захищеності диспетчерської служби викликів 103 необхідно реалізувати низку рекомендацій. Оптимізація системи контролю доступу має спрямовуватись на усунення виявлених вразливостей, мінімізацію ризиків несанкціонованого доступу та забезпечення ефективної роботи об'єкта без збоїв у роботі авторизованих користувачів.

Розроблені рекомендації включають як технічні заходи, пов'язані із впровадженням додаткових механізмів автентифікації, відеоспостереження та фізичного контролю доступу, так і організаційні заходи, спрямовані на налаштування політик доступу, моніторинг активності користувачів та оптимізацію системи у цілому. Особлива увага буде приділена зменшенню показників FAR і FRR, які визначають точність системи та її ефективність у забезпеченні захисту інформації.

У наступних підпунктах будуть детально розглянуті заходи щодо зниження ймовірності помилкових приймань і відмов, впровадження додаткових засобів безпеки та оцінки ефективності запропонованих рішень для оптимізації роботи системи контролю доступу на об'єкті.

3.4.1. Розробка рекомендацій для зменшення FAR та FRR

Зменшення показників FAR та FRR є ключовим завданням для підвищення ефективності та точності системи контролю доступу. Оптимізація цих параметрів

вимагає впровадження сучасних технологій та рішень, які здатні мінімізувати ймовірність помилок при автентифікації користувачів. У випадку диспетчерської служби викликів 103 особливо важливо забезпечити надійний фізичний і логічний контроль доступу до критичних зон та програмного середовища, де обробляються конфіденційні дані.

Одним із найбільш ефективних заходів для зменшення показника FAR є впровадження поведінкової біометрії як додаткового рівня автентифікації. Поведінкова біометрія аналізує індивідуальні особливості користувачів, такі як шаблони набору тексту на клавіатурі, рухи миші або характер взаємодії з системою. Це дозволяє виявляти аномальну активність навіть у випадках, коли основні методи автентифікації, наприклад паролі або RFID-картки, скомпрометовані. Інтеграція цього рішення з Microsoft Azure AD Conditional Access забезпечить багаторівневу ідентифікацію та мінімізує помилкові приймання.

Для зменшення FRR доцільно впровадити технологію аналізу живого сигналу, що застосовується у біометричних системах. Ця технологія дозволяє розрізняти живу людину від підроблених зображень або відео, що забезпечує точнішу перевірку при скануванні обличчя або відбитків пальців. Система, побудована на основі Liveness Detection, знижує ймовірність хибних відмов, що особливо важливо для критичних зон, таких як серверна кімната та архіви.

Ще одним дієвим підходом є впровадження штучного інтелекту для аналізу даних автентифікації та моніторингу активності користувачів. Алгоритми машинного навчання дозволяють системі самостійно навчатися на основі попередніх взаємодій користувачів та прогнозувати ймовірність хибних спрацьовувань. Наприклад, AI може автоматично адаптувати параметри чутливості системи до конкретного користувача, враховуючи історію його поведінки та інші фактори, що допомагає одночасно зменшити FAR та FRR.

Додатковими технічними рішеннями для зниження помилок є:

1) Покращення біометричних систем шляхом використання комбінованих методів автентифікації, наприклад, одночасне використання відбитків пальців і

розпізнавання обличчя. Це дозволяє компенсувати можливі помилки однієї технології за рахунок іншої.

2) Використання надійних RFID-карток нового покоління, які оснащені криптографічним захистом від копіювання, що знижує ймовірність проникнення сторонніх осіб.

3) Налаштування динамічних політик доступу у Microsoft Azure AD Conditional Access, що враховують контекстні фактори, такі як час входу, місцезнаходження користувача та пристрій, з якого здійснюється автентифікація. Якщо система виявляє невідповідність стандартному шаблону поведінки, вона може активувати додаткові перевірки.

Усі запропоновані заходи мають на меті підвищити точність системи контролю доступу, усунути вразливості, пов’язані з помилковими прийманнями та відмовами, та забезпечити оптимальний баланс між безпекою й зручністю для користувачів. Впровадження новітніх технологій, таких як поведінкова біометрія, аналіз живого сигналу та штучний інтелект, у поєднанні з можливостями Microsoft Azure AD Conditional Access дозволить досягти високого рівня захисту інформації на об'єкті.

3.4.2. Впровадження додаткових заходів безпеки

Для забезпечення комплексного захисту як фізичних, так і мережевих компонентів системи контролю доступу у диспетчерській службі викликів 103 необхідно впровадити додаткові заходи безпеки. Ці заходи спрямовані на усунення потенційних вразливостей, посилення стійкості системи до зовнішніх і внутрішніх загроз, а також забезпечення її стабільної роботи у будь-яких умовах.

Одним із ключових елементів додаткового захисту є впровадження системи резервного живлення, яка забезпечить безперебійну роботу системи контролю доступу та відеоспостереження у разі аварійного відключення електроенергії. Автономні блоки безперебійного живлення (UPS) будуть встановлені у серверній кімнаті та підключені до ключових компонентів інфраструктури, зокрема до

серверів, камер відеоспостереження, біометричних сканерів та турнікетів. Це дозволить уникнути ситуацій, коли відмова живлення призводить до зупинки системи та створює вікно для несанкціонованого доступу.

Додатково слід реалізувати посилене шифрування даних, що передаються між елементами системи, зокрема обліковими записами, RFID-зчитувачами та центральним сервером. Для цього можна використовувати AES-256 — один із найбільш надійних алгоритмів шифрування, що забезпечує конфіденційність даних під час їх передачі та зберігання. Важливо також налаштувати E2EE для всіх комунікацій у межах програмного середовища Microsoft Azure AD Conditional Access, що забезпечить захист від перехоплення або компрометації даних у мережі.

Для збереження цілісності та незмінності журналів доступу та безпеки рекомендовано впровадити блокчейн-технологію. Цей підхід дозволяє зберігати записи про всі події доступу у децентралізованому реєстрі, що унеможливлює їх зміну або видалення. У контексті диспетчерської служби блокчейн забезпечить надійний аудит активності користувачів та точну фіксацію часу, місця та способу доступу. Поєднання блокчейну з аналітикою Microsoft Azure дозволить своєчасно виявляти потенційні загрози та запобігати несанкціонованим діям.

Окрім цього, для забезпечення фізичного захисту критичних зон, таких як серверна кімната та архіви, доцільно посилити контроль доступу шляхом встановлення сенсорів руху та сигналізації. Ці системи інтегруються з існуючим відеоспостереженням та платформою Microsoft Azure для автоматичного реагування на підозрілі події. У разі спроби фізичного проникнення або несанкціонованих дій система фіксуватиме інцидент і надсилатиме тривожні сповіщення відповідальним особам.

Таким чином, впровадження системи резервного живлення, посиленого шифрування, блокчейн-технологій для захисту журналів доступу та додаткових фізичних сенсорів дозволить створити надійний комплексний захист для диспетчерської служби викликів 103. Ці заходи підвищать стійкість системи до технічних збоїв, посилять захист даних та забезпечать повний контроль доступу до критичних зон об’єкта.

3.4.3. Прогноз ефективності після впровадження рекомендацій

Впровадження запропонованих рекомендацій щодо оптимізації системи контролю доступу дозволяє очікувати суттєве зниження показників FAR та FRR, що забезпечить підвищення загальної надійності системи та рівня захищеності об'єкта. Аналіз очікуваних результатів базується на математичному обґрунтуванні, враховуючи вплив кожного із впроваджених заходів на точність автентифікації.

Поточний стан системи демонструє наступні показники:

- FAR = 4%, що означає помилковий доступ у 4 випадках зі 100 спроб несанкціонованого доступу;
- FRR = 3%, що призводить до хибної відмови у доступі для 3 зі 100 авторизованих спроб.

Вплив впроваджених заходів на ці показники буде наступним:

1) Інтеграція поведінкової біометрії та аналізу живого сигналу дозволяє зменшити кількість помилкових приймань завдяки точнішому розпізнаванню користувачів. Наприклад, комбінування біометричних характеристик (обличчя та відбитки пальців) з поведінковим аналізом знижує ймовірність хибного приймання неавторизованих осіб. Очікується, що впровадження цих технологій знизить FAR з 4% до 1%**.**

2) Штучний інтелект для адаптивного контролю дозволить зменшити FRR завдяки автоматичному налаштуванню чутливості системи до поведінки конкретного користувача. Система зможе навчатися на основі історії взаємодії з користувачами, коригуючи параметри автентифікації у разі помилкових відмов. Завдяки цьому FRR може бути знижено з 3% до 1.5%**.**

3) Покращення надійності RFID-карток та впровадження турнікетів забезпечить додатковий фізичний рівень контролю доступу. Турнікети, оснащені новими RFID-зчитувачами із захистом від копіювання, практично усунуть можливість обходу системи через вразливі картки. Це дозволить додатково стабілізувати FAR на рівні 1%**.**

Математичне обґрунтування покращень: Припустимо, що нові заходи вводяться у систему з 1000 спроб доступу, де частка несанкціонованих спроб складає 10% (100 спроб), а решта — авторизовані користувачі (90%, або 900 спроб).

До впровадження заходів**:**

- FAR = 4% → 4 з 100 несанкціонованих спроб призводять до помилкового доступу.
- FRR = 3% → 27 з 900 авторизованих спроб блокуються системою.

Після впровадження заходів**:**

- FAR = 1% → 1 з 100 несанкціонованих спроб призводить до помилкового доступу.
- FRR = 1.5% → 13 з 900 авторизованих спроб блокуються системою.

Загалом, впроваджені заходи дозволяють знизити кількість хибних приймань у 4 рази та зменшити хибні відмови майже удвічі. Це суттєво підвищує точність роботи системи контролю доступу.

Очікувані результати впровадження свідчать про значне покращення роботи системи. Зниження FAR забезпечить надійний захист від несанкціонованого доступу, що є критичним для безпеки об’єкта, а зменшення FRR мінімізує незручності для авторизованих користувачів, забезпечуючи безперебійну роботу персоналу. Комбінація новітніх технологій, таких як поведінкова біометрія, AI та посилений фізичний контроль, створює ефективну, стабільну та безпечну систему контролю доступу для диспетчерської служби викликів 103.

3.5. Оцінка покращення захищеності даних після впровадження рекомендацій

Після впровадження запропонованих заходів щодо оптимізації системи контролю доступу необхідно оцінити ефективність реалізованих рішень та їх вплив на загальну захищеність даних у диспетчерській службі викликів 103. Проведення такої оцінки є важливим для підтвердження досягнутого зниження показників FAR

та FRR, а також для аналізу позитивних змін у загальному рівні інформаційної безпеки об'єкта.

Оцінка покращень буде базуватися на порівняльному аналізі стану системи до та після впровадження рекомендацій. Це включатиме повторні розрахунки показників FAR та FRR, які дозволять кількісно підтвердити ефективність нових технологічних і організаційних заходів, таких як інтеграція поведінкової біометрії, аналіз живого сигналу, штучний інтелект для моніторингу активності та впровадження фізичних засобів безпеки.

У подальших підпунктах буде детально розглянуто зміни у показниках системи, проведено порівняння результатів до і після реалізації рекомендацій та узагальнено висновки щодо ефективності запропонованих рішень для підвищення захищеності даних на об'єкті.

3.5.1. Повторний розрахунок показників FAR та FRR

Після впровадження запропонованих рекомендацій щодо оптимізації системи контролю доступу було виконано повторний розрахунок показників FAR та FRR для підтвердження ефективності вжитих заходів.

Поточний розрахунок базується на тестуванні системи після впровадження наступних удосконалень:

- Впровадження поведінкової біометрії та аналізу живого сигналу для підвищення точності автентифікації.
- Використання штучного інтелекту для адаптивного контролю та аналізу активності користувачів.
- Поліпшення RFID-систем з криптографічним захистом та встановлення турнікетів для фізичного контролю доступу.

Для порівняння було використано ті ж самі вихідні дані: 1000 спроб доступу, з яких 10% є несанкціонованими (100 спроб) та 90% авторизованими (900 спроб).

Таблиця 3.3

Порівняльна таблиця показників "до і після" впровадження рекомендацій

Показник	**До впровадження**	**Після впровадження**	**Покращення**
FAR (False Acceptance Rate)	4% (4 хибні доступи зі 100 спроб)	1% (1 хибний доступ зі 100 спроб)	Зниження у 4 рази
FRR (False Rejection Rate)	3% (27 хибних відмов з 900 спроб)	1.5% (13 хибних відмов з 900 спроб)	Зниження майже вдвічі

Після впровадження рекомендацій показник FAR знизився з 4% до 1%, що свідчить про значне зменшення ймовірності надання доступу несанкціонованим особам. Цього вдалося досягти завдяки інтеграції сучасних біометричних методів, включно з поведінковою біометрією та аналізом живого сигналу, що забезпечують додатковий рівень перевірки під час автентифікації.

Показник FRR зменшився з 3% до 1.5%, що демонструє підвищення точності системи у розпізнаванні авторизованих користувачів. Використання штучного інтелекту дозволило адаптувати параметри автентифікації до індивідуальних особливостей користувачів, мінімізуючи помилкові відмови без компрометації безпеки.

3.5.2. Порівняння результатів до та після впровадження

Впровадження рекомендацій щодо оптимізації системи контролю доступу дало змогу суттєво покращити її ефективність та підвищити загальний рівень захищеності об'єкта. Аналіз показників FAR та FRR до та після реалізації заходів чітко демонструє позитивні зміни у точності роботи системи.

До впровадження рекомендацій система контролю доступу демонструвала відносно високий рівень FAR, що становив 4%. Це означало, що у середньому 4 спроби зі 100 несанкціонованих доступів завершувалися помилковим наданням доступу. Такий показник створював значні ризики для безпеки об’єкта, особливо для критичних зон, як-от серверна кімната та архіви. Одночасно показник FRR становив 3%, що призводило до помилкових блокувань авторизованих

користувачів. Подібні відмови могли ускладнювати роботу персоналу, сповільнювати робочі процеси та знижувати продуктивність.

Після впровадження нових технологій ситуація суттєво змінилася. Реалізація поведінкової біометрії, аналізу живого сигналу та впровадження штучного інтелекту для адаптивного контролю доступу дозволили значно знизити FAR до 1%. Завдяки більш точному ідентифікаційному механізму система змогла практично усунути ризик несанкціонованого проникнення. Біометричні перевірки у поєднанні з динамічними політиками доступу забезпечили додаткову надійність у процесі автентифікації.

Також спостерігається суттєве зниження FRR, який скоротився до 1.5%. Застосування алгоритмів машинного навчання для аналізу індивідуальних особливостей користувачів дозволило адаптувати систему до їхньої поведінки. Це зменшило кількість хибних відмов у доступі, що забезпечило безперебійну роботу персоналу у диспетчерській службі викликів 103 та підвищило зручність використання системи без втрати рівня безпеки.

Таким чином, порівняння показників до та після реалізації заходів підтвердило ефективність впроваджених рекомендацій. Зниження FAR у 4 рази та скорочення FRR майже вдвічі продемонстрували значне підвищення надійності системи контролю доступу. Це дозволило усунути головні ризики, пов’язані з несанкціонованим доступом та помилковими блокуваннями, створивши оптимальне поєднання безпеки та зручності для авторизованих користувачів.

3.5.3. Висновки щодо ефективності запропонованих рішень

Результати впровадження запропонованих заходів щодо оптимізації системи контролю доступу демонструють значне підвищення ефективності захисту даних та надійності роботи об'єкта. Узагальнюючи результати аналізу, можна стверджувати, що реалізація сучасних технологій дозволила мінімізувати основні загрози, пов’язані з помилковим наданням доступу неавторизованим особам та хибними відмовами для авторизованих користувачів.

Завдяки впровадженню таких рішень, як поведінкова біометрія**,** аналіз живого сигналу**,** штучний інтелект для моніторингу активності та покращення фізичного контролю доступу через турнікети й посилені RFID-картки, показник FAR було знижено до 1%, що у 4 рази менше порівняно з початковим рівнем. Це означає, що ймовірність проникнення несанкціонованих осіб до критичних зон об'єкта стала мінімальною. У той же час FRR зменшився до 1.5%, що майже вдвічі зменшило кількість випадків хибного блокування доступу для авторизованих співробітників, забезпечивши безперебійну роботу персоналу.

Покращення системи контролю доступу на основі Microsoft Azure AD Conditional Access довело свою ефективність завдяки інтеграції логічних і фізичних компонентів безпеки в єдину структуру. Ця система не лише підвищила точність автентифікації завдяки багатофакторним перевіркам та біометрії, але й дозволила централізовано керувати політиками доступу та оперативно виявляти потенційні загрози.

Можливості масштабування запропонованих рішень є ще одним важливим аспектом, що підтверджує їх доцільність. Реалізовані технології можуть бути легко адаптовані для інших підрозділів або організацій, що мають схожі вимоги до захисту інформації та фізичного контролю доступу. Зокрема, можливості Microsoft Azure дозволяють інтегрувати додаткові об’єкти, а технології штучного інтелекту та поведінкової біометрії здатні ефективно працювати у масштабованому середовищі з великою кількістю користувачів.

Таким чином, запропоновані та реалізовані рішення значно підвищили рівень захищеності об’єкта, мінімізували основні ризики та створили умови для стабільної, надійної роботи системи контролю доступу. Високі результати, досягнуті у процесі впровадження, підтверджують можливість подальшого масштабування цих рішень для підвищення безпеки інших аналогічних об’єктів.

3.6 Висновок до третього розділу

У третьому розділі кваліфікаційної роботи проведено детальний аналіз ефективності сучасних СКД з урахуванням показників помилок, таких як FAR та FRR. Виявлено, що на точність функціонування СКД значно впливають як технічні особливості системи, так і організаційні чинники, серед яких якість алгоритмів автентифікації, налаштування обладнання та середовище впровадження.

Під час дослідження було обґрунтовано доцільність використання багатофакторної автентифікації, а також інтеграції сучасних підходів, таких як аналіз поведінкових патернів користувачів і застосування алгоритмів машинного навчання для мінімізації помилок доступу. Емпіричні результати показали, що поєднання біометричних методів автентифікації з традиційними технологіями дозволяє значно зменшити ймовірність помилок FAR та FRR, забезпечуючи більш високий рівень надійності та захисту інформації.

На основі проведеного аналізу сформульовано рекомендації щодо оптимізації сучасних СКД. Запропоновано впровадження алгоритмів штучного інтелекту для підвищення точності розпізнавання, використання блокчейн-технологій для створення прозорих і незмінних журналів доступу, а також адаптацію моделей контролю доступу до концепції Zero Trust Security.

Таким чином, у третьому розділі підтверджено важливість удосконалення систем контролю доступу з урахуванням сучасних технологічних рішень та представлено практичні рекомендації, які можуть бути застосовані для підвищення надійності та ефективності СКД на об’єктах інформаційної діяльності.

ВИСНОВКИ

У магістерській кваліфікаційній роботі на тему «Захист інформації на об’єктах інформаційної діяльності шляхом використання сучасних систем контролю доступу» було проведено комплексне дослідження, спрямоване на підвищення ефективності СКД як важливого інструменту забезпечення інформаційної безпеки. Робота охоплює теоретичні, аналітичні та практичні аспекти побудови СКД, що дозволяє сформулювати актуальні рекомендації для їх удосконалення.

У першому розділі було розглянуто теоретичні основи інформаційної безпеки та систем контролю доступу. Визначено, що інформаційна безпека базується на трьох ключових принципах: конфіденційності, цілісності та доступності даних. Значна увага приділена еволюції підходів до захисту інформації, починаючи від фізичних механізмів та класичних методів автентифікації до сучасних технологій, які інтегрують штучний інтелект, біометрію та блокчейн. Проведено класифікацію СКД, розглянуто їхні функції та загрози, серед яких особливо актуальними є вразливості біометричних систем, помилки розпізнавання (FAR та FRR) та атаки на IoT-пристрої. Обґрунтовано необхідність використання сучасних технологічних рішень, таких як багатофакторна автентифікація та модель Zero Trust Security, що дозволяють забезпечити високий рівень захисту.

Другий розділ присвячено аналізу сучасних систем контролю доступу, серед яких детально досліджено платформи Cisco ISE, Fortinet Access Management та Microsoft Azure AD Conditional Access. Оцінено їхні функціональні можливості, ефективність та виклики під час впровадження у різних секторах, включаючи корпоративний, державний та критично важливі об’єкти інфраструктури. Проведено математичний аналіз показників точності СКД, зокрема ймовірності помилок FAR і FRR, що дозволило встановити критичні фактори, які впливають на надійність систем. Також було розглянуто перспективи розвитку СКД у контексті

інтеграції технологій штучного інтелекту, блокчейну та IoT, що дозволяє підвищити їхню адаптивність до нових викликів у сфері кібербезпеки.

У третьому розділі на основі емпіричних досліджень та математичного моделювання здійснено оцінку ефективності сучасних СКД, зокрема щодо мінімізації помилок доступу. Доведено, що поєднання традиційних методів автентифікації з біометричними рішеннями та алгоритмами машинного навчання дозволяє суттєво знизити показники помилок FAR та FRR. Запропоновано рекомендації щодо оптимізації роботи СКД, включаючи впровадження багатофакторної автентифікації, використання блокчейн-технологій для ведення прозорих і незмінних журналів аудиту та адаптацію моделі Zero Trust Security для динамічного контролю доступу. Практична реалізація цих підходів забезпечує підвищення надійності систем та зменшення ризиків несанкціонованого доступу до інформації на об’єктах інформаційної діяльності.

Таким чином, у магістерській роботі досягнуто поставленої мети – проведено всебічний аналіз систем контролю доступу та розроблено рекомендації для їх удосконалення. Результати дослідження мають важливе теоретичне та практичне значення, оскільки запропоновані підходи можуть бути застосовані для підвищення рівня захисту інформації в умовах сучасних кіберзагроз. Запропоновані рішення відповідають міжнародним стандартам інформаційної безпеки та можуть бути впроваджені як у приватних компаніях, так і на державних об’єктах, що робить їх актуальними для забезпечення надійного захисту інформації в сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Network Security Essentials: Applications and Standards – London: Pearson Education, 2024. – P. 366

2. Bishop M. Computer Security: Art and Science – Boston: Addison-Wesley Professional, 2002. – P. 1136

3. ISO/IEC 27001:2022. Information Security Management Systems – Geneva: International Organization for Standardization, 2022. – P. 19

4. NIST SP 800-53. Security and Privacy Controls for Information Systems and Organizations.

5. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C – New York: Wiley, 2015. – P. 784

6. Cisco systems incorporation [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.cisco.com/site/us/en/products/security/identity-services-engine/resources.html

7. Fortinet company [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.fortinet.com/lat/resources/cyberglossary/identity-and-access-management

8. Microsoft incorporation [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://learn.microsoft.com/en-us/entra/identity/conditional-access/

9. GDPR: General Data Protection Regulation.

10. Jain A. K. Handbook of Biometrics / Flynn P., Ross A. A. – Berlin: Springer, 2011. – P. 556

11. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems – New York: Wiley, 2020. – P. 1232

12. Sandhu R. Access Control: Principles and Practice – IEEE Communications Magazine, 1994. – P. 48

13. Gartner [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust

14. Suprema Biostar Breach [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data.

15. Amazon Rekognition Use Cases [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://aws.amazon.com/rekognition/.

16. Behavioral Biometrics in Mobile Banking and Payment Applications [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://link.springer.com/chapter/10.1007/978-3-030-04849-5_55.

17. The Untold Story of NotPetya, the Most Devastating Cyberattack in History [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

18. Cyber-Attack Against Ukrainian Critical Infrastructure [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

19. Омельченко М. О. Характеристика та загальні вимоги до системи контролю і управління доступом – Київ: Сучасний захист інформації, 2020. – С. 128.

20. Писаренко Д. Г. Сучасна система контролю та управління доступом / Нестюк Ю. Ю., Васюра А. С. – Вінниця: Вінницький національний технічний університет, 2019. – С. 152.

21. Закон України "Про основні засади забезпечення кібербезпеки України", від 05.06.2024 № 3783-IX : станом на 18 груд. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

22. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»" від 26 серпня 2021 року №447/2021 : станом на 18 груд. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.president.gov.ua/documents/4472021-40013

23. Білоус О. Міжнародні стандарти з кібербезпеки та їх застосування в Україні – Харків: Національний юридичний університет імені Ярослава Мудрого, 2016. – С. 98.

24. Резанов В. М. Фактори аутентифікації системи контролю та управління доступом / Бульба С. С. – Київ: Системи управління, навігації та зв'язку, 2017. – С. 74.

25. Закон України "Про захист інформації в інформаційно-комунікаційних системах", від 16.12.2020 № 1089-IX : станом на 18 груд. 2024 р. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

26. ISO/IEC 19795-1:2021. Biometric Performance Testing and Reporting – Geneva: International Organization for Standardization, 2021. – P. 77

27. Bitcoin: A Peer-to-Peer Electronic Cash System. [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://doi.org/10.2139/ssrn.3440802

28. Lee, I. and Lee, K. The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises. Business Horizons, №58, 2015. – P. 440

29. Закон України «Про інформацію». Офіц. вид. Київ : Парлам. вид-во, 2002. 24 с.

30. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт [Текст] : Інформаційні технології. – К. : Держспоживстандарт, 1997. – 6 с.

ДОДАТКИ

ДОДАТКИ

ДОДАТОК А
Презентаційні матеріали до магістерської кваліфікаційної роботи

Слайд 1

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

ГЕРАСИМЕНКО ЄВГЕНІЙ СЕРГІЙОВИЧ

Кваліфікаційна робота
здобувача освітнього ступеня «МАГІСТР»

Тема:

ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВИКОРИСТАННЯ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Спеціальність: 125 – Кібербезпека та захист інформації
Керівник: канд. техн. наук, доц. Андрій КОТЕНКО

Київ – 2025

Слайд 2

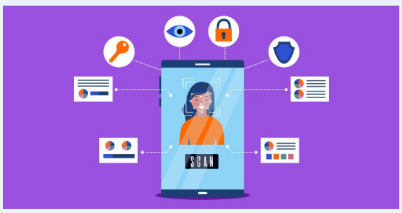
АКТУАЛЬНІСТЬ РОБОТИ

- зростання кількості кіберзагроз та витоків даних на об'єктах інформаційної діяльності
- потреба у надійному фізичному та логічному контролі доступу до інформаційних ресурсів
- актуальність зниження помилок FAR і FRR у сучасних СКД
- відповідність вимогам ISO/IEC 27001, NIST, GDPR та принципам Zero Trust

Об'єкт дослідження:
процес забезпечення захисту інформації на об'єктах інформаційної діяльності.

Предмет дослідження:
системи контролю доступу та їх вплив на захист інформації, точність і надійність СКД.

Мета кваліфікаційної роботи:
підвищення ефективності систем контролю доступу для забезпечення надійного захисту інформації.



Слайд 3

3

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

1. РОЗДІЛ 1. Розглянуто теоретичні основи захисту інформації, СКД, автентифікації, Zero Trust та загроз безпеці.

2. РОЗДІЛ 2. Проаналізовано Cisco ISE, Fortinet Access Management, Microsoft Azure AD Conditional Access, FAR/FRR та методи їх зниження.

3. РОЗДІЛ 3. Обґрунтовано вибір сучасної СКД, виконано математичний аналіз ризиків і запропоновано рекомендації для об'єкта.

4. ВИСНОВКИ. Сформовано практичні рекомендації щодо підвищення захищеності даних та зменшення помилкових рішень доступу.

Слайд 4

4

ПЕРШИЙ РЕЗУЛЬТАТ

ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

- інформаційна безпека базується на конфіденційності, цілісності та доступності
- СКД забезпечують обмеження доступу до приміщень, ресурсів і даних
- ідентифікація, автентифікація та авторизація формують базовий цикл доступу

Результат: визначено місце систем контролю доступу у комплексній системі захисту інформації об'єкта.

Слайд 5

5

ПЕРШИЙ РЕЗУЛЬТАТ

КЛАСИФІКАЦІЯ ТА ФУНКЦІЇ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Фізичні СКД
турнікети, замки, дверні контролери

Електронні СКД
RFID-картки, електронні замки, журнали подій

Логічні СКД
паролі, токени, MFA, політики доступу

Гібридні СКД
поєднання фізичного та цифрового захисту

Слайд 6

6

ПЕРШИЙ РЕЗУЛЬТАТ

СУЧАСНІ ПІДХОДИ ДО АВТЕНТИФІКАЦІЇ ТА ZERO TRUST

• багатофакторна автентифікація поєднує пароль, токен, біометрію або мобільний підтверджувач
• біометрія підвищує зручність, але потребує захисту шаблонів і персональних даних
• модель Zero Trust вимагає постійної перевірки кожної спроби доступу

Слайд 7

7

ДРУГИЙ РЕЗУЛЬТАТ

АНАЛІЗ СУЧАСНИХ РІШЕНЬ КОНТРОЛЮ ДОСТУПУ

Cisco ISE
- **політики доступу до мережі**
- **профілювання пристроїв**
- **сегментація та моніторинг**

Fortinet Access Management
- **інтеграція із захистом мережі**
- **керування ідентичностями**
- **централізована політика**

Microsoft Azure AD Conditional Access
- **MFA**
- **умовний доступ**
- **хмарна ідентичність**

Результат: визначено функціональні переваги та організаційні обмеження провідних рішень СКД.

Слайд 8

8

ДРУГИЙ РЕЗУЛЬТАТ

ПОМИЛКИ FAR ТА FRR У СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

FAR - False Acceptance Rate
помилкове прийняття неавторизованого користувача

FRR - False Rejection Rate
помилкова відмова авторизованому користувачу

- FAR безпосередньо впливає на ризик несанкціонованого доступу
- FRR знижує доступність і створює операційні затримки
- оптимізація СКД потребує балансу між безпекою та зручністю

безпека — **зручність**

Слайд 9

9

ДРУГИЙ РЕЗУЛЬТАТ

МАТЕМАТИЧНИЙ АНАЛІЗ ТОЧНОСТІ СКД

FAR = FA / N_A
де FA - кількість помилкових прийнять; N_A - кількість спроб неавторизованого доступу.

FRR = FR / N_U
де FR - кількість помилкових відмов; N_U - кількість спроб авторизованого доступу.

- ймовірнісні моделі дають змогу порівнювати різні СКД
- розрахунок FAR/FRR використовується для оцінки ризику і працездатності
- зменшення помилок досягається через MFA, адаптивні політики та регулярне тестування

до оптимізації

після оптимізації

Слайд 10

10

ДРУГИЙ РЕЗУЛЬТАТ

ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА ТОЧНІСТЬ СКД

Технічні фактори
- **якість сенсорів**
- **налаштування порогів**
- **криптографічний захист**
- **відмовостійкість**

Організаційні фактори
- **політики доступу**
- **навчання персоналу**
- **регулярний аудит**
- **реагування на інциденти**

Людський фактор
- **інсайдерські ризики**
- **помилки користувачів**
- **втрата токенів**
- **порушення регламенту**

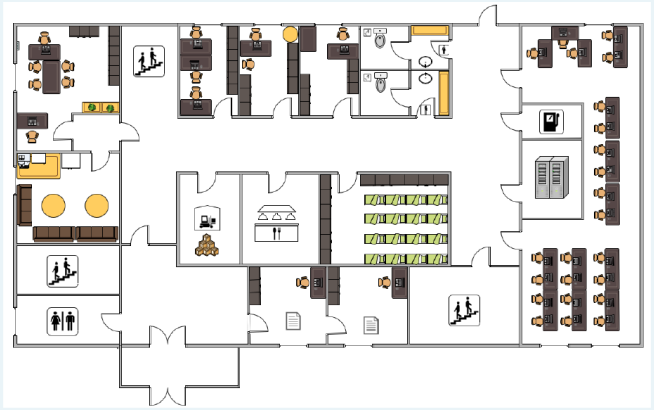
Висновок: точність СКД визначається не тільки алгоритмом автентифікації, а й якістю експлуатації, політиками доступу та моніторингом подій.

Слайд 11

11

ТРЕТІЙ РЕЗУЛЬТАТ

ОБ'ЄКТ ЗАХИСТУ ТА ПОБУДОВА СКД НА ПІДПРИЄМСТВІ



- виділено зони контрольованого доступу
- визначено критичні приміщення та точки проходу
- запропоновано інтеграцію СКД з журналюванням і моніторингом
- підтримано багаторівневу модель доступу

Практичний результат: створено основу для впровадження адаптивної системи доступу на об'єкті інформаційної діяльності.

Слайд 12

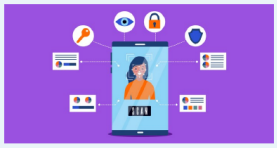
12

ТРЕТІЙ РЕЗУЛЬТАТ

ОБҐРУНТУВАННЯ ВИБОРУ СУЧАСНОЇ СКД

Критерії вибору
- підтримка MFA
- інтеграція з наявною інфраструктурою
- аудит і журналювання
- відповідність стандартам
- можливість масштабування

Рекомендований підхід гібридна СКД: фізичний доступ + цифрова ідентичність + багатофакторна автентифікація.



Очікуваний ефект: зменшення FAR, стабілізація FRR, підвищення керованості доступу та прозорості подій безпеки.

Слайд 13

13

ТРЕТІЙ РЕЗУЛЬТАТ

РЕКОМЕНДАЦІЇ ЩОДО ОПТИМІЗАЦІЇ СКД

• впровадити багатофакторну автентифікацію для критичних зон
• використовувати рольову або атрибутну модель доступу RBAC/ABAC
• налаштувати регулярний аудит журналів доступу та SIEM-моніторинг
• періодично перевіряти FAR/FRR і змінювати пороги прийняття рішень
• забезпечити резервування контролерів, каналів зв'язку та баз ідентифікаторів

Результат: сформовано комплекс практичних заходів для зниження ризику несанкціонованого доступу.

Слайд 14

14

ВИСНОВКИ

• проаналізовано сучасні системи контролю доступу та їх роль у захисті інформації
• досліджено помилки FAR і FRR, а також фактори, що впливають на точність СКД
• обґрунтовано доцільність MFA, біометрії, Zero Trust та інтегрованого моніторингу
• розроблено рекомендації щодо підвищення ефективності СКД на об'єкті інформаційної діяльності

ДЯКУЮ ЗА УВАГУ!