Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу

Виконав: ст 2-го курсу, групи КІТС-22м
спеціальності 125 – Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
Кметюк Олександр Олександрович
Керівник: к.т.н., доцент каф. МБІС
Карпінець В.В.
«04» грудня 2023р.
Опонент: к.т.н., доц., доцент каф. ОТ
Тарновський М.І.
«04» грудня 2023р.

Допущено до захисту
Голова секції УБ кафедри МБІС

_____ Юрій ЯРЕМЧУК
«04» грудня 2023р.

Вінниця ВНТУ - 2023 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС

_____ **Юрій ЯРЕМЧУК**
“ 20 ” вересня 2023 р.

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу студенту

Кметюку Олександру Олександровичу

1. Тема роботи «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу»

Керівник роботи Карпінець В.В. к.т.н., доцент затверджені наказом вищого навчального закладу від “18” вересня 2023 року № 247

2. Строк подання студентом роботи за тиждень до захисту

3. Вихідні дані до роботи: нормативно-правова база, монографії та сучасні наукові статті по темі, Інтернет-ресурси, стандарти, існуюче ПЗ.

4. Зміст текстової частини: в першому розділі проаналізувати існуючі системи моніторингу управління доступом; в другому розділі здійснити вдосконалення методу, провести проектування розробки, розробити алгоритми програмної частини, розробити алгоритми апаратної частини; в третьому розділі здійснити апаратну реалізацію розробки, програмну реалізацію розробки, та аналіз результатів; в четвертому розділі проаналізувати економічну ефективність розробленого програмного забезпечення.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень)

– у першому розділі наведено 7 рис., 1 табл.;

– у другому розділі наведено 4 рис., 3 табл.;

– у третьому розділі наведено 7 рис.;

– у четвертому розділі наведено 12 табл.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	к.т.н., доц. каф. МБІС Карпінець В.В.		
Економічна частина	к.е.н., доц. каф. ЕПВМ Причепа І.В.		

7.Дата видачі завдання 20 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку МКР, формулювання теми	20.09.2023	25.09.2023	
2.	Аналіз предметної області обраної теми	26.09.2023	10.10.2023	
3.	Розробка алгоритму роботи	11.10.2023	22.10.2023	
4.	Написання МКР на основі розробленої теми	23.10.2023	16.11.2023	
5.	Розробка економічної частини	17.11.2023	23.11.2023	
6.	Попередній захист МКР	24.11.2023	25.11.2023	
7.	Виправлення, уточнення, коригування роботи	26.11.2023	30.11.2023	
8.	Захист МКР	15.12.2023	15.12.2023	

Студент _____ Кметюк О.О.

Керівник роботи _____ Карпінець В.В.

АНОТАЦІЯ

УДК: 004.056.53:004.6.056.55

Кметюк О.О. Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2023. 99 с.

На укр. мові. Бібліогр.: 42 назв; рис.: 18; табл.: 16.

У магістерській кваліфікаційній роботі представлено підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу із подальшою реалізацією даної вдосконаленої системи.

В першому розділі роботи здійснено аналіз теоретичного матеріалу обраної галузі: досліджено існуючі аналоги систем контролю та управління доступом та виявлення їх слабких місць.

У другому розділі роботи описано вдосконалення системи контролю та управління за рахунок інтеграції резервного каналу на основі GSM модему та шифрування даних за допомогою симетричного алгоритму блочного шифрування AES.

У третьому розділі роботи здійснено практичну реалізацію розробленої системи із використанням вдосконаленого алгоритму та дослідження результатів роботи, за підсумками яких зроблено висновок, що розроблений алгоритм дозволяє успішно реагувати на атаки шляхом блокування основних каналів зв’язку.

У четвертому розділі роботи здійснено аналіз економічної доцільності розробки, який свідчить про її високий комерційний потенціал та доцільність подальшого впровадження.

Ключові слова: система контролю та управління доступом, СКУД, система реального часу, система моніторингу, резервний канал, GSM, AES, ESP32.

ABSTRACT

O.O. Kmetiuk. Enhancing Security Against Cyber Threats through an Improved Access Control Monitoring System with Data Encryption and a Backup Channel. Master's Qualification Work in Specialty 125 - "Cybersecurity," Educational Program "Cybersecurity of Information Technologies and Systems." Vinnytsia: VNTU, 2023. 99 p.

In Ukrainian language. Bibliography: 42 titles; figures: 18; tables: 16.

The master's qualification work introduces improvements in security against cyber threats based on an enhanced access control monitoring system with data encryption and a backup channel, followed by the implementation of this enhanced system.

The first chapter of the work conducts an analysis of the theoretical material in the chosen field, exploring existing analogs of access control and management systems and identifying their weaknesses.

The second chapter describes the enhancement of the access control and management system through the integration of a backup channel based on a GSM modem and data encryption using the symmetric block cipher algorithm AES.

The third chapter of the work implements the developed system practically, utilizing the improved algorithm, and investigates the results. The conclusion is drawn that the developed algorithm successfully responds to attacks by blocking the main communication channels.

In the fourth chapter of the work, an analysis of the economic feasibility of the development is carried out, indicating its high commercial potential and the expediency of further implementation. Keywords: access control and management system, ACS, real-time system, monitoring system, backup channel, GSM, AES, ESP32.

ЗМІСТ

ВСТУП

Актуальність. Завдання забезпечення високого рівня безпеки в інформаційних системах у сучасному світі визначається не тільки потужністю технологічного розвитку, але й загостренням кіберзагроз. Несанкціонований доступ до конфіденційної інформації стає все важче завадити, оскільки зловмисники вдосконалюють свої техніки та використовують різноманітні стратегії атак.

За останні роки спостерігається значний приріст якісних та кількісних характеристик кіберзагроз. Зокрема, фішингові атаки, розповсюдження шкідливих програм та атаки на інфраструктуру стають більш вишуканими та складними для виявлення традиційними методами захисту.

У зв'язку з цим, існує пряма потреба у вдосконаленні систем моніторингу управління доступом, щоб ефективно протистояти сучасним кіберзагрозам. Використання шифрування даних та резервних каналів стає стратегічно важливим для забезпечення високого рівня захисту конфіденційної інформації.

Розробка та впровадження вдосконалених систем безпеки є важливим завданням як для наукового співтовариства, так і для сфери виробництва. Новаторські підходи до захисту інформації не тільки підвищать рівень безпеки, але й сприятимуть розвитку нових стандартів та практик в галузі кібербезпеки.

Отже, розробка та впровадження вдосконалених систем моніторингу управління доступом, з фокусом на шифруванні даних та резервних каналах, стає необхідністю у контексті постійного зростання кіберзагроз. Ця робота має на меті принести вагомий внесок у вдосконалення методів захисту в інформаційних системах та визначити нові стандарти безпеки в цьому швидкозмінюваному цифровому ландшафті.

Мета і задачі дослідження. Метою даної роботи є розробка вдосконаленої системи моніторингу контролю та управління доступом з використанням шифрування даних та резервним каналом.

Задачами дослідження є:

– провести докладний аналіз існуючих систем управління доступом, враховуючи їхню ефективність та можливі слабкі точки.

– розробити та впровадити покращену систему моніторингу управління доступом, що базується на передових технологіях та алгоритмах.

– впровадити механізми шифрування даних для захисту конфіденційної інформації в режимі реального часу та під час зберігання.

– розробити та імплементувати механізми створення резервного каналу, що забезпечить безперебійний доступ у випадку виникнення атак або неполадок.

– провести комплексне тестування розробленої системи, включаючи симуляцію кібератак та аналіз реакції системи на них, з метою оцінки її ефективності.

− економічне обґрунтування доцільності впровадження здійсненої розробки.

Об’єкт дослідження – система моніторингу контролю та управління доступом.

Предмет дослідження – розробка та оптимізація системи моніторингу управління доступом з шифруванням даних та резервним каналом для підвищення ефективності захисту інформаційних систем від несанкціонованого доступу.

Новизна роботи: вдосконалення системи моніторингу контролю та управління доступом за допомогою резервного каналу та шифрування даних.

Практична цінність: розроблено апаратний та програмний продукт який реалізує захист системи контролю та управління доступом від атак блокуванням основних каналів зв’язку

1 АНАЛІЗ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ТА ОГЛЯД ЇХ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ

1.1 Загальний огляд систем контролю та управління доступом

Системи контролю та управління доступом (СКУД), через свою специфіку, відносяться до систем реального часу (СРЧ). СРЧ - це складні пристрої, які включають в себе датчики, що реєструють події на об'єкті, модулі введення-виводу, які перетворюють сигнали з датчиків в цифровий формат, зрозумілий комп'ютеру, і комп'ютер з програмним забезпеченням, яке реагує на події, що відбуваються на об'єкті. Основна мета будь-якої СРЧ полягає в тому, щоб реагувати на непередбачувані події вчасно і у передбачуваний спосіб. Це означає, що система повинна реагувати на події, які виникають на об'єкті, у встановлений передбачуваний час, який зазвичай є критичним для цих подій [1]. Час реакції системи повинен бути заздалегідь розрахованим під час створення системи. Невиконання реакції в установлений час вважається помилкою для систем реального часу [2 – 3].

Крім того, система повинна бути здатна реагувати на події, які стаються одночасно. Навіть якщо дві або більше зовнішніх подій відбуваються одночасно, система повинна встигнути реагувати на кожну з них протягом часових інтервалів, які критичні для цих подій [8]. Розрізняють два типи систем реального часу - жорсткого та м'якого. Системи жорсткого реального часу не допускають будь-яких затримок у реакції системи, оскільки в цих випадках можуть виникнути серйозні наслідки, включаючи катастрофи або великі втрати. Системи м'якого реального часу, допускають певні затримки у реакції, які можуть впливати на результати та продуктивність системи, але не призводити до катастроф.

Системи контролю та управління доступу відносяться до систем м'якого реального часу, оскільки деякі затримки у реакції можуть бути прийнятними, але система повинна все ж реагувати на події без надмірних затримок. Загалом, важливо розуміти, що СКУД, яка є системою реального часу, має свої особливості та вимагає використання конкретних механізмів, які суттєво впливають на її архітектуру.

Розглянемо деякі важливі класифікації систем контролю та управління доступом, подані в [4].

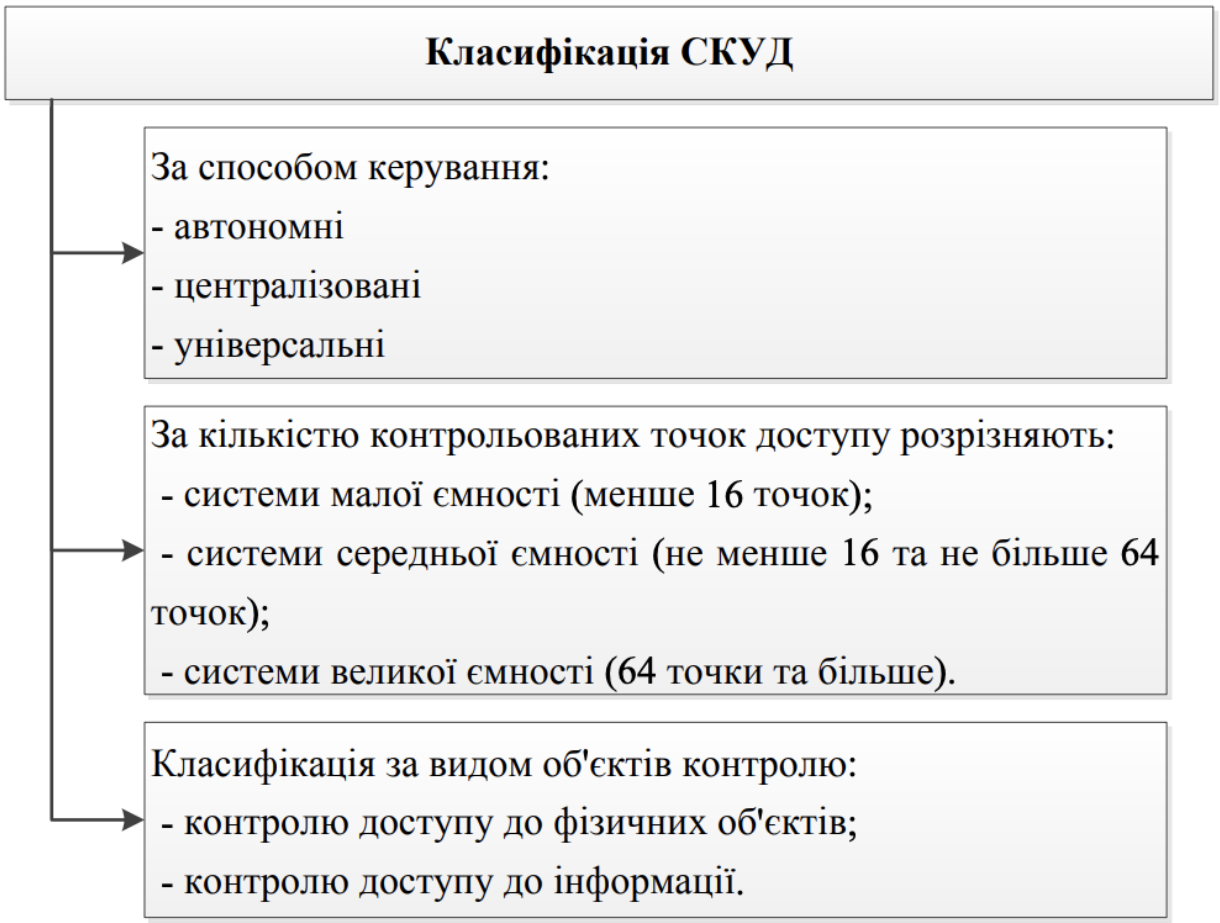


Рисунок 1.1 – Загальна класифікація СКУД (за [5 – 6])

Системи контролю доступу (СКУД) можна класифікувати наступним чином в залежності від способу управління [6]:

Автономні системи: Це прості системи, які призначені для керування доступом до об'єктів без необхідності спілкування з центральним контрольним центром або оператором. Зазвичай це електронні замки, які обмежують доступ до певних місць. Вони часто використовуються в житлових будинках та невеликих об'єктах.

Централізовані (мережеві) системи: Ці системи вимагають обміну інформацією з центральним контрольним центром або оператором для управління доступом. Вони надають можливість постійного контролю за об'єктом і оперативного втручання в роботу системи. У таких системах доступ контролюється автоматично на основі різних обмежень, які визначаються для окремих користувачів або груп користувачів за допомогою спеціальної програми. Оператор може управляти базами даних користувачів, реєструвати та редагувати правила доступу.

Універсальні системи: Ці системи поєднують функції автономних і мережевих систем. Вони можуть працювати у мережевому режимі під керуванням центрального пристрою керування, але переключатися в автономний режим в разі відмови мережевого обладнання, центрального пристрою або обриву зв'язку. Ця класифікація допомагає розуміти, як саме системи контролю доступу організовані і як вони взаємодіють з операторами або центральними контрольними центрами. Важливо враховувати технічні характеристики та функціональні можливості при виборі підходящої СКУД для конкретних потреб.

Критеріями оцінки СКУД є основні технічні характеристики та функціональні можливості.

Основні технічні характеристики представлені рис. 1.2.

Рисунок 1.2 – Основні технічні характеристики СКУД

Вибір структури та технічних засобів СКУД тісно пов'язаний із вимогами системної концепції забезпечення безпеки конкретного об'єкта. Цей вибір визначається під час розробки проекту обладнання для цього об'єкта, яке включає комплекси технічних засобів для забезпечення охорони. Такий підхід передбачає врахування конкретних вимог та завдань щодо безпеки об'єкта при виборі як структури, так і апаратно-програмних засобів СКУД.

1.2 Персональні системи контролю доступу

Зародження приватної власності породило необхідність захищати її від можливих вторгнень. З цією метою були винайдені двері та замки. Замки для вхідних дверей, разом із відповідними ключами, з'явилися ще в ранніх цивілізаціях, про що свідчать згадки в старовинних міфах. Але в перші часи ці замки були великі та мають просту конструкцію. Принцип їхньої роботи лягав в основу перших штифтових замків. Античні пристосування для замикання вхідних

дверей виготовлялися з доступних матеріалів, таких як очерет, волокна, дерево, або пізніше — метал.

Прогрес, як відомо, поширюється на всі сфери життя і включає покращення майже усіх аспектів повсякденного існування. Це також стосується механізмів відкривання дверей. У сучасному світі спостерігається перехід від традиційних механічних ключів до різних форм автоматизованого відкриття дверей за допомогою ідентифікації відвідувача.

У сучасний період еволюція охоплює практично всі аспекти, які використовує людство. Системи замків для дверей є однією з технологій, які не тільки залишаються в активному використанні, але й продовжують свій розвиток. Ця технологія вдосконалюється в процесі переходу від застарілих механічних ключів до більш сучасних методів відкриття дверей. Один із сучасних методів — це використання електронних замків. Ці електронні замки можуть мати різні варіації, як показано на рисунку (рис. 1.3):

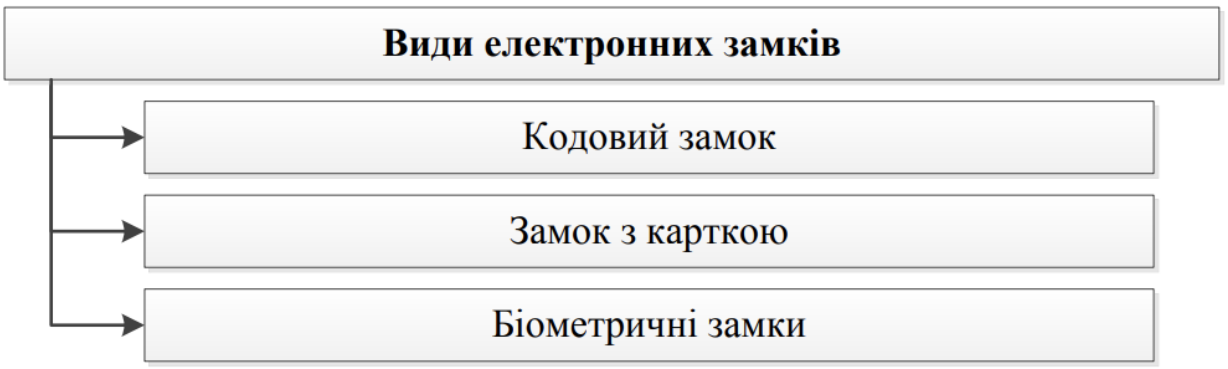


Рисунок 1.3 – Різновиди електронних замків

Більшість сучасних систем замків поєднують кілька механізмів або їх комбінації для захисту від можливих спроб несанкціонованого доступу. Це включає захист від злому шляхом відмикання ключа, використання відмичок або застосування грубої сили. Крім того, якщо замок обладнаний функцією перекодування, у разі втрати ключа можна легко змінити внутрішнє розташування елементів у сердечнику замка, не змінюючи сам замок, і

виготовити новий ключ, щоб унеможливити несанкціонований доступ за допомогою втраченого ключа.

Кодовий замок - це замок, для відкриття якого потрібно ввести спеціальний код доступу з клавіатури. Правильний код зберігається в пам'яті самого пристрою. Цей тип замка має свої переваги:

– Відсутність потреби в ключі, який можна втратити чи скопіювати зловмисником відсутності власника.

– Можливість швидко змінювати код, і це можна робити щодня.

– Зручність передачі коду іншій особі без залучення сторонніх осіб і без втрати доступу власнику.

Проте існують його недоліки:

– Існує ризик забуття коду, особливо якщо він довго не використовувався, але це можна компенсувати його записом.

– Ризик підглядання коду під час введення, тому важливо зберігати конфіденційність при введенні коду.

– Часто як коди використовуються легкозапам'ятовувані числа чи дати, що може полегшити їх взлом методом підбору.

Електронний замок з картою представляє сучасне рішення для забезпечення доступу до офісу виключно для співробітників компанії. Ця система відкриває двері при наближенні магнітної картки або магнітного чіпа. Замок може бути встановлений на двері будь-якого типу. До переваг електромагнітного замка відносяться:

– Легкість запису та видалення даних співробітників з карт, що особливо зручно при зміні користувачів.

– Високий рівень безпеки та тривалість служби.

До недоліків можна віднести:

– Можливість втрати ідентифікаційної картки або чіпа.

– Періодична необхідність заміни акумулятора.

Системи аутентифікації, які використовують біометричні характеристики особи, забезпечують майже 100% точність ідентифікації, вирішуючи проблеми, пов'язані з можливістю втрати або забуття паролів та персональних ідентифікаторів. Прикладами цих методів є системи ідентифікації за райдужною оболонкою ока, відбитками долоні, формою вух, по почерку, за запахом, за тембром голосу та навіть за структурою ДНК.

Прогресивний напрямок використання біометричних характеристик полягає в їх впровадженні в повсякденне життя людини, такі як розрахункові картки, жетони-пропуска та засоби стільникового зв'язку. Наприклад, в деяких передових магазинах країн Європи клієнт може підтвердити власність картки, просто вкладаючи палець на сканер для ідентифікації [10].

В той же час, біометрична аутентифікація має свої обмеження та недоліки:

– Отриманий шаблон порівнюється не з результатом первісної обробки, а з тим, що надійшло до місця порівняння результатів. Під час передачі можуть виникнути перешкоди або навіть можлива підміна.

– Первинна база шаблонів може стати предметом підміни зловмисником.

– Важливо враховувати різницю між застосуванням біометрії на контрольованій території та в умовах, коли пристрій сканування може бути обманутий фальшивим муляжем тощо.

– Більшість біометричних даних людини піддаються змінам (внаслідок старіння, травм, опіків, захворювань, ампутацій і т.д.), що вимагає постійного оновлення бази шаблонів, ускладнюючи контроль і роботу для користувачів та адміністраторів.

– У випадку витоку або компрометації біометричних даних, їх ненадійності призводить до постійних проблем, оскільки, на відміну від паролів, біометричні характеристики важко або неможливо змінити.

– Біометричні характеристики людини, хоч і є унікальними ідентифікаторами, не можна зберігати в абсолютній та абсолютній таємниці.

Ураховуючи усі вищезазначені переваги та недоліки кожного типу замків та методів аутентифікації, важливо спрямувати увагу на призначення системи контролю доступу та її кінцеві цілі. Різні системи можуть встановлювати відмінні завдання для впровадження методів контролю доступу.

Оскільки розроблювана система контролю доступу в даній роботі орієнтована на дистанційний контроль, основна увага має бути приділена електронним замкам з можливістю віддаленого управління. Такі замки надають можливість ефективно впроваджувати дистанційний контроль над доступом та забезпечують додаткові переваги, які можуть бути важливими для даної системи.

Ключовим аспектом є також збалансування між безпекою та зручністю використання, щоб система відповідала вимогам та потребам користувачів, забезпечуючи при цьому ефективний та надійний контроль доступу.

1.3 Можливості дистанційного управління системами контролю доступу

На сьогоднішній день дистанційне відстеження стрімко розвивається і знаходить широке застосування в різних сферах людської діяльності. Дистанційне відстеження визначається як передача інформації від об'єкта управління до оператора, який перебуває на відстані. Цей процес поступово інтегрується в системи автоматизації, оскільки не завжди можливо безпосередньо спостерігати за об'єктом управління. Наприклад, це особливо актуально у випадках, коли об'єкт пересувається, знаходиться на великій відстані або в агресивному середовищі.

Дистанційне відстеження системи управління доступом насамперед важливе з погляду забезпечення безпеки об'єкта. У випадку виникнення надзвичайних ситуацій, таких як порушення в приміщенні, обладнаному системою дистанційного відстеження, це значно полегшує виявлення винуватця

події. Завдяки сучасним технологіям можна легко налаштувати дистанційне керування в домашніх умовах за невеликі витрати на складові системи.

Реалізація дистанційного спостереження за системою управління доступом має широкий спектр застосувань, залежно від конкретної мети використання. Це може бути відстеження за дверима гаража, будинку, квартири чи навіть сейфа. Важливо відзначити, що існують багато інших можливостей використання такої системи відстеження, які виходять за межі зазначених прикладів.

Передача цифрової інформації від джерела до одержувача відбувається за допомогою різних засобів транспортування, які можна класифікувати (див. рис. 1.4) [13]:

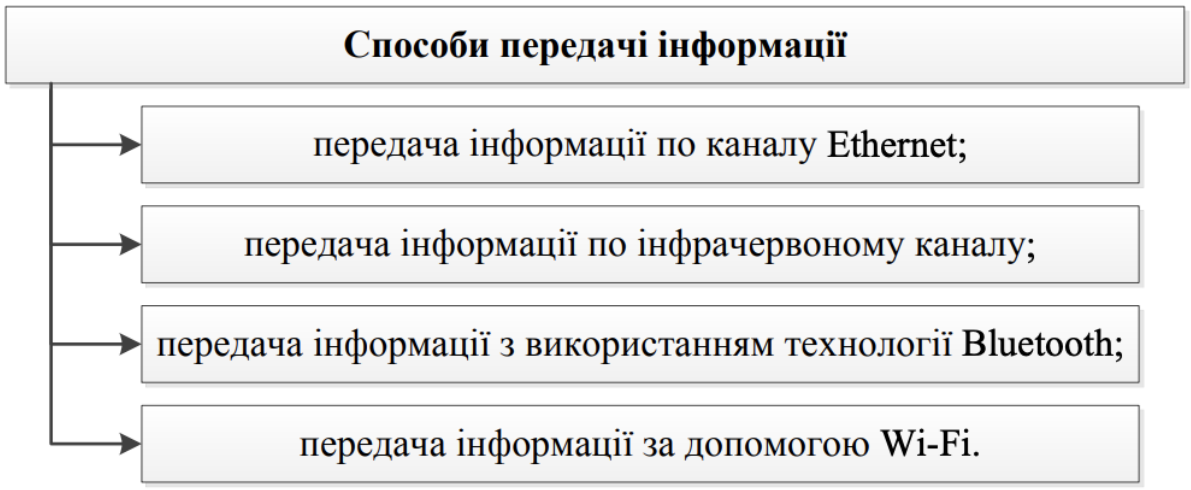


Рисунок 1.4 – Способи передачі інформації від джерела до одержувача

Ethernet [14 – 15] – це технологія пакетної передачі даних, розроблена для інформаційних електронних мереж та комп'ютерних систем. Стандарти Ethernet визначають дротяні з'єднання та електричні сигнали на фізичному рівні, формат кадру та протоколи управління доступом до інформаційного середовища на канальному рівні моделі OSI. В основному, Ethernet описується стандартами групи IEEE 802.3. Назва "Ethernet" (буквально перекладається як "Ефірна мережа" або "середовище мережі") відображає основний принцип роботи цієї технології: інформація, відправлена одним пристроєм, одночасно приймається всіма іншими.

У сучасному використанні, підключення відбувається переважно через комутатори, що дозволяє кадрам, відправленим одним вузлом, досягати лише адресата (з винятком передач на широкомовну адресу), підвищуючи тим самим швидкість та безпеку мережі. Початкові версії Ethernet використовували коаксіальний кабель як середовище передачі, але з часом його замінили оптоволокном і витою парою [16].. Це стало обумовлене тим, що коаксіальний кабель є поділюваним середовищем передачі, і його можуть використовувати одночасно кілька інтерфейсів, але тільки один може передавати інформацію в кожен момент часу. Така топологія називається "шина". Однак, при одночасній передачі інформації двома вузлами на одній шині, їх сигнали можуть накладатися один на одного, що ускладнює прийом сигналів іншими вузлами.

Передача інформації за допомогою ІЧ каналу [17 – 18] є методом передачі даних, що не вимагає провідних з'єднань для свого функціонування. Цей метод широко використовується в комп'ютерній техніці для з'єднання комп'ютерів з периферійними пристроями.

Сигнали вхідного інтерфейсу системи використовуються для модуляції сигналу у відкритому оптичному каналі. Основна технологія передачі базується на передачі даних за допомогою модульованого випромінювання в інфрачервоній частині спектра через атмосферу. Напівпровідниковий випромінюючий діод виступає як передавач, а високочутливий фотодіод використовується як приймач. Випромінювання впливає на фотодіод, регенеруючи вихідний модульований сигнал.

Далі сигнал демодулюється та перетворюється на сигнали вихідного інтерфейсу. З обох боків використовується система лінз, на передавальній стороні – для отримання колімованого променя, а на приймальній стороні – для фокусування прийнятого випромінювання на фотодіоді. Для дуплексної передачі організується такий самий зворотний канал.

Переваги цього методу передачі інформації включають відсутність потреби в проводах, нечутливість до електромагнітних завад, і відсутність потреби в ліцензуванні в інспекції електрозв'язку, відмінно від радіозв'язку.

Недоліки включають необхідність прямого видимості між приймачем і передавачем, високі витрати на приймачі та передавачі, а також обмежену швидкість передачі даних.

Передача інформації за допомогою технології Bluetooth [20 – 21] визначається як перша технологія, яка забезпечила бездротові персональні мережі передачі даних WPAN. Ця технологія дозволяє передавати дані та голосові повідомлення по радіоканалу на короткі відстані, до 100 метрів, в частотному діапазоні 2,4 ГГц, і здійснювати з'єднання між портативними пристроями навіть при відсутності прямої видимості. Технологія Bluetooth підтримує як з'єднання типу "точка-точка", так і "точка-багато точок".

У системі Bluetooth два або більше користувачів можуть використовувати один і той же канал для утворення пікомережі. Один пристрій працює в ролі сервера, а інші виступають як клієнти. У межах однієї пікомережі може бути до семи активних клієнтів, інші ж знаходяться в режимі "очікування", залишаючись синхронізованими з сервером. Такий підхід дозволяє ефективно організовувати комунікацію між різними пристроями, роблячи їх взаємодію зручною і бездротовою на невеликій відстані.

В системі Bluetooth в кожній пікомережі працює тільки один сервер, але клієнтські пристрої можуть входити в різні пікомережі. Це означає, що один сервер може взаємодіяти з різними групами клієнтів в різних мережах. До того ж, сервер, який служить в одній пікомережі, може виконувати роль клієнта в іншій пікомережі (див. рис. 1.5). Такий принцип дозволяє створювати гнучкі та ефективні комунікаційні зв'язки між різними пристроями, роблячи їх взаємодію більш універсальною та розширеною.

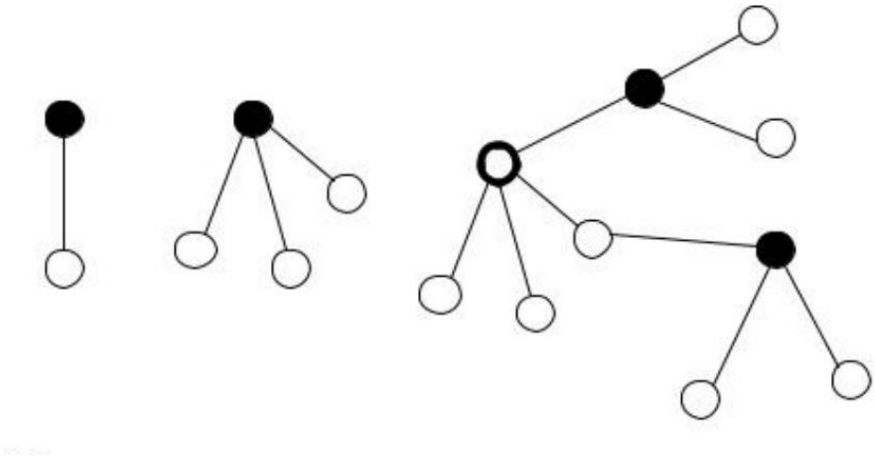


Рисунок 1.5 – Пікомережі з підлеглими пристроями: а) з одним клієнтом; б) з багатьма клієнтами; в) дворівнева мережа (за [22])

В сучасний час на ринку присутня велика кількість компаній, які пропонують модулі Bluetooth, а також компоненти для самостійної реалізації апаратної частини Bluetooth-пристроїв. Це включає виробників бездротових чіпів, антен, мікроконтролерів та інших важливих елементів, необхідних для створення різноманітних Bluetooth-продуктів. Завдяки такому різноманіттю компонентів і модулів, розробники можуть легко і швидко вбудовувати технологію Bluetooth в свої пристрої та додатки.

Це створює благоприятні умови для розширення ринку Bluetooth-рішень і сприяє розвитку різноманітних бездротових пристроїв, які використовують цю технологію для забезпечення комунікації та обміну даними на коротких відстанях.

Технологія Wi-Fi (англ. Wireless Fidelity – "бездротова точність") [23 – 24] є бездротовою технологією для передачі даних між пристроями в мережі. Зазвичай схема Wi-Fi-мережі включає не менше однієї точки доступу (режим infrastructure) та не менше одного клієнта. Також можливе підключення двох клієнтів у режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережних адаптерів безпосередньо.

Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0.1 Мбіт/с кожні 100 мс, що є

найменшою швидкістю передачі даних для Wi-Fi. При попаданні в зону дії двох точок доступу з ідентичними SSID, приймач може вибирати між ними на підставі даних про рівень сигналу. Стандарт Wi-Fi надає клієнту повну свободу при виборі критеріїв для з'єднання.

Переваги Wi-Fi включають можливість розгортання мережі без прокладання кабелю, що зменшує вартість розгортання та/або розширення мережі. В місцях, де неможливо провести кабель (наприклад, поза приміщеннями або в історичних будівлях), можна використовувати бездротові мережі. Технологія також дозволяє отримувати доступ до мережі з мобільних пристроїв.

Вибір технологій для дистанційного доступу до розроблюваної системи контролю доступу варто здійснювати, враховуючи поставлені функціональні вимоги до системи та особливості її використання. Кожна з розглянутих технологій (дистанційне відстеження, ІЧ канал, Bluetooth, Wi-Fi) має свої переваги та обмеження, і їхнє застосування може бути ефективним в різних сценаріях.

Наприклад, дистанційне відстеження може бути корисним для забезпечення безпеки та виявлення подій в приміщенні, ІЧ канал може використовуватися для безпровідного обміну даними на коротких відстанях, Bluetooth може бути зручним для створення бездротових персональних мереж, а Wi-Fi надає широкі можливості для розгортання бездротових мереж на великій площі.

Підбираючи технологію, важливо враховувати потреби та вимоги конкретного застосування, а також забезпечити сумісність інфраструктури і зручність використання для користувачів.

1.4 Моніторинг систем контролю та управління доступом

Моніторинг систем контролю та управління доступом (СКУД) - це комплекс технічних засобів, програмних рішень та процедур, спрямованих на забезпечення безпеки об'єкта чи території шляхом контролю доступу до них.

Основні компоненти системи моніторингу СКУД включають в себе:

1. Програмне забезпечення управління: Це комп'ютерні програми, які обробляють інформацію від считувачів та контролерів, встановлюють правила доступу та ведуть журнали подій. Це також може включати інтерфейс для адміністрування системи та встановлення правил.

2. Журналізація і аналіз подій: Система СКУД фіксує події, пов'язані з доступом, такі як спроби входу, виходу, помилки аутентифікації і т.д. Це важливий елемент для аналізу та виявлення незвичайної активності чи порушень безпеки.

3. Блокування і сигналізація: У разі виявлення неправомірної спроби доступу система може викликати блокування дверей, активувати сигналізацію або повідомляти відповідних служб чи адміністраторів.

4. Інтеграція з іншими системами безпеки: Система СКУД може інтегруватися з іншими системами безпеки, такими як відеоспостереження, системи виявлення вторгнень і т.д., щоб забезпечити комплексний підхід до безпеки об'єкта.

Мониторинг систем управління доступом сприяє підвищенню безпеки, шляхом ефективного контролю та відстеження руху осіб у приміщеннях або на території об'єкта. Він дозволяє оперативно реагувати на непередбачені ситуації та забезпечує можливість аналізу даних для підвищення ефективності системи.

Також розглянемо деякі аспекти систем моніторингу СКУД:

Аудит історії доступу:

- Логування подій: Моніторинг систем управління доступом забезпечує деталізований журнал подій, який містить інформацію про кожен доступ та спробу доступу.

- Аналіз історії: Системи можуть аналізувати ці логи для виявлення підозрілих дій або аномалій.

Управління рівнями доступу:

- Ієрархія доступу: Моніторинг дозволяє адміністраторам стежити за змінами рівнів доступу та ролей користувачів.

- Сповіщення про зміни: Адміністратори можуть отримувати повідомлення про будь-які зміни у рівнях доступу або правилах безпеки.

Аналіз зон доступу:

- Визначення зон: Великі приміщення можуть бути розділені на зони з різними рівнями доступу. Моніторинг дозволяє відстежувати, хто, де і коли має доступ.

- Спостереження за рухом: Використання додаткових сенсорів або камер для відстеження руху в окремих зонах.

Системи виявлення вторгнень:

- Сповіщення про вторгнення: Моніторинг може бути інтегрований з системами виявлення вторгнень для вчасного виявлення та реагування на неправомірні спроби доступу.

- Аналіз зміни стану: Системи можуть аналізувати зміни в стані приміщення для виявлення можливих загроз.

Мобільний доступ і дистанційний контроль:

- Системи мобільного доступу: Моніторинг може бути доступний через мобільні додатки, дозволяючи адміністраторам слідкувати за подіями в будь-який час і з будь-якого місця.

- Дистанційне управління: Можливість віддалено керувати параметрами системи та здійснювати негайні зміни в режимах доступу.

Автоматизація процесів:

- Розпізнавання поведінки: Моніторинг може використовувати алгоритми машинного навчання для аналізу типової поведінки користувачів та виявлення аномалій.

- Автоматизована реакція: Можливість встановлення автоматичних реакцій на певні події або спроби вторгнення.

Моніторинг систем управління доступом інтегрує ці аспекти, щоб забезпечити не лише ефективний контроль доступу, але й швидке виявлення та

реагування на потенційні загрози безпеки. Це допомагає забезпечити безпеку приміщень, захист інформації та оптимізувати управління доступом.

1.5 Існуючі аналоги сучасних замків СКУД

З урахуванням швидкого технологічного розвитку розглянемо найпоширеніші аналоги електронних замків для забезпечення доступу до об'єктів з різними системами управління [27 – 28].. Електронні замки можуть бути виготовлені у різних конструкціях, слугуючи або самостійними пристроями, або надбудовами до звичайних механічних замків [29 – 30]..

1. Замок Z-wave Dana Lock. Замок Z-wave Dana Lock підходить для більшості дверей. Працює спільно з контролером Z-wave або шлюзу Z-wave, крім них сумісний із контролерами Fibaro Home Center 2 та Home Center lite.

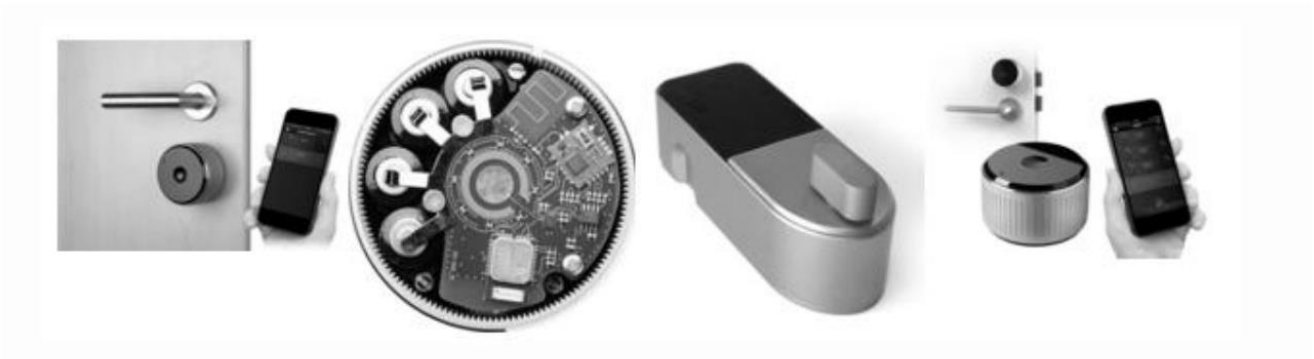


Рисунок 1.6 – Замок Z-wave Dana Lock (за [31])

Цей розумний замок від компанії Z-wave легко встановлюється, замінюючи лише серцевину старого механізму, при цьому залишаючи основний замковий механізм незмінним. Додатково до самого замка, система розумного будинку включає в себе різні пристрої, такі як загальний контролер Fibaro Home Center. Цей контролер взаємодіє з усією підключеною побутовою електронікою та датчиками.

Fibaro Home Center може бути керований як віддалено через Інтернет, так і зі смартфона, надаючи зручний та дистанційний доступ до управління системою розумного будинку. На момент написання роботи вартість цього розумного замка становить приблизно 200-250 доларів.

2. Kewo Kwikset. Kewo Kwikset [31] - це інтелектуальний замок, який автоматично розблоковує двері, якщо до них підходить особа зі смартфоном або брелоком у кишені. Цей розумний замок доступний за ціною приблизно 200 доларів на платформі Amazon. Для користування цим замком потрібно встановити спеціальну програму на смартфоні, яка працює у фоновому режимі. Для отримання доступу використовується безстроковий електронний ключ.

Рисунок 1.7 – Розумний замок Kewo Kwikset (за [31])

Зв'язок між замком та смартфоном відбувається через технологію Bluetooth. Крім того, доступ можна отримати за допомогою фірмових брелоків, які продаються окремо за 25 доларів кожен, і у комплект входить один брелок. Електронні ключі, які можуть бути перепризначені іншим людям, коштують 2 долари кожен. Є також опція придбати Kewo Plus за 99 доларів та отримати необмежену кількість електронних ключів.

Цей замок відзначається тим, що має унікальну особливість – можливість використовувати традиційні "механічні" ключі. Крім того, для свого функціонування він потребує чотирьох пальчикових батарей стандарту AA, що робить його енергоефективним. Брелок для цього замка також працює від батареї, але використовує батарею типорозміру CR2025.

Важливо відзначити, що замок забезпечує можливість використовувати як електронні, так і традиційні методи доступу. Виробник пропонує дві версії замка – одна з закругленою внутрішньою та зовнішньою частиною, а інша з квадратними.

3. Goji Smart Lock. Goji Smart Lock [33] - це інноваційний замок, який пропонує розумне рішення для заміни традиційного механічного замка. Вартість цього розумного замка оцінюється приблизно від 300 до 350 доларів. Для свого функціонування пристрій використовує чотири батареї типу AA, які, за словами виробника, вистачають на рік роботи.

Goji Smart Lock може взаємодіяти зі смартфоном через Bluetooth LE або Wi-Fi. Замок складається з двох частин: зовнішньої і внутрішньої. Зовнішня частина має круглу форму, нагадуючи шайбу, з дисплеєм і індикацією на лицьовій частині. Цей блок закриває звичайну замкову щілину і відкидається для отримання доступу. Також в зовнішній частині розташована камера, яка може надсилати фотографії тих, хто намагається відкрити двері, на смартфон власника.

Внутрішній бік замка має класичну форму і нагадує звичайний замок. Двері можна відчиняти за допомогою смартфона або спеціального Bluetooth-брелока. Ключі можна надсилати гостям на їхні смартфони з обмеженим терміном дії, і власник може скасувати або змінити параметри доступу за необхідності.

4. OkidoKeys. OkidoKeys [33] - це ще один представник розумних замків, розроблений компанією OpenWays Group. Він використовує 256-бітне AES-шифрування для забезпечення високого рівня безпеки. Цей розумний замок

сумісний із системами Android та iOS і використовує Bluetooth 4.0 для забезпечення зручного управління.

Вартість OkidoKeys залежить від моделі та комплектації і може варіюватися в межах від 180 до 350 доларів. Окрім управління зі смартфона, цей розумний замок також розпізнає RFID-мітки. Власник може налаштовувати графік доступу для кожного гостя або мітки, щоб уникнути несанкціонованого доступу в неналежний час. Мітки можуть бути вбудовані у брелоки, пластикові карти або браслети, роблячи систему більш гнучкою і зручною для користувачів.

5. Schlage Sense Smart Deadbolt. Schlage Sense Smart Deadbolt [34] - це ще один розумний замок, який пропонує передові можливості контролю доступу. Цей замок сумісний з технологією HomeKit від Apple і також інтегрується з платформою SmartThings від Samsung. Зовнішній елемент включає сенсорний екран з підсвічуванням та цифровою клавіатурою, що дозволяє зручно керувати замком.

Ціна Schlage Sense Smart Deadbolt становить приблизно 200 доларів. Завдяки підключенню Schlage Sense Wi-Fi Adapter, ви можете віддалено управляти замком через смартфон під управлінням iOS або Android, а також відчиняти двері з будь-якої точки світу через Інтернет. Крім того, ви отримуєте повідомлення про низький рівень заряду батарей.

Програмне забезпечення дозволяє вам надавати віртуальні ключі для гостей, а якщо у них немає смартфонів з цією програмою, вони можуть увійти, вводячи код доступу з клавіатури, що робить цей замок дуже зручним і функціональним.

Далі наведено порівняльну таблицю, яка висвітлить сильні та слабкі сторони цих пристроїв.

Таблиця 1.1 – Порівняльна таблиця сучасних замківа СКУД

	Z-wave Dana Lock	Kewo Kwikset	Goji Smart Lock	Okido Keys	Schlage Sense
Керування за допомогою смартфона	Так	Так	Так	Так	Так
Wi-Fi	Так	Ні	Так	Ні	Так
Bluetooth	Так	Так	Так	Так	Ні
Керування електронним ключем/картою	Ні	Так	Так	Так	Ні
Резервний канал зв’язку	Ні	Ні	Ні	Ні	Ні

1.6 Висновки та постановка задач

В цьому розділі проведено аналіз теоретичного матеріалу в обраній галузі. Були досліджені та проаналізовані персоналізуючі системи контролю доступу. Також було розглянуто можливості дистанційного моніторингу систем контролю доступу. Окрім того, проведено аналіз існуючих аналогів сучасних електронних замків, звертаючи увагу на їхні функціональні можливості та характеристики.

Після аналізу ринку систем контролю та управління доступом стало очевидним, що значна частина таких систем не мають надійного захисту від потенційного блокування основного каналу управління. Додатково, виявлено, що багато з цих систем не забезпечують ефективного сповіщення в разі несанкціонованого доступу, обходячи саму систему контролю доступу. Це може ставити під загрозу безпеку, оскільки недостатній захист та непрозорість в обробці неправомірних доступів можуть призвести до небажаних наслідків. Існує потреба у вдосконаленні та розширенні функціоналу таких систем для забезпечення високого рівня захисту та ефективного виявлення небезпек.

2 ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ВІД НСД НА ОСНОВІ ВДОСКОНАЛЕНОЇ СИСТЕМИ МОНІТОРИНГУ УПРАВЛІННЯ ДОСТУПОМ

В сучасному інформаційному середовищі, де кількість та складність кіберзагроз та несанкціонованого доступу постійно зростає, безпека інформації стає питанням вищої важливості для підприємств та організацій. Щоб забезпечити надійний захист конфіденційної інформації та уникнути можливих втрат, важливо вдосконалювати систему контролю та управління доступом, зосереджуючись на ефективному використанні резервного каналу та шифруванні даних.

У цьому розділі проводиться аналіз можливостей для впровадження резервного каналу та шифрування даних як ключових елементів стратегії забезпечення безпеки інформації. Розглядаються конкретні аспекти дублювання мережевих з'єднань, автоматичного перемикання, а також використання шифрування даних на різних рівнях системи. Цей аналіз надасть глибше розуміння можливостей впровадження та вдосконалення системи моніторингу управління доступом, спрямованого на максимізацію конфіденційності та доступності інформації.

Розділ подає конкретні рекомендації та стратегії для оптимального використання резервного каналу та шифрування даних, сприяючи створенню високопродуктивної та безпечної системи моніторингу управління доступом.

2.1 Алгоритм роботи системи контролю та управління доступом

Основний алгоритм роботи системи контролю та управління доступом (СКУД) включає в себе кілька етапів:

1. Реєстрація користувачів:

– Додавання нових користувачів до бази даних системи.

– Встановлення прав доступу для кожного користувача відповідно до його ролі чи функції.

2. Видача ідентифікаційних карток або інших засобів:

– Прив'язка ідентифікаційних засобів (карток, брелоків, біометричних даних) до кожного користувача.

– Видача цих засобів для подальшого використання при вході на об'єкт чи в окремі зони.

3. Считування інформації:

– Розміщення считувачів на точках доступу (вхідні двері, бар'єри тощо).

– Считування ідентифікаційної інформації з карточки або іншого засобу користувача.

4. Перевірка доступу:

– Перевірка ідентифікаційної інформації в системі.

– Порівняння прав доступу користувача із заданими правами для даної зони.

5. Прийняття рішення:

– На підставі результатів перевірки приймається рішення про дозвіл або відмову в доступі.

6. Виконання рішення:

– У випадку дозволу виконується відповідна дія (відкриття двері, підняття бар'єру).

– У випадку відмови відбувається відмова у доступі (звуковий або світловий сигнал, відмова від відкриття).

7. Запис подій:

– Фіксація подій у системному журналі (вхід, вихід, помилки).

– Збереження історії подій для подальшого аналізу та аудиту.

8. Адміністрування системи:

– Можливість адміністратора налаштовувати систему, додавати чи вилучати користувачів, змінювати права доступу.

Цей алгоритм може варіюватися в залежності від конкретної реалізації СКУД та вимог користувача. Далі на рисунку наведено приклад стандартної системи скуд з управлінням за допомогою смартфона з використанням Wi-Fi та Bluetooth (рис. 2.1)

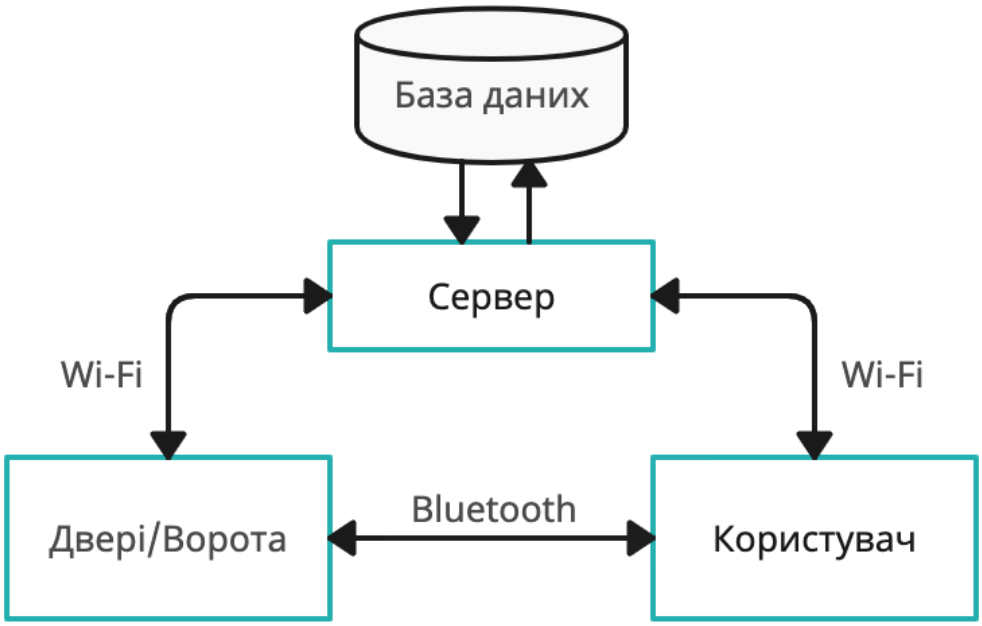


Рисунок 2.1 – Система контролю та управління доступом

2.2 Аналіз можливостей вдосконалення системи контролю та управління доступом

Враховуючи висновки попереднього розділу, для вдосконалення систем контролю та управління доступом необхідно зосередитися на таких напрямках:

– здійснити вибір елементної бази та розробку вдосконаленого алгоритму роботи системи моніторингу СКУД;

– здійснити вибір та обґрунтування додаткових (резервних) каналів зв’язку зі СКУД;

– обрати алгоритм шифрування даних у системі моніторингу управління доступом.

В контексті подальшого удосконалення системи моніторингу управління доступом, глибокий аналіз можливостей використання резервного каналу та шифрування даних виявляється ключовим для забезпечення високого рівня безпеки та ефективності інформаційної інфраструктури.

Резервний канал: Резервний канал не лише гарантує безперервність роботи системи, але і відкриває можливості для оптимізації та підвищення продуктивності. Враховуючи сучасні загрози кібербезпеки та потенційні відмови, важливо впроваджувати механізми автоматичного виявлення проблем і переключення на резервний канал без втрати ефективності. Це стає стратегічним рішенням для підвищення стійкості та забезпечення безперервності обміну даними в будь-яких умовах.

Крім того, резервний канал може слугувати не тільки як запасний шлях для уникнення відмов, але й як ресурс для оптимізації мережевого трафіку. Ефективне розподілення трафіку між різними каналами може призвести до поліпшення продуктивності та більш ефективного використання мережевих ресурсів.

Шифрування даних: Шифрування даних в системі моніторингу управління доступом відіграє критичну роль у забезпеченні безпеки інформації. Використання сучасних криптографічних алгоритмів гарантує конфіденційність даних, запобігаючи несанкціонованому доступу та перехопленню.

Шифрування не обмежується лише конфіденційністю, воно також забезпечує цілісність даних. Захист від внутрішніх та зовнішніх загроз включає в себе не лише захист від несанкціонованого доступу, але й забезпечення того, що інформація не буде змінена чи пошкоджена під час передачі.

Комплексний Підхід: Об'єднуючи резервний канал та шифрування даних, система отримує комплексний підхід до забезпечення безпеки та ефективності. Цей підхід враховує не лише можливі відмови та загрози, але й створює мережу захисту, що допомагає запобігати атакам та непередбаченим ситуаціям. Він сприяє не тільки захисту, але і оптимізації роботи системи, щоб забезпечити максимальну продуктивність та надійність.

Резервний канал та шифрування даних також можуть впливати на оптимізацію процесів управління доступом. Забезпечуючи неперервність та безпеку обміну даними, система стає менш вразливою до внутрішніх та зовнішніх викликів. Це може сприяти збільшенню ефективності внутрішніх процесів управління доступом, адже вона оперативно реагує на будь-які небезпеки та атаки, забезпечуючи безперервну роботу системи.

Застосування шифрування даних також враховує аспекти відповідності законодавству та регулятивам. Захист конфіденційної інформації через шифрування може допомогти організації виконувати вимоги щодо захисту особистих даних та забезпечити дотримання різних стандартів безпеки даних.

Враховуючи постійний розвиток кіберзагроз, важливо зазначити, що використання резервного каналу та шифрування даних - це не тільки поточні заходи безпеки, але і стратегічна інвестиція в майбутнє. Підвищення складності атак вимагає постійного вдосконалення заходів безпеки, і обрані стратегії є прогресивними рішеннями для забезпечення стійкості системи у довгостроковій перспективі.

Резервний канал та шифрування даних, як елементи вдосконалення системи моніторингу управління доступом, стають фундаментом для створення сучасної та надійної інформаційної інфраструктури. Їхнє впровадження в систему надає більше, ніж просто захист від поточних загроз – це стратегічний крок у напрямку майбутньої стійкості та ефективності.

Враховуючи результати аналізу можливостей вдосконалення системи моніторингу управління доступом, можна визначити низку вимог до розроблюваної системи моніторингу.

Вимоги до резервного каналу зв’язку:

– захищеність протоколу резервного каналу зв'язку від перешкод та спроб стороннього впливу;

– забезпечення безперебійного зв’язку із системою при виникненні проблем з основним каналом;

– максимальна швидкість автоматичного перемикання на резервний канал у випадку блокування або відмови основного;

Вимоги до шифрування даних:

– сучасний криптографічний алгоритм з максимальною довжиною ключа для забезпечення високого рівня конфіденційності;

– забезпечення безпечного та ефективного управління ключами, включаючи їхнє зберігання, обмін та оновлення, щоб запобігти витоку ключової інформації та забезпечити стабільність шифрування;

– здатність забезпечити ефективне шифрування даних без суттєвого впливу на продуктивність системи та забезпечення швидкого доступу до розшифрованих даних.

Далі на рисунку наведено приклад атаки блокуванням основного каналу на систему з запропонованими вдосконаленнями (рис. 2.2)

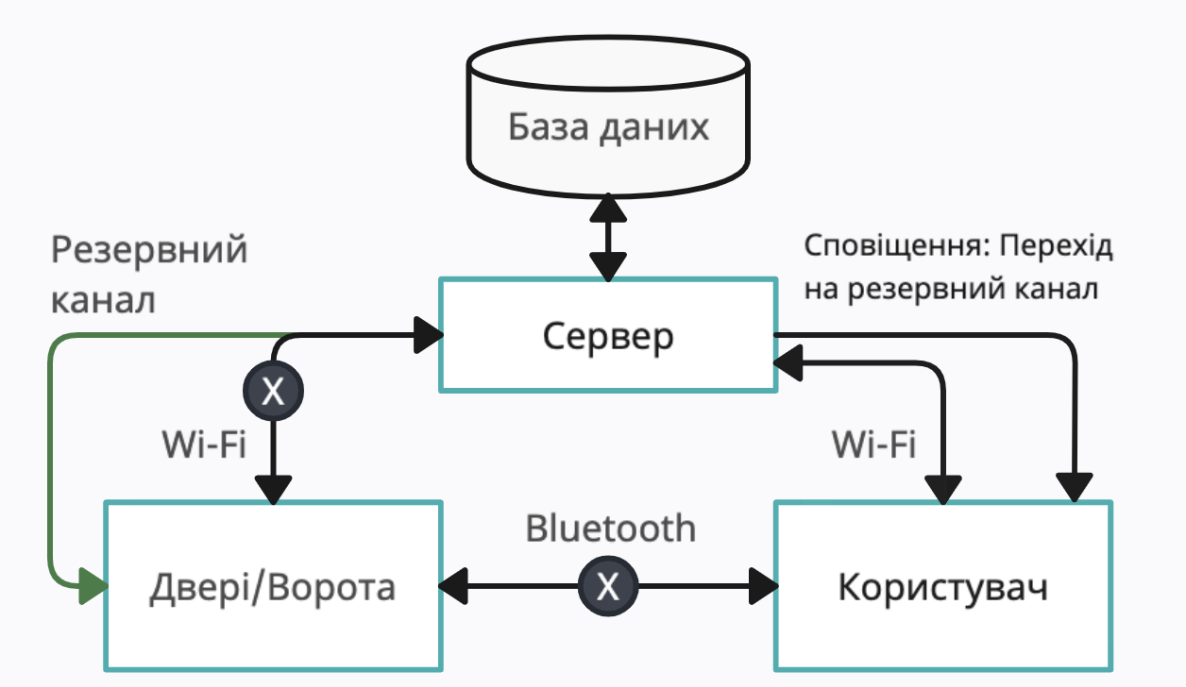


Рисунок 2.2 – Робота вдосконаленої СКУД при атаці блокуванням основних каналів зв’язку

2.3 Розробка алгоритму роботи вдосконаленої системи контролю та управління доступом

Алгоритм роботи системи контролю та управління доступом (СКУД) з резервним каналом при атаках блокуванням основних каналів зв'язку має на меті забезпечення безперебійності функціонування та виявлення подій в умовах атаки на основний комунікаційний канал. Нижче наведений загальний опис можливого алгоритму:

1. Виявлення блокування основних каналів: СКУД постійно моніторить стан основних каналів зв'язку для виявлення будь-яких аномалій, таких як зниження пропускної здатності, втрата зв'язку чи інші ознаки блокування.

2. Перехід на резервний канал: При виявленні аномалій або блокування основних каналів, система автоматично перемикається на резервний канал. Цей процес може включати автоматичне визначення доступності резервного каналу та перенастроювання зв'язку.

3. Ініціація сповіщень та аналіз ситуації: СКУД активує систему сповіщень для інформування адміністраторів та відповідальних осіб про перехід на резервний канал та можливий інцидент. Запускається аналіз ситуації для визначення причин блокування та прийняття відповідних заходів.

4. Збереження журналу інцидентів: Система веде детальний журнал інцидентів, фіксуючи час та обставини переход, у на резервний канал, а також всі виявлені аномалії чи атаки. Це допомагає в подальшому аналізі та вдосконаленні заходів безпеки.

5. Відновлення основного зв'язку: Після усунення причин блокування основних каналів або стабілізації ситуації, система повертається до основного каналу і повідомляє про це зацікавлених сторін.

Далі, схематично наведено приклад роботи вдосконаленаленої системи контролю та управління доступом із резервним каналом під час атаки блокуванням основних каналів зв’язку (рис. 2.3)

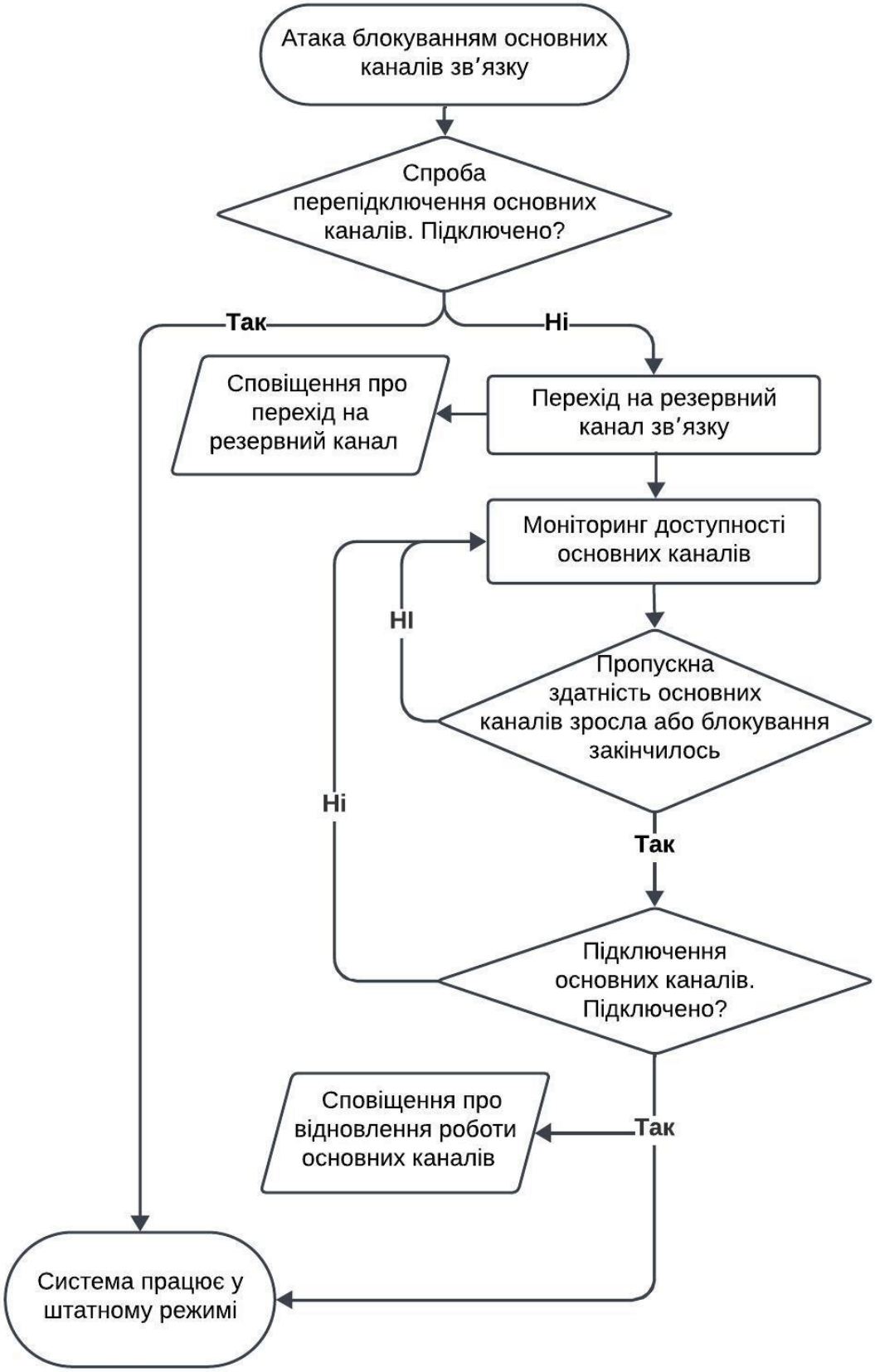


Рисунок 2.3 - Алгоритм роботи вдосконаленої системи контролю та управління доступом під час атаки блокуванням основних каналів зв’язку

Описаний алгоритм роботи системи контролю та управління доступом (СКУД) з резервним каналом при атаках блокуванням основних каналів зв'язку є докладним та збалансованим підходом до забезпечення безперебійності функціонування системи в умовах впливу атак.

Алгоритм включає етапи виявлення блокування, автоматичний перехід на резервний канал, ініціацію сповіщень та аналіз ситуації, збереження журналу інцидентів та відновлення основного зв'язку. Це дозволяє системі оперативно реагувати на аномалії та забезпечує швидке відновлення зв'язку під час атак.

Важливим елементом є ініціація системи сповіщень та аналіз ситуації, що дозволяє оперативно реагувати та інформувати відповідальних осіб. Збереження детального журналу інцидентів сприяє подальшому вдосконаленню системи та вивченню патернів атак.

Загалом, алгоритм є ефективним заходом для забезпечення стійкості та надійності системи контролю та управління доступом під час атак на основні комунікаційні канали.

2.4 Вибір технологій резервного каналу для вдосконалення системи контролю та управління доступом

Зважаючи на те, що багато систем контролю та управління доступом використовують технології Bluetooth та Wi-Fi для основного зв'язку, розглянемо можливість впровадження альтернативного каналу для резервного зв'язку.

Оптимальною стратегією може стати використання технології, яка відрізняється від Bluetooth та Wi-Fi, щоб уникнути можливих конфліктів та перешкод. Це дозволить підвищити надійність системи та забезпечити ефективний резервний зв'язок в ситуаціях, коли основні канали недоступні або не спроможні забезпечити потрібний рівень зв'язку.

Розглянемо такі альтернативні канали зв’язку:

Ethernet. Інтеграція Ethernet як резервного каналу може підвищити надійність системи управління доступом, забезпечуючи ефективний зв'язок у ситуаціях, коли бездротові основні канали недоступні або не можуть забезпечити необхідний рівень зв'язку. Це може стати додатковим заходом для забезпечення стійкості системи у випадку непередбачених обставин.

Переваги використання Ethernet у резервному зв'язку включають в себе стабільність та надійність зв'язку, особливо в умовах, де бездротові технології можуть стикатися з електромагнітними перешкодами або перевантаженням мережі. Крім того, провідне підключення може бути менш вразливим до втрати сигналу чи інтерференції, що може стати критичним у вимогливих до безпеки системах.

Імплементація Ethernet як альтернативи може підвищити надійність та ефективність систем контролю доступу в тих випадках, коли безперебійний зв'язок є пріоритетом. Однак важливо також враховувати особливості конкретної інфраструктури та вимоги системи для досягнення оптимального результату.

Додатково, інтеграція Ethernet як альтернативного каналу для резервного зв'язку може сприяти забезпеченню ефективної комунікації у випадку відмови або недоступності бездротових мереж. Це особливо важливо в сферах, де забезпечення неперервності роботи систем контролю та управління доступом має критичне значення, таких як об'єкти з високим рівнем безпеки або інфраструктура критично важливих об'єктів.

Ethernet може бути також більш простим у налаштуванні та управлінні порівняно із складнішими бездротовими конфігураціями. Це може спростити процес обслуговування та знизити ймовірність помилок у системі.

Наприкінці, обрання Ethernet як альтернативного каналу для резервного зв'язку вимагає виваженості між передовими технологіями та конкретними потребами системи. Такий підхід може підсилити стійкість та ефективність

систем контролю доступу, роблячи їх менш вразливими до можливих випадків втрати зв'язку чи перешкод.

GSM. Зв'язковий стандарт GSM (Global System for Mobile Communications) є міжнародним стандартом для мобільного зв'язку. Виникнення GSM стало ключовим етапом у розвитку бездротового зв'язку, і його впровадження сприяло широкому поширенню мобільних телефонів.

GSM використовує цифровий спосіб передачі даних із використанням комутації каналів, що дозволяє обробляти одночасні дзвінки та передачу даних. Основні характеристики GSM включають частотний спектр в радіодіапазоні, призначений для передачі інформації, та алгоритми шифрування для забезпечення конфіденційності даних.

Застосування GSM включає мобільний телефонний зв'язок, передачу коротких текстових повідомлень (SMS), передачу даних (GPRS, EDGE), інтернет-з'єднання через мобільний зв'язок (3G, 4G, тощо).

У GSM використовується шифрування для захисту конфіденційності та безпеки передачі даних. Основним алгоритмом шифрування в GSM є A5 (A5/1, A5/2, A5/3), який застосовується для зашифрування голосового та SMS-трафіку.

Основні характеристики шифрування в GSM:

– A5/1 (и A5/3): A5/1 є оригінальним алгоритмом шифрування в GSM, і використовується для голосового трафіку. Однак внаслідок виявлення деяких слабкостей, був створений алгоритм A5/3 (також відомий як Касумі), який є більш безпечним і застосовується для зашифрування данних передачі.

– A5/2: A5/2 був розроблений як альтернатива A5/1 з метою забезпечення меншого рівня захисту і використовується, коли клієнт не підтримує A5/1. Однак A5/2 також має слабкості у відносині безпеки.

– Ключі шифрування: В GSM використовуються ключі для ініціалізації алгоритмів шифрування. Ці ключі включають Kc (ключ шифрування для голосового трафіку) і KcGPRS (ключ для шифрування даних передачі).

– Частота зміни ключів: У GSM ключі шифрування періодично змінюються для забезпечення додаткового рівня безпеки. Кожен кадр голосового трафіку може мати свій власний ключ шифрування.

Шифрування у GSM призначене для ускладнення можливостей прослуховування інформації і підвищення конфіденційності користувачів мобільних мереж. Однак, слід враховувати, що існують методи і атаки, спрямовані на алгоритми шифрування, тому безпека системи завжди вимагає уважного стеження за останніми технологічними розробками та оновленнями.

Тепер, щодо розгляду GSM як альтернативного каналу зв'язку в системах контролю та управління доступом, варто зазначити, що можливість використання GSM для цілей забезпечення резервного зв'язку полягає у його бездротовій природі та гнучкості. GSM може слугувати як ефективний резервний канал у випадку відмови інших засобів зв'язку, таких як Ethernet, Wi-Fi або Bluetooth.

Використання GSM для резервного зв'язку може бути особливо корисним у сценаріях, де мобільність та швидкість відновлення зв'язку є важливими факторами. Це дозволяє системам контролю та управління доступом підтримувати стійку роботу навіть у випадку виникнення проблем з основними каналами зв'язку.

В підсумку, GSM є міжнародним стандартом мобільного зв'язку, який використовує цифровий підхід для передачі даних через бездротові мережі. У контексті систем контролю та управління доступом, використання GSM як альтернативного каналу зв'язку може бути важливим стратегічним рішенням. Його бездротова природа, гнучкість та глобальне покриття роблять його ефективним в резервному зв'язку, особливо в сценаріях, де мобільність та швидкість відновлення зв'язку є пріоритетними. Однак важливо враховувати можливі обмеження в зоні покриття та витрати на мобільний зв'язок. Рішення використання GSM повинно бути прийняте на основі конкретних вимог та умов використання системи.

У виборі між GSM (мобільний зв'язок) та Ethernet (провідний зв'язок) для системи контролю доступу, GSM виявляється перевагою у ряді важливих аспектів.

GSM має вагому перевагу в плані мобільності та гнучкості. Завдяки технології мобільного зв'язку, вона забезпечує доступність в будь-якому місці з наявністю мобільного покриття. Це особливо важливо для об'єктів, що розташовані в різних локаціях або в ситуаціях, де проведення кабельної інфраструктури є витратним або неефективним.

Додатково, GSM дозволяє економити витрати на провідні комунікації та полегшує розгортання системи, оскільки не вимагає складних інженерних робіт для прокладання кабелів. Це робить його ефективним рішенням в умовах, де важко або неможливо встановити провідний зв'язок.

Крім того, GSM дозволяє оперативно розширювати мережу та додає нові об'єкти без необхідності додаткового провідного підключення.

Отже, у випадках, коли важливі мобільність, гнучкість та вартість розгортання, GSM виходить на передній план як ефективне та практичне рішення для систем контролю доступу.

2.5 Вибір алгоритму шифрування даних для підвищення захищеності системи контролю та управління доступом

Шифрування даних є критичним аспектом в розробці системи моніторингу управління доступом для підвищення захищеності від несанкціонованого доступу. Розглянемо декілька сучасних алгоритмів шифрування, вивчаючи їх особливості та переваги для забезпечення ефективного захисту інформації.

Rivest–Shamir–Adleman (RSA)

RSA [40] є асиметричним алгоритмом шифрування, винайденим в 1977 році. Він базується на складності факторизації великих простих чисел та використовує два ключі: публічний та приватний.

Основні характеристики:

– Розмір ключа: Зазвичай використовуються ключі довжиною в 1024, 2048, або навіть 4096 біт.

– Тип шифрування: Асиметричний, де ключ для шифрування відрізняється від ключа для розшифрування.

– Застосування: Зазвичай використовується для шифрування малих об'ємів даних або передачі ключів симетричних алгоритмів.

Переваги:

– Безпека ключа: Відповідно до теорії чисел, що робить його стійким до криптографічних атак.

– Цифровий підпис: Використовується для створення цифрових підписів для перевірки автентичності даних.

Недоліки:

– Обчислювальна складність для великих ключів: Використання ключів великої довжини може призвести до значного збільшення часу, необхідного для шифрування та розшифрування.

–Обмеженість об'єму даних: Ефективність RSA зменшується при шифруванні великих об'ємів даних через обчислювальну складність.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) [41] є асиметричним методом шифрування, використовуючи властивості еліптичних кривих для створення ключів та зашифровування даних.

Основні характеристики:

– Розмір ключа: Забезпечує високий рівень безпеки при коротших ключах порівняно з іншими асиметричними алгоритмами.

– Швидкодія: Ефективний у використанні ресурсів та підходить для обміну даними в обмежених системах.

Переваги:

– Мінімальні обчислювальні вимоги: Забезпечує високий рівень безпеки при ефективному використанні ресурсів.

– Широке застосування: Використовується в різних областях, включаючи електронні платежі та безпеку мережі.

Недоліки:

– Залежність від параметрів кривої: Ефективність ECC може залежати від правильного вибору параметрів еліптичної кривої. Невірно вибрані параметри можуть вплинути на безпеку.

– Можливість атаки на квантових комп'ютерах: Деякі експерти вказують на те, що ECC може бути менш стійким до атак з використанням квантових комп'ютерів порівняно з іншими алгоритмами.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) [38-39] є сучасним симетричним алгоритмом шифрування, розробленим заміною застарілого DES (Data Encryption Standard). Вперше стандартизований у 2001 році, AES став широко використовуваним для захисту конфіденційної інформації.

Основні характеристики:

– Розмір ключа: AES підтримує ключі розміром 128, 192 та 256 біт.

– Тип шифрування: Симетричний. Однак, його ефективність узагальнюється через використання різних ключів для шифрування та розшифрування.

– Швидкодія: AES славиться своєю високою швидкодією та низькими вимогами до обчислювальних ресурсів.

Переваги:

– Надійність: AES забезпечує надійний захист від різноманітних криптографічних атак та є відомим своєю стійкістю.

– Широке використання: Являючись стандартом у багатьох галузях, AES є добре вивченим і широко використовується для шифрування даних.

– Швидкодійність: AES забезпечує високу швидкодію при шифруванні та розшифруванні, що робить його ефективним для застосувань в реальному часі.

Недоліки:

– Симетричний характер: Як симетричний алгоритм, один ключ використовується для шифрування і розшифрування. Пошкодження чи втрата ключа може призвести до неправомірного доступу до даних.

Таблиця 2.1 – Порівняльна таблиця запропонованих алгоритмів шифрування даних

Характеристика	RSA	ECC	AES
Тип алгоритму	Асиметричний шифр	Асиметричний шифр	Симетричний шифр
Застосування	Зашифрування та підпис електронних даних, обмін ключами	Зашифрування, підпис, обмін ключами	Зашифрування повідомлень, дані в спеціальних режимах
Довжина ключа	Зазвичай 1024, 2048, 3072 біт та більше	Зазвичай 256, 384, 521 біт	128, 192, 256 біт
Ефективність ключа	Зменшується зі збільшенням довжини ключа	Висока ефективність при коротших ключах	Забезпечує високий рівень ефективності для невеликих ключів
Обчислювальна складність	Велика, особливо для довших ключів	Низька порівняно з RSA	Залежить від конкретного режиму шифрування та довжини ключа
Використання ресурсів	Велика кількість ресурсів для шифрування та розшифрування	Вимагає менше ресурсів порівняно з RSA	Вимагає менше ресурсів порівняно з асиметричними шифрами

Підходи до ключового обміну	Використовується для безпечного обміну сесійним ключем	Зазвичай використовуєтьс я для безпечного обміну сесійним ключем	Використовуєтьс я для симетричного обміну ключами через інші алгоритми (наприклад, RSA)
Підтримка апаратного прискорення	Можлива, але менше поширена	Можлива	Широко підтримується апаратними пристроями

Проаналізувавши попередні дані, для системи моніторингу управління доступом обираємо Advanced Encryption Standard (AES). Цей вибір обумовлений декількома ключовими факторами:

1. Симетричний алгоритм: AES є симетричним алгоритмом, що означає, що один і той же ключ використовується для шифрування та розшифрування даних. Це дозволяє забезпечити високий рівень ефективності та швидкодії.

2. Широкий розмах довжин ключа: AES підтримує різні довжини ключа, включаючи 128, 192 та 256 біт, що дозволяє вибрати рівень безпеки в залежності від конкретних потреб та загроз.

3. Безпека: AES був обраний Національним Інститутом Стандартів та Технологій (NIST) після вивчення різноманітних кандидатів. Його безпека базується на математичних властивостях, таких як складність алгоритмів зламу.

4. Стійкість до криптоаналізу: AES володіє високою стійкістю до різноманітних видів криптоаналізу, включаючи атаки на основі лінійного та диференціального криптоаналізу.

5. Широка підтримка в апаратурі та програмному забезпеченні: AES отримав широку підтримку в апаратних засобах та програмному забезпеченні, що дозволяє ефективно використовувати його в різних екосистемах.

6. Ефективність на сучасних платформах: Існує ефективне апаратне прискорення для AES на багатьох платформах, що робить його ідеальним для використання в різних пристроях та системах.

З урахуванням цих факторів AES стає переважаючим вибором для багатьох застосувань, особливо коли необхідно забезпечити ефективне та безпечне симетричне шифрування.

2.6 Вибір елементної бази апаратної частини системи

Основуючись на проведеному аналізі різних варіантів для забезпечення резервного зв'язку з системою контролю та управління доступом (СКУД), було вирішено використовувати GSM зв'язок як резервний канал зв'язку. Розглянемо тепер можливий спосіб реалізації цієї технології з точки зору апаратного забезпечення.

З метою забезпечення стійкості та надійності СКУД у випадку відмови основного каналу зв'язку, використання GSM з'єднання є стратегічно важливим рішенням. Для цього потрібно розглянути апаратну реалізацію, яка дозволить ефективно використовувати GSM технологію як резервний канал.

На першому етапі оберемо адаптивний GSM модем, який може працювати в режимі очікування, але активується автоматично в разі втрати основного зв'язку. Такий модем має вбудовані механізми моніторингу та автоматичного переключення, що забезпечить швидке відновлення зв'язку у разі потреби.

Для забезпечення безпеки передачі даних через GSM з'єднання, рекомендується використовувати шифрування трафіку. Це може бути досягнуто за допомогою використання протоколів шифрування, таких як SSL або IPSec, залежно від вимог конкретного застосування.

Також для забезпечення автономності системи у випадку відмови основного джерела енергії, слід врахувати можливість використання альтернативного джерела живлення, такого як батарея або акумулятор.

Важливим етапом є налаштування системи автоматичного моніторингу та виявлення відмов, яка буде вчасно реагувати на втрату основного каналу та автоматично активувати GSM з'єднання.

Таким чином, апаратна реалізація резервного GSM зв'язку для СКУД передбачає вибір відповідного модему, застосування шифрування для забезпечення безпеки, використання альтернативного джерела енергії та налаштування системи моніторингу та реакції на відмови.

Далі наведено таблицю з вибіркою модемів представлених на ринку та порівняння їх характеристик.

Таблиця 2.2 GSM модеми та їх характеристики

Модем \ Параметр	Швидкість передачі даних	Роз'єми	Підтримка стандартів	Вибір версій
Quectel UC20-G	Завантаження: до 5.76 Mbps Вивантаження: до 7.2 Mbps	USB, UART	GSM, GPRS, EDGE	Обмежений
SIMCom SIM7100E	Завантаження: до 100 Mbps Вивантаження: до 50 Mbps	USB, UART	GSM, GPRS, EDGE, WCDMA, HSPA+, LTE	Обширний
Telit LE910	Завантаження: до 10 Mbps Вивантаження: до 5.76 Mbps	USB, UART	GSM, GPRS, EDGE, WCDMA, HSPA+, LTE	Обширний
Huawei MS2131	Завантаження: до 21 Mbps Вивантаження: до 5.76 Mbps	USB, UART	GSM, GPRS, EDGE, WCDMA	Обмежений
U-blox SARA-U201	Завантаження: до 7.2 Mbps Вивантаження: до 5.76 Mbps	USB, UART	GSM, GPRS, EDGE	Обмежений

Quectel EC25	Завантаження: до 150 Mbps Вивантаження: до 50 Mbps	USB, UART	GSM, GPRS, EDGE, WCDMA, HSPA+, LTE	Обширний

Одним із потенційно підходящих модемів для резервного GSM зв'язку в системі контролю та управління доступом може бути Quectel EC25 [41] (рис. 2.4).

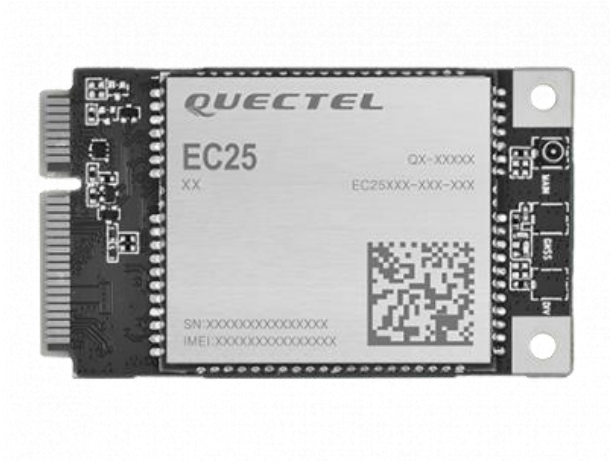


Рисунок 2.4 - GSM-модем Quectel EC25

Вибір цього модему може бути обгрунтований кількома факторами:

– Широкий спектр підтримуваних мереж: Quectel EC25 підтримує роботу в різних типах мереж, включаючи GSM, WCDMA, LTE, що дозволяє використовувати його в різних географічних областях і умовах зв'язку.

– Автоматичне переключення мереж: Модем Quectel EC25 має вбудовані функції автоматичного переключення між різними мережами, що є важливим аспектом для забезпечення сталого зв'язку. Це робить його ефективним варіантом для резервного каналу, оскільки він може швидко адаптуватися до змін у зовнішніх умовах.

– Низьке споживання енергії: Модеми Quectel відомі своєю оптимізацією енергоспоживання, що важливо для систем, які можуть працювати в режимі очікування протягом тривалого часу. Це особливо актуально для резервного GSM зв'язку, де модем повинен бути готовий до використання у разі потреби.

– Висока швидкість передачі даних: Quectel EC25 підтримує високу швидкість передачі даних в мережах LTE, що може бути важливим для ефективного використання зв'язку, особливо в умовах, де швидкість передачі даних грає ключову роль.

Далі у таблиці наведемо ключові характерні особисті застосовуваного модему.

Таблиця 2.3 – Повні технічні характеристики модему Quectel EC25

Мережева підтримка	GSM/GPRS/EDGE: 850/900/1800/1900 МГц WCDMA: B1/B2/B5/B8 LTE FDD: B1/B3/B7/B8/B20 LTE TDD: B38/B40/B41
Швидкість передачі даних	LTE Cat 4 (до 150 Мбіт/с вниз, до 50 Мбіт/с вгору) HSPA+ (до 42 Мбіт/с вниз, до 5.76 Мбіт/с вгору)
Інтерфейси	USB 2.0 High-Speed UART, I2C, GPIO, PCM, etc.
Підтримка GNSS:	GPS, GLONASS, BeiDou, Galileo
SIM-карта	1.8V/3V
Робоча температура	Від -40°C до +85°C
Розміри	32 мм × 29 мм × 2.4 мм
Підтримка ОС	Windows 7/8/8.1/10, Linux, Android, eCall
Живлення	Вхідна напруга: 3.4V - 4.2V Режим сну: менше 10 мкА
Інші особливості	Вбудований TCP/IP stack Режим віддаленого відладки Підтримка AT-команд

Враховуючи ці фактори, модем Quectel EC25 може бути розглянутий як оптимальний вибір для апаратної реалізації резервного GSM зв'язку в системі контролю та управління доступом.

2.7 Висновки до розділу

У процесі вивчення та аналізу заходів щодо підвищення захищеності системи моніторингу управління доступом від несанкціонованого доступу (НСД), було прийнято стратегічне рішення щодо використання резервного каналу GSM та алгоритму шифрування Advanced Encryption Standard (AES).

Обране рішення базується на добре встановлених принципах безпеки та сучасних підходах до захисту інформації. Використання резервного каналу GSM дозволяє забезпечити надійний зв'язок у випадку відмови основного каналу, забезпечуючи неперервну функціональність системи.

Щодо алгоритму шифрування, обрання Advanced Encryption Standard (AES) є обґрунтованим вибором. AES надає високий рівень безпеки та швидкодії, властивості, які є критичними для системи моніторингу управління доступом. Його широке використання в різних сферах свідчить про визнану ефективність та надійність.

Загалом, обрана комбінація резервного каналу GSM та алгоритму шифрування AES визначає найкращі практики в області захисту інформації та допоможе ефективно протистояти потенційним загрозам несанкціонованого доступу.

3 РОЗРОБКА ВДОСКОНАЛЕНОЇ СИСТЕМИ МОНІТОРИНГУ УПРАВЛІННЯ ДОСТУПОМ

Цей розділ присвячений розробці вдосконаленої системи моніторингу, яка базується на попередньо розробленій системі контролю та управління доступом (СКУД) на основі плати з чипом ESP32. Подальша розробка дозволить нам створити сучасну та ефективну систему моніторингу, яка відповідає сучасним вимогам безпеки та управління доступом.

Короткий опис попередньо розробленої системи:

– Це універсальний модуль розроблений на основі плати з чипом ESP32 [35-37], який встановлюється на електронні замки, автоматичні ворота та шлагбауми;

– Керування відбувається за допомогою додатку на смартфоні через Bluetooth та Wi-Fi канали;

– За обробку всієї інформації системи відповідає віддалений сервер, який також виконує роль системи моніторингу;

3.1 Інтеграція апаратної частини резервного каналу у СКУД для вдосконалення системи

Виходячи з того, що за основу розробки було взято попередньо розроблену СКУД, апаратна частина якої базується на платі з чипом ESP32, будемо інтегрувати наш GSM модуль безпосередньо у цю плату.

В ході інтеграції важливо визначити та реалізувати оптимальний спосіб взаємодії між ESP32 та GSM модулем, використовуючи наявні інтерфейси, такі як UART або SPI. Налаштування обміну даними має відбуватися з врахуванням специфіки системи моніторингу та вимог щодо передачі інформації через GSM мережу.

Важливим етапом є інтеграція з вже існуючим програмним забезпеченням системи моніторингу. Використання AT-команд для ефективного управління

GSM модулем дозволить реалізувати необхідні функції зв'язку та забезпечити сумісність з існуючими модулями системи моніторингу.

Далі ми ретельно розглянемо процес фізичного з'єднання модуля Quectel EC25 з платою ESP32 через інтерфейс UART. Цей етап є ключовим для успішної інтеграції, спрямованої на підвищення стійкості та надійності резервного каналу у системі моніторингу управління доступом.

Визначення Пінів:

– TX (Transmit) Quectel EC25 -> RX (Receive) ESP32: Важливо зазначити, що вивід передачі (TX) модуля Quectel EC25 повинен бути з'єднаний із виводом прийому (RX) на ESP32. Це забезпечить передачу даних від модуля Quectel EC25 до ESP32;

– RX (Receive) Quectel EC25 -> TX (Transmit) ESP32: З'єднаємо вивід прийому (RX) Quectel EC25 із виводом передачі (TX) ESP32. Ця конфігурація дозволить ESP32 приймати дані від модуля;

– Нульовий Потенціал (GND): Проведемо з'єднання земельних виводів (GND) Quectel EC25 та ESP32. Це необхідно для створення спільного потенціалу землі;

– Живлення (VCC): Підключимо вивід живлення (VCC) Quectel EC25 до відповідного виводу живлення на ESP32. Врахуємо, що напруга живлення повинна відповідати вимогам Quectel EC25;

Після проведення з'єднань обов'язково перевіримо правильність та надійність фіксації з'єднань, відповідно до схеми підключення, наведеної в документації Quectel EC25 та ESP32.

Далі наведено приклад інтеграції GSM модуля Quectel EC25 в плату з чипом ESP32 (рис. 3.1 та рис 3.2)

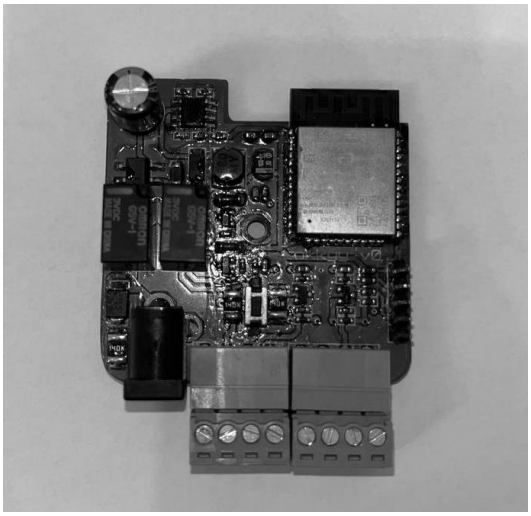


Рисунок 3.1 - Попередньо розроблений модуль з чипом ESP32 без GSM модема

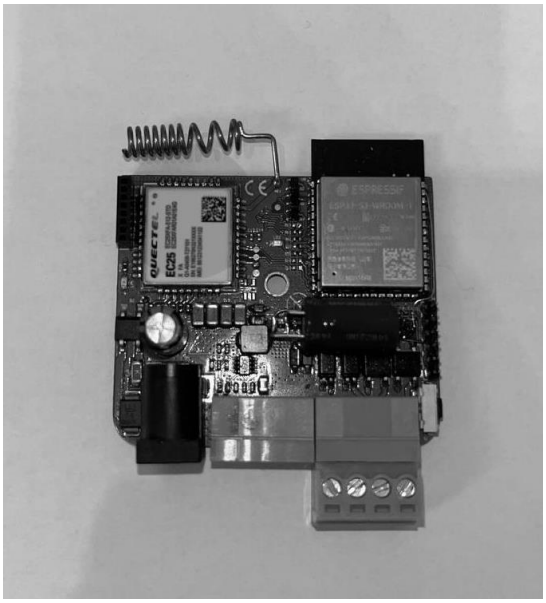


Рисунок 3.2 - Результат інтеграції GSM модема Quectel EC25 в модуль з чипом ESP32

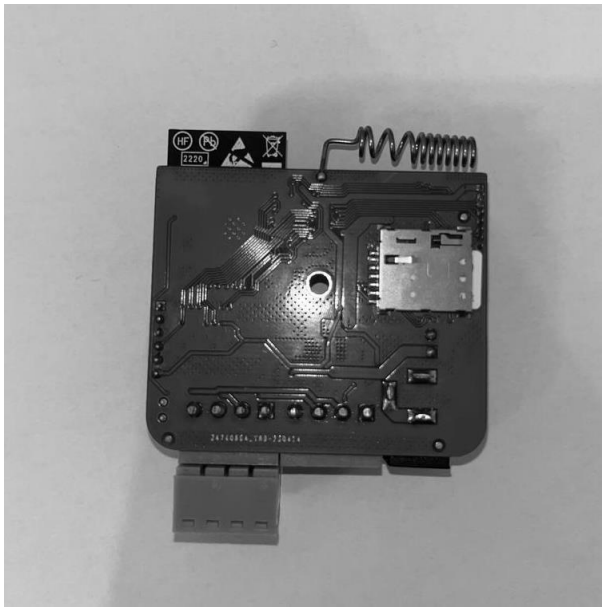


Рисунок 3.3 – Результат інтеграції роз’єму SIM-карти для GSM модема Quectel EC25 в модуль з чипом ESP32

Також, під час інтеграції GSM модуля було додано антену для покращення якості з’єднання. Під час впаювання антени на плату ESP32 важливо дотримуватися ретельного підходу для забезпечення надійного та ефективного з'єднання.

В процесі цього етапу фізичної інтеграції враховуються такі аспекти:

– Визначення оптимального розташування: Перед початком впаювання важливо визначити оптимальне місце для антени на платі ESP32. Це враховує електромагнітні властивості та потреби конкретного проекту. Позначення та

– Підготовка контактів: Відмітьте на платі виводи, які будуть використовуватися для підключення антени. Важливо грамотно розташувати ці виводи та забезпечити відповідність їхніх функцій.

– Впаювання з використанням техніки паяння: Використовуйте відповідні інструменти та техніку паяння для з'єднання контактів антени з відповідними виводами на платі ESP32. Дотримуйтеся рекомендацій щодо температури та тривалості паяння.

– Виконання Тестування: Після впаювання проведіть тестування, щоб переконатися в якісному з'єднанні та відсутності коротких замикань. Забезпечте стабільність та ефективність з'єднання антени.

Грамотне впаювання антени на плату ESP32 є важливим етапом фізичної інтеграції, що визначає якість бездротового з'єднання та надійність системи.

Далі буде розглянуто розробку програмної частини резервного каналу.

3.2 Розробка програмної частини резервного каналу вдосконаленої системи

Виходячи з особливостей розроблюваної системи моніторингу управління доступом, було обрано здійснити розробку мікропрограми для мікроконтролера ESP32 та GSM модема Quectel EC25 у середовищі ESP IDF.

Далі розглянемо ключові елементи програмування апаратного пристрою для розроблюваної системи контролю доступом:

Ініціалізація GSM модема:

```
void pppos_client_init(void)
{
        config_pwrkey_gpio();
        power_on_modem();

    /* Ініціалізація системних компонентів */
    ESP_ERROR_CHECK(esp_event_handler_register(IP_EVENT,
ESP_EVENT_ANY_ID, &on_ip_event, NULL));
    ESP_ERROR_CHECK(esp_event_handler_register(NETIF_PPP_STATUS,
ESP_EVENT_ANY_ID, &on_ppp_changed, NULL));

    /* Конфігурація PPP (Point-to-Point Protocol) протоколу */
    esp_modem_dce_config_t dce_config =
ESP_MODEM_DCE_DEFAULT_CONFIG(CONFIG_EXAMPLE_MODEM_PPP_APN);
    esp_netif_config_t netif_ppp_config = ESP_NETIF_DEFAULT_PPP();
    esp_netif_t *esp_netif = esp_netif_new(&netif_ppp_config);
    assert(esp_netif);
```

```
        event_group = xEventGroupCreate();

        /* Конфігурація терміналу для виведення даних */
    #if defined(CONFIG_EXAMPLE_SERIAL_CONFIG_UART)
        esp_modem_dte_config_t dte_config = ESP_MODEM_DTE_DEFAULT_CONFIG();
        /* setup UART specific configuration based on kconfig options */
        dte_config.uart_config.tx_io_num = CONFIG_EXAMPLE_MODEM_UART_TX_PIN;
        dte_config.uart_config.rx_io_num =
CONFIG_EXAMPLE_MODEM_UART_RX_PIN;
        dte_config.uart_config.rts_io_num =
CONFIG_EXAMPLE_MODEM_UART_RTS_PIN;
        dte_config.uart_config.cts_io_num =
CONFIG_EXAMPLE_MODEM_UART_CTS_PIN;
        dte_config.uart_config.flow_control = EXAMPLE_FLOW_CONTROL;
        dte_config.uart_config.rx_buffer_size =
CONFIG_EXAMPLE_MODEM_UART_RX_BUFFER_SIZE;
        dte_config.uart_config.tx_buffer_size =
CONFIG_EXAMPLE_MODEM_UART_TX_BUFFER_SIZE;
        dte_config.uart_config.event_queue_size =
CONFIG_EXAMPLE_MODEM_UART_EVENT_QUEUE_SIZE;
        dte_config.task_stack_size =
CONFIG_EXAMPLE_MODEM_UART_EVENT_TASK_STACK_SIZE;
        dte_config.task_priority =
CONFIG_EXAMPLE_MODEM_UART_EVENT_TASK_PRIORITY;
        dte_config.dte_buffer_size =
CONFIG_EXAMPLE_MODEM_UART_RX_BUFFER_SIZE / 2;

    #if CONFIG_EXAMPLE_MODEM_DEVICE_BG96 == 1
        ESP_LOGI(TAG, "Initializing esp_modem for the BG96 module...");
        esp_modem_dce_t *dce = esp_modem_new_dev(ESP_MODEM_DCE_BG96,
&dte_config, &dce_config, esp_netif);
    #elif CONFIG_EXAMPLE_MODEM_DEVICE_SIM800 == 1
        ESP_LOGI(TAG, "Initializing esp_modem for the SIM800 module...");
        esp_modem_dce_t *dce = esp_modem_new_dev(ESP_MODEM_DCE_SIM800,
&dte_config, &dce_config, esp_netif);
    #elif CONFIG_EXAMPLE_MODEM_DEVICE_SIM7000 == 1
        ESP_LOGI(TAG, "Initializing esp_modem for the SIM7000 module...");
        esp_modem_dce_t *dce = esp_modem_new_dev(ESP_MODEM_DCE_SIM7000,
&dte_config, &dce_config, esp_netif);
    #elif CONFIG_EXAMPLE_MODEM_DEVICE_SIM7070 == 1
        ESP_LOGI(TAG, "Initializing esp_modem for the SIM7070 module...");
        esp_modem_dce_t *dce = esp_modem_new_dev(ESP_MODEM_DCE_SIM7070,
&dte_config, &dce_config, esp_netif);
    #elif CONFIG_EXAMPLE_MODEM_DEVICE_SIM7600 == 1
        ESP_LOGI(TAG, "Initializing esp_modem for the A7682E module...");
```

```
            /*esp_modem_dce_t **/dce =
esp_modem_new_dev(ESP_MODEM_DCE_SIM7600, &dte_config, &dce_config, esp_netif);
        #else
            ESP_LOGI(TAG, "Initializing esp_modem for a generic module...");
            esp_modem_dce_t *dce = esp_modem_new(&dte_config, &dce_config, esp_netif);
        #endif
            assert(dce);
            if (dte_config.uart_config.flow_control == ESP_MODEM_FLOW_CONTROL_HW) {
                esp_err_t err = esp_modem_set_flow_control(dce, 2, 2);  //2/2 means HW Flow
Control.
                if (err != ESP_OK) {
                    ESP_LOGE(TAG, "Failed to set the set_flow_control mode");
                    goto dte_cleanup;
                }
                ESP_LOGI(TAG, "HW set_flow_control OK");
            }

        #elif defined(CONFIG_EXAMPLE_SERIAL_CONFIG_USB)
            while (1) {
        #if CONFIG_EXAMPLE_MODEM_DEVICE_BG96 == 1
                ESP_LOGI(TAG, "Initializing esp_modem for the BG96 module...");
                struct esp_modem_usb_term_config usb_config =
ESP_MODEM_BG96_USB_CONFIG();
                esp_modem_dce_device_t usb_dev_type = ESP_MODEM_DCE_BG96;
        #elif CONFIG_EXAMPLE_MODEM_DEVICE_SIM7600 == 1
                ESP_LOGI(TAG, "Initializing esp_modem for the SIM7600 module...");
                struct esp_modem_usb_term_config usb_config =
ESP_MODEM_SIM7600_USB_CONFIG();
                esp_modem_dce_device_t usb_dev_type = ESP_MODEM_DCE_SIM7600;
        #elif CONFIG_EXAMPLE_MODEM_DEVICE_A7670 == 1
                ESP_LOGI(TAG, "Initializing esp_modem for the A7682 module...");
                struct esp_modem_usb_term_config usb_config =
ESP_MODEM_A7670_USB_CONFIG();
                esp_modem_dce_device_t usb_dev_type = ESP_MODEM_DCE_SIM7600;
        #else
        #error USB modem not selected
        #endif
                const esp_modem_dte_config_t dte_usb_config =
ESP_MODEM_DTE_DEFAULT_USB_CONFIG(usb_config);
                ESP_LOGI(TAG, "Waiting for USB device connection...");
                esp_modem_dce_t *dce = esp_modem_new_dev_usb(usb_dev_type,
&dte_usb_config, &dce_config, esp_netif);
                assert(dce);
                esp_modem_set_error_cb(dce, usb_terminal_error_handler);
                ESP_LOGI(TAG, "Modem connected, waiting 10 seconds for boot...");
```

```
            vTaskDelay(pdMS_TO_TICKS(10000)); // Give DTE some time to boot

        #else
        #error Invalid serial connection to modem.
        #endif

            xEventGroupClearBits(event_group, CONNECT_BIT | GOT_DATA_BIT |
USB_DISCONNECTED_BIT);

            /* Run the modem demo app */
        #if CONFIG_EXAMPLE_NEED_SIM_PIN == 1
            // check if PIN needed
            bool pin_ok = false;
            if (esp_modem_read_pin(dce, &pin_ok) == ESP_OK && pin_ok == false) {
                if (esp_modem_set_pin(dce, CONFIG_EXAMPLE_SIM_PIN) == ESP_OK) {
                    vTaskDelay(pdMS_TO_TICKS(1000));
                } else {
                    abort();
                }
            }
        #endif

            uint8_t cnt = 0;
            char data[32];
            int volt, bcl, temperature, rssi, ber;
            bool sim_card_status = SIM_CARD_ABSENT;

            // Sync between DTE and DCE
                while (ESP_OK != esp_modem_sync(dce)) {
                        ESP_LOGI(TAG, "AT command failed %ds, retry...", ++cnt);
                        ACS_response();
                        vTaskDelay(pdMS_TO_TICKS(500));
                        xEventGroupSetBits(wdt_event_group, ALIVE_BIT);
                        if (cnt) {
                                ESP_LOGW(TAG, "Modem does not sync!");
                                reset_modem();
                        }
                }
                ESP_LOGI(TAG, "Test AT startup OK");
                esp_err_t err = esp_modem_set_echo(dce, 0);
                if (err != ESP_OK) {
                ESP_LOGE(TAG, "set_echo failed with %d", err);
                } else {
                        ESP_LOGI(TAG, "Switch echo off");
                }
```

```
        err = esp_modem_get_battery_status(dce, &volt, &bcl, &bcl);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "esp_modem_get_battery_status failed with %d %s", err,
esp_err_to_name(err));
        } else {
            ESP_LOGI(TAG, "Voltage: %d mV", volt);
        }
        err = esp_modem_get_temperature(dce, &temperature);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "esp_modem_get_temperature failed with %d %s", err,
esp_err_to_name(err));
        } else {
            ESP_LOGI(TAG, "Temperature: %d degC", temperature);
        }
        err = esp_modem_get_manufacturer(dce, data);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "get_manufacturer failed with %d", err);
        } else {
            ESP_LOGI(TAG, "Manufacturer: %s", data);
        }
        err = esp_modem_get_module_name(dce, data);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "get_module_name failed with %d", err);
        } else {
            ESP_LOGI(TAG, "Model: %s", data);
        }
        err = esp_modem_get_firmware_revision(dce, data);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "get_firmware_revision failed with %d", err);
        } else {
            ESP_LOGI(TAG, "Revision: %s", data);
        }
        err = esp_modem_get_iccid(dce, data);
        if (err != ESP_OK) {
            ESP_LOGE(TAG, "get_iccid failed with %d", err);
        } else {
            sim_card_status = SIM_CARD_PRESENT;
            ESP_LOGI(TAG, "ICCID: %s", data);
        }
        if (sim_card_status == SIM_CARD_PRESENT) {
                err = esp_modem_get_imsi(dce, data);
                if (err != ESP_OK) {
                        ESP_LOGE(TAG, "get_imsi failed with %d", err);
                } else {
                        ESP_LOGI(TAG, "IMSI: %s", data);
```

```
                    }
                    err = esp_modem_get_imei(dce, data);
                    if (err != ESP_OK) {
                        ESP_LOGE(TAG, "esp_modem_get_imei failed with %d", err);
                    } else {
                        ESP_LOGI(TAG, "IMEI: %s", data);
                    }
                    err = esp_modem_get_provider_name(dce, data);
                    if (err != ESP_OK) {
                        ESP_LOGE(TAG, "get_provider_name failed with %d", err);
                    } else {
                        ESP_LOGI(TAG, "Provider: %s", data);
                    }
                err = esp_modem_get_signal_quality(dce, &rssi, &ber);
                if (err != ESP_OK) {
                   ESP_LOGE(TAG, "esp_modem_get_signal_quality failed with %d %s",
err, esp_err_to_name(err));
                } else {
                    ESP_LOGI(TAG, "Signal quality: rssi %d, ber %d", rssi, ber);
                }
            } else {
                ESP_LOGW(TAG, "SIM card not inserted!");
                goto dte_cleanup;
            }
        #if CONFIG_EXAMPLE_SEND_MSG
            if (esp_modem_sms_txt_mode(dce, true) != ESP_OK ||
esp_modem_sms_character_set(dce) != ESP_OK) {
                ESP_LOGE(TAG, "Setting text mode or GSM character set failed");
                return;
            }
            err = esp_modem_send_sms(dce,
CONFIG_EXAMPLE_SEND_MSG_PEER_PHONE_NUMBER, "Text message from esp-
modem");
            if (err != ESP_OK) {
                ESP_LOGE(TAG, "esp_modem_send_sms() failed with %d", err);
                return;
            }
        #endif
            if (!mqtt_get_status()) {
            err = esp_modem_set_mode(dce, ESP_MODEM_MODE_DATA);
            if (err != ESP_OK) {
                ESP_LOGE(TAG, "esp_modem_set_mode(ESP_MODEM_MODE_DATA) failed
with %d", err);
                goto dte_cleanup;
            }
```

```
            ESP_LOGI(TAG, "LED state: LED_GSM_WAITING_FOR_IP...");
            last_led_state = ACS_led_state = LED_GSM_WAITING_FOR_IP;
            gptimer_update(ACS_led_state);
            cnt = 0;

            /* Очікування IP-адреси */
            ESP_LOGI(TAG, "Waiting for IP address");
            while (1) {
                        xEventGroupWaitBits(event_group, CONNECT_BIT |
USB_DISCONNECTED_BIT, pdFALSE, pdFALSE,
pdMS_TO_TICKS(1000));//portMAX_DELAY);
                        CHECK_USB_DISCONNECTION(event_group);
                        ESP_LOGW(TAG, "waiting for ip %ds, retry...", ++cnt);
                        ACS_response();
                        xEventGroupSetBits(wdt_event_group, ALIVE_BIT);
                        if ((xEventGroupGetBits(event_group) & CONNECT_BIT) ==
CONNECT_BIT) {
                                    ESP_LOGW(TAG, "Modem got ip!");
                                    break;
                        }
            }
                        mqtt_start();
            }
            return;
        #if 0
            /* Налаштування MQQT  підключення */
        #if ESP_IDF_VERSION >= ESP_IDF_VERSION_VAL(5, 0, 0)
            esp_mqtt_client_config_t mqtt_config = {
               //.broker.address.uri = CONFIG_EXAMPLE_MQTT_BROKER_URI,

                        .broker.address.hostname = "mqtt.app.ACS.com",
                        .broker.address.port = 8883,
                        .broker.address.transport = MQTT_TRANSPORT_OVER_SSL,
                        .credentials.username = "ACS",
                        .credentials.authentication.password = "******"
            };
        #else
            esp_mqtt_client_config_t mqtt_config = {
               .uri = CONFIG_EXAMPLE_MQTT_BROKER_URI,
            };
        #endif
            esp_mqtt_client_handle_t mqtt_client = esp_mqtt_client_init(&mqtt_config);
            esp_mqtt_client_register_event(mqtt_client, ESP_EVENT_ANY_ID,
mqtt_event_handler, NULL);
```

```
            esp_mqtt_client_start(mqtt_client);
            ESP_LOGI(TAG, "Waiting for MQTT data");

            xEventGroupWaitBits(event_group, GOT_DATA_BIT |
USB_DISCONNECTED_BIT, pdFALSE, pdFALSE, portMAX_DELAY);
            CHECK_USB_DISCONNECTION(event_group);
        #endif//0

        #if defined(CONFIG_EXAMPLE_SERIAL_CONFIG_USB)
            ESP_LOGI(TAG, "USB demo finished. Disconnect and connect the modem to run it
again");
            xEventGroupWaitBits(event_group, USB_DISCONNECTED_BIT, pdFALSE,
pdFALSE, portMAX_DELAY);
            CHECK_USB_DISCONNECTION(event_group); // dce will be destroyed here
        } // while (1)
        #else
        dte_cleanup:
            esp_modem_destroy(dce);
            esp_netif_destroy(esp_netif);
        #endif
        }
```

Підключення до мережі:

```
        void pppos_client_connect(void)
        {
            uint8_t cnt = 0;

            ESP_LOGI(TAG, "pppos_client connect...");

            // Sync between DTE and DCE
                while (ESP_OK != esp_modem_sync(dce)) {
                        ESP_LOGI(TAG, "AT command failed %ds, retry...", ++cnt);
                        ACS_response();
                        vTaskDelay(pdMS_TO_TICKS(500));
                        xEventGroupSetBits(wdt_event_group, ALIVE_BIT);

                        if (cnt) {
                                ESP_LOGW(TAG, "Modem does not sync!");
                                reset_modem();
                        }
                }

                ESP_LOGI(TAG, "Test AT startup OK!");
```

```
            esp_err_t err = esp_modem_set_echo(dce, 0);
            if (err != ESP_OK) {
            ESP_LOGE(TAG, "set_echo failed with %d", err);
            } else {
                    ESP_LOGI(TAG, "Switch echo off");
            }

            xEventGroupClearBits(event_group, CONNECT_BIT | GOT_DATA_BIT |
USB_DISCONNECTED_BIT);

        err = esp_modem_set_mode(dce, ESP_MODEM_MODE_DATA);
        if (err != ESP_OK) {
           ESP_LOGE(TAG, "esp_modem_set_mode(ESP_MODEM_MODE_DATA) failed
with %d", err);
           return;
        }

        ESP_LOGI(TAG, "LED state: LED_GSM_WAITING_FOR_IP...");
        last_led_state = ACS_led_state = LED_GSM_WAITING_FOR_IP;
        gptimer_update(ACS_led_state);

        cnt = 0;

        /* Wait for IP address */
        ESP_LOGI(TAG, "Waiting for IP address");
        while (1) {
                    xEventGroupWaitBits(event_group, CONNECT_BIT |
USB_DISCONNECTED_BIT, pdFALSE, pdFALSE, pdMS_TO_TICKS(1000));
                    CHECK_USB_DISCONNECTION(event_group);

                    ESP_LOGW(TAG, "waiting for IP %ds, retry...", ++cnt);
                    ACS_response();
                    xEventGroupSetBits(wdt_event_group, ALIVE_BIT);
                    if ((xEventGroupGetBits(event_group) & CONNECT_BIT) ==
CONNECT_BIT) {
                            ESP_LOGW(TAG, "Modem got ip!!!");
                            return;
                    }
        }
    }
```

Обробка команд пристроєм:

```
    static void parser_task(void *parameters) {
            parser_queue_request_item_t parser_request = { 0 };
```

```
        char* response = NULL;

        parser_request_queue = xQueueCreate(PARSER_QUEUE_SIZE,
sizeof(parser_queue_request_item_t));
        if (parser_request_queue == NULL) {
            ESP_LOGE(TAG, "can not create request queue");
            vTaskDelete(NULL);
            return;
        }
        parser_response_queue = xQueueCreate(PARSER_QUEUE_SIZE,
sizeof(parser_queue_response_item_t));
        if (parser_response_queue == NULL) {
            ESP_LOGE(TAG, "can't create response queue");
            vTaskDelete(NULL);
            return;
        }
        while (1) {
            memset(parser_request.data, 0, sizeof(parser_request.data));
            response = NULL;
            if (xQueueReceive(parser_request_queue, &parser_request,
portMAX_DELAY) == pdPASS) {
                if (parser_request.channel == PARSER_CHANNEL_BLE) {
                    response = parser_ble(parser_request.data,
PARSER_CHANNEL_BLE);
                } else if (parser_request.channel == PARSER_CHANNEL_MQTT)
{
                    response = parser_mqtt(parser_request.data);
                }
                if (response != NULL) {
                    parser_queue_response_item_t parser_response;
                    parser_response.channel = parser_request.channel;
                    parser_response.data = response;
                    if (xQueueSend(parser_response_queue, (void
*)&parser_response, pdMS_TO_TICKS(100)) == errQUEUE_FULL) {
                        ESP_LOGE(TAG, "response queue is full");
                    }
                }
            }
        }
        vTaskDelete(NULL);
    }
```

Отже, за рахунок розробки програмної частини вдосконаленої системи моніторингу було реалізовано практичну частину реалізації резервного каналу зв’зку.

3.3 Інтеграція шифрування даних у резервний канал системи моніторингу

У цьому розділі ми розглянемо практичну інтеграцію алгоритму шифрування AES256 у резервний канал системи моніторингу. Цей метод шифрування обраний завдяки своїй високій ступені безпеки та ефективності. Тепер ми перейдемо до конкретних етапів та кроків, які включаються в процес інтеграції шифрування даних для забезпечення конфіденційності та захисту пакетів інформації у резервному каналі.

Далі буде розглянуто інтеграцію шифрування AES256 у код програми:

Шифрування:

```
void chiper_encrypt(char* data, char* key, char* output_buffer) {
        char key_buffer[16] = { 0 };
        char *data_buffer = NULL;
        mbedtls_aes_context aes;
        unsigned char output_buffer_enc[2048] = { 0 };
        unsigned char iv[16] = { 0 };

        size_t key_size = strlen(key) > 16 ? 16 : strlen(key);
        memcpy(key_buffer, key, key_size);

        esp_fill_random(iv, 16);

        size_t data_size = strlen(data) % 16 ? ((strlen(data) / 16) * 16) + 32 :
strlen(data) + 32;
        data_buffer = (char *)malloc(data_size);
        memset(data_buffer, 0, data_size);
        memcpy(data_buffer, iv, 16);
        memcpy(&data_buffer[16], data, strlen(data));
        data_buffer[16 + strlen(data)] = 0x80;

        mbedtls_aes_init(&aes);
```

```
        mbedtls_aes_setkey_enc(&aes, (const unsigned char*)key_buffer, 256);
        mbedtls_aes_crypt_cbc(&aes, MBEDTLS_AES_ENCRYPT, data_size, iv,
(const unsigned char*)data_buffer, output_buffer_enc);
        mbedtls_aes_free(&aes);

        free(data_buffer);

        base64_encode(output_buffer_enc, data_size, (unsigned char*)output_buffer);
    }
```

Дешифрування:

```
    void chiper_decrypt(char* data, char* key, char* output_buffer) {
        char key_buffer[16] = { 0 };
        unsigned char buffer[2048] = { 0 };
        mbedtls_aes_context aes;
        unsigned char iv[16] = { 0 };

        size_t key_size = strlen(key) > 16 ? 16 : strlen(key);
        memcpy(key_buffer, key, key_size);
        size_t data_size = base64_decode((unsigned char*)data, strlen(data), buffer);
        memcpy(iv, buffer, 16);
        mbedtls_aes_init(&aes);
        mbedtls_aes_setkey_dec(&aes, (const unsigned char*)key_buffer, 256);
        mbedtls_aes_crypt_cbc(&aes, MBEDTLS_AES_DECRYPT, data_size, iv,
(const unsigned char *)&buffer[16], (unsigned char *)output_buffer);
        mbedtls_aes_free(&aes);
    }
```

3.4 Тестування вдосконаленої системи контролю та управління доступом з резервним каналом та шифруванням даних

Етап тестування розробленої системи є вкрай важливим, адже саме під час цього етапу ми маємо можливість зімітувати атаку, спрямовану на блокування основного каналу зв'язку у вдосконаленій системі контролю та управління доступом.

Для початку ініціалізуємо систему та здійснимо підключення до основних каналів зв’язку (рис 3.4 та рис 3.5)

```
I (2032) ble: init
I (2032) BLE_INIT: BT controller compile version [963cad4]
I (2042) phy_init: phy_version 601,98f2a71,Jun 29 2023,09:58:12
I (2072) BLE_INIT: Bluetooth MAC: 34:85:18:46:e1:ee

I (2092) ble: GATTS_REG_EVT, status 0, app_id 0
I (2092) ble: GATTS_CREATE_EVT, status 0, service_handle 40
I (2092) ble: GATTS_START_EVT, status 0, service_handle 40
I (2102) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 42, service_handle 40
I (2112) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 44, service_handle 40
I (2122) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 46, service_handle 40
I (2122) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 48, service_handle 40
I (2132) ble: GATTS_ADD_CHAR_DESCR_EVT, status 0, attr_handle 49, service_handle 40
```

Рисунок 3.4 – Ініціалізація Bluetooth підключення

```
I (2212) wifi:wifi driver task: 3fcde108, prio:23, stack:6656, core=0
I (2212) wifi:wifi firmware version: ce9244d
I (2222) wifi:wifi certification version: v7.0
I (2222) wifi:config NVS flash: enabled
I (2222) wifi:config nano formating: disabled
I (2232) wifi:Init data frame dynamic rx buffer num: 32
I (2232) wifi:Init management frame dynamic rx buffer num: 32
I (2242) wifi:Init management short buffer num: 32
I (2242) wifi:Init dynamic tx buffer num: 32
I (2242) wifi:Init static tx FG buffer num: 2
I (2252) wifi:Init static rx buffer size: 1600
I (2252) wifi:Init static rx buffer num: 10
I (2252) wifi:Init dynamic rx buffer num: 32
I (2262) wifi_init: rx ba win: 6
I (2272) wifi_init: tcpip mbox: 32
I (2272) wifi_init: udp mbox: 6
I (2282) wifi_init: tcp mbox: 6
I (2282) wifi_init: tcp tx win: 5744
I (2282) wifi_init: tcp rx win: 5744
I (2292) wifi_init: tcp mss: 1440
I (2292) wifi_init: WiFi IRAM OP enabled
I (2292) wifi_init: WiFi RX IRAM OP enabled
I (2302) wifi: init
I (2302) wifi:mode : sta (34:85:18:46:e1:ec)
I (2302) wifi:enable tsf
I (2312) wifi: started
I (4722) wifi:new:<11,2>, old:<1,0>, ap:<255,255>, sta:<11,2>, prof:1
I (5452) wifi:state: init -> auth (b0)
I (5452) wifi:state: auth -> assoc (0)
I (5462) wifi:state: assoc -> run (10)
I (5572) wifi:connected with TP-Link_30FC, aid = 1, channel 11, 40D, bssid = 0c:80:63:c0:30:fc
I (5572) wifi:security: WPA2-PSK, phy: bgn, rssi: -65
I (5592) wifi:pm start, type: 1

I (5592) wifi:set rx beacon pti, rx_bcn_pti: 14, bcn_timeout: 25000, mt_pti: 14, mt_time: 10000
I (5602) wifi:<ba-add>idx:0 (ifx:0, 0c:80:63:c0:30:fc), tid:0, ssn:2, winSize:64
I (5622) wifi:AP's beacon interval = 102400 us, DTIM period = 1
I (7092) esp_netif_handlers: sta ip: 192.168.0.109, mask: 255.255.255.0, gw: 192.168.0.1
I (7092) wifi: connect, got ip: 192.168.0.109
I (7102) lokkyy: connect to WIFI
I (7102) mqtt: other event id:7
I (7102) wifi: rssi: -64
```

Рисунок 3.5 – Ініціалізація Wi-Fi підключення

Як бачимо зі знімків екрану терміналу систему успішно ініціалізовано, виконано успішне підключення до основних каналів зв’язку.

Система працює у штатному режимі.

На наступному етапі спробуємо відтворити глушіння Wi-Fi сигналу, вимкнувши точку доступу (рис. 3.6)

```
I (152282) wifi:<ba-del>idx:0, tid:0
I (152282) wifi:new:<11,0>, old:<11,2>, ap:<255,255>, sta:<11,2>, prof:1
E (152292) esp-tls: [sock=55] delayed connect error: Software caused connection abort
I (152292) wifi: disconnect
E (152302) transport_base: Failed to open a new connection: 32772
E (152312) mqtt_client: Error transport connect
I (152312) mqtt: MQTT_EVENT_ERROR
I (152312) mqtt: MQTT_EVENT_DISCONNECTED
I (152322) lokkyy: MQTT client not connect
E (152292) esp-tls: [sock=54] delayed connect error: Software caused connection abort
I (152302) lokkyy: not connect to WIFI
E (152332) transport_base: Failed to open a new connection: 32772
E (152352) mqtt_client: Error transport connect
I (152352) mqtt: MQTT_EVENT_ERROR
I (152362) mqtt: MQTT_EVENT_DISCONNECTED
I (152362) lokkyy: MQTT client not connect
I (152332) mqtt: disconnect
```

Рисунок 3.6 – Імітація атаки блокуванням Wi-Fi сигналу

Переглянемо як система відреагувала на цю атаку (рис. 3.7)

```
I (23767) pppos_client: Module Name=SIMCOM_SIM800C
I (23867) pppos_client: Product Name and Release information: SIM800 R14.18
I (23967) pppos_client: Product Revision information: Revision:1418B10SIM800C24_TLS12
I (24067) pppos_client: Product Serial Number: 869627034683896
I (24167) pppos_client: Voltage: 4120 mV, bcs=0, bcl=89
I (24267) pppos_client: SIM Card inserted
I (24367) pppos_client: IMSI=255011673154378
I (24467) pppos_client: IMEI=869627034683896
I (24567) pppos_client: Operator Name=UMC, 1007778424
I (24667) pppos_client: Mobile Subscriber: 255011673154378
I (24767) pppos_client: Signal quality: rssi -79dbm, rssi value 17, ber 0
I (25017) pppos_client: Waiting for IP address
I (25017) pppos_client: LED state: LED_GSM_WAITING_FOR_IP...
I (25017) gptimer: Stop gptimer
I (25027) gptimer: Start gptimer with led state: LED_GSM_WAITING_FOR_IP
I (31757) esp-netif_lwip-ppp: Connected
I (31757) pppos_client: Modem Connect to PPP Server
I (31757) pppos_client: ~~~~~~~~~~~~~~
I (31767) pppos_client: IP          : 10.142.120.9
I (31767) pppos_client: Netmask     : 255.255.255.255
I (31777) pppos_client: Gateway     : 192.168.254.254
I (31777) pppos_client: Name Server1: 80.255.64.23
I (31797) pppos_client: Name Server2: 80.255.64.24
I (31797) pppos_client: ~~~~~~~~~~~~~~
```

Рисунок 3.7 – Реакція системи на блокування Wi-Fi

З виведених системних даних у терміналі видно, що в результаті атаки, яка полягала в блокуванні Wi-Fi сигналу, наша система успішно активувала резервний канал та встановила з'єднання, обходячи блокування Wi-Fi. Цей успішний сценарій свідчить про ефективність механізму резервного каналу.

З врахуванням цього результату можна зробити висновок, що система демонструє надійну працездатність та здатність вчасно реагувати на потенційні загрози, такі як блокування основного каналу зв’язку.

3.5 Висновки до розділу

В ході розробки та вдосконалення системи моніторингу та управління доступом було зазначено декілька ключових висновків.

Щодо інтеграції шифрування AES256, обрана стратегія забезпечила високий рівень безпеки та конфіденційності передаваних даних. Практична реалізація шифрування в програмному коді забезпечила ефективність та надійність в обміні інформацією. Фізичне підключення GSM модему виявилося критичним етапом, де врахування оптимального розташування та точне впаювання грали важливу роль у створенні надійного електричного з'єднання. Систематичне тестування дозволило вчасно виявити та усунути можливі проблеми, забезпечуючи стабільну роботу антени.

Інтеграція засобів зв'язку, зокрема Quectel EC25 через UART на ESP32, забезпечила надійний та ефективний обмін даними у системі моніторингу.

У цілому, ці вдосконалення додають високу рівень безпеки, ефективності та надійності до системи моніторингу та управління доступом, відповідаючи вимогам сучасних стандартів та забезпечуючи стійкість до можливих загроз.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

1) проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

2) розраховано витрати на здійснення науково-технічної розробки;

3) розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Підвищення захищеності від НСД на основі вдосконаленої системи

моніторингу управління доступом з шифруванням даних та резервного каналу» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [43].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуютьс я у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		

1. Технічна здійсненність концепції	3	3	3
2. Ринкові переваги (наявність аналогів)	3	3	4
3. Ринкові переваги (ціна продукту)	3	3	3
4. Ринкові переваги (технічні властивості)	4	3	3
5. Ринкові переваги (експлуатаційні витрати)	3	3	3
6. Ринкові перспективи (розмір ринку)	3	3	3
7. Ринкові перспективи (конкуренція)	2	2	2
8. Практична здійсненність (наявність фахівців)	3	3	3
9. Практична здійсненність (наявність фінансів)	3	3	3
10. Практична здійсненність (необхідність нових матеріалів)	3	3	3
11. Практична здійсненність (термін реалізації)	3	4	4
12. Практична здійсненність (розробка документів)	4	3	3
Сума балів	37	36	37
Середньоарифметична сума балів $СБ_c$	36,7		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [43].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ ,розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу» становить 36,7 балів, що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вищий середнього).

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості (Вн) для нового технічного рішення розрахуємо за формулою [44]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i \quad , \tag{4.1}$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

αі – коефіцієнт, який враховує питому вагу і-го технічного показника в загальній якості розробки. Коефіцієнт αі визначається експертним шляхом і при цьому має виконуватись умова ;

βі – відносне значення і-го технічного показника якості нової розробки.

Відносні значення βі для різних випадків розраховуємо за такими формулами:

- для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{нi}}{I_{ai}} \quad , \tag{4.2}$$

де Іні та Іна – чисельні значення конкретного і-го технічного показника якості відповідно для нової розробки та аналога;

- для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ai}}{I_{ni}} \quad ; \qquad (4.3)$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників. Експертами проведено оцінювання усіх параметрів за 10-ти бальною шкалою, а також визначено вагомості кожного показника в загальній їх системі. Результати зведено в табл. 4.4.

Таблиця 4.4 – Порівняння основних параметрів розробки та аналога

Показник	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (товар-конкурент)	Новий (інноваційне рішення)		
1	2	3	4	5
1.Технічні показники				
Максимум ключів	10000	15000	1,5	0.3
Напрацювання на відмову, год	25000	25000	1	0,30
Масо-габарити, кг	0,2	0,2	1	0,10
Температурний режим, °С	-25 – +30	-25 – +50	1	0,30
2. Економічні показники				
Ціна придбання, грн	4200	8000	0,525	1

Узагальнений коефіцієнт якості (Вн) для нового технічного рішення складе:

Вн= 1,5·0,3+1,0·0,3+1·0,1+1·0,3= 1,15.

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,15 рази.

Визначимо загальний показник конкурентоспроможності:

Кзаг = 1,15/0,525 = 2,19, що є досить високим показником конкурентоспроможності.

Також у результаті аналізу комерційного та наукового потенціалу доведено актуальність розробки.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов'язані з проведенням науково-дослідної роботи на тему «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [43]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.1)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дні;

T_p – середнє число робочих днів в місяці, T_p=21 день.

$$З_о = 22000{,}00 \cdot 60 / 21 = 62857{,}14 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	22000	1047,62	60	62857,14
Інженер-розробник програмного забезпечення	20000	952,38	60	57142,86
Інженер-розробник апаратної частини	20000	952,38	60	57142,86
Консультант	18000	857,14	40	34285,71
Всього				211428,57

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \quad , \tag{4.2}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \quad , \tag{4.3}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [43];

$К_с$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$Т_р$ – середнє число робочих днів в місяці, приблизно $Т_р$ = 21 день;

$t_{зм}$ – тривалість зміни, год.

$С_1 = 6700,00 \cdot 1,5 \cdot 1,65 / (21 \cdot 8) = 98,71$ грн.
$З_{р1} = 98,71 \cdot 8,00 = 789,64$грн.

Таблиця 4.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника, грн
Первинне налаштування робочих станцій	8	4	1,5	98,71	789,64
Налаштування локальної мережі для обладнання	10	4	1,5	98,71	987,05
Підготовка робочого місця дослідника	2,4	2	1,1	72,38	173,72
Монтаж обладнання	10	5	1,7	111,87	1118,66
Всього					3069,08

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.4)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 12%.

$З_{дод} = (211428,57 + 3069,08) \cdot 12 / 100\% = 25739,72$грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.5)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (211428,57+ 3069,08+ 25739,72) · 22 / 100% = 52852,22 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень.

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} Н_{вj} Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц \quad , \quad (4.6)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1$ = 3 · 180,00 · 1,1 - 0,000 · 0,00 = 660,0 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за од, грн	Норма витрат, од	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Офісний папір А4 MAESTRO 80г/м2 500арк	180	3	0	0	660
Папір для записів Economix	110	1	0	0	121
Настільний набір Buromax 16 предметів	215	2	0	0	473
Картридж для принтера Canon LBP6500	1300	1	0	0	1430
Flesh-пам'ять Kingston 16 GB	130	1	0	0	143
Всього					2761

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР нового технічного рішення, розраховуються, згідно з їхньою номенклатурою, за формулою:

$$Кв = \sum Н_j Ц_j К_j, \quad (4.7)$$

де Нj – кількість комплектуючих j-го виду, шт.;

Цj – покупна ціна комплектуючих j-го виду, грн;

Кj – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15).

Проведені розрахунки зводимо до таблиці.

М1 = 1 · 3000,00 · 1,1 = 3300 грн.

Таблиця 4.8 – Витрати на комплектуючі

Найменування	Кількість, од	Ціна, грн/од	Сума, грн
GSM модем quectel EC25	1	3000	3300
Плата електронного замка на основі ESP32	1	4200	4620
Всього			7920

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \quad , \qquad (4.8)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i = *1,10…1,12);*

k – кількість найменувань устаткування.

$B_{спец}$ = *25000· 2 · 1,1 = 55000 грн.*

Отримані результати зведемо до таблиці.

Таблиця 4.9– Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Робоча станція (ПК)	2	25000	55000
Маршрутизатор	1	2300	2530
Всього			57530

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для

проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \quad , \tag{4.9}$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (K_i = *1,10…1,12);*

k – кількість найменувань програмних засобів.

$B_{прг} = 12000{,}00 \cdot 2 \cdot 1{,}12 = 26880$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.10 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Операційна система Microsoft Windows 10	2	12000	26880
Система розробки Project Rider	1	4200	4704
Всього			31584

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12} \quad , \tag{4.10}$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (5500{,}00 \cdot 3) / (5 \cdot 12) =$ 2750,00 *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Робоча станція (ПК)	55000	5	3	2750,00
Маршрутизатор	2530	3	3	210,83
Оргтехніка	6000	5	2	200,00
Приміщення лабораторії	212000	20	3	2650,00
ОС Windows 11	26880	3	3	2240,00
Система розробки Project Rider	4704	2	2	392,00
Всього				8442,83

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію ($B_е$) розраховуємо за формулою:

$$B_е = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_е \cdot K_{вni}}{\eta_i}, \quad (4.11)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е$ = 7,50 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_е = 2 * 0{,}5 \cdot 480{,}0 \cdot 7{,}50 \cdot 0{,}95 / 0{,}97 = 3525{,}77$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.12 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Робоча станція (ПК) -2шт	0,5	480	3525,77
Маршрутизатор	0,02	480	70,52
Робоче місце дослідника	0,15	480	528,87
Оргтехніка	0,45	20	66,11
Всього			4191,26

4.3.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \quad (4.12)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$B_{св}$ = (211428,57+ 3069,08) · 20 / 100% = 42899,53грн.

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.13)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$B_{сп}$ = (211428,57+ 3069,08) · 30 / 100% = 64349,30грн.

4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (211428,57+ 3069,08) · 50 / 100% = 107248,83 грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 120%.

$B_{нзв}$ = (211428,57+ 3069,08) · 120 / 100% = 257 397,18грн.

Витрати на проведення науково-дослідної роботи розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.16)$$

$B_{заг}$= 877413,52грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.17)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,7.

$$ЗВ = 877413,52/ 0,7 = 1253447,88грн.$$

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу» передбачають комерціалізацію протягом 3-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

1-й рік – 10000 користувачів;

2-й рік – 15000 користувачів;

3-й рік – 12000 користувачів.

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 200000 користувачів;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 8000 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 500 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 3-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [43]:

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.18)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо ρ =30%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1 =$(200000,00·500,00+8500,00·10000)·0,83·0,3·(1-0,18/100%)= 37909830 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2 =$(200000,00·500,00+8500,00·(10000+15000))·0,83·0,3·(1-0,18/100%)=64036875 грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 =$(200000,00·500,00+8500,00·(10000+15000+12000))·0,83·0,3·(1-0,18/100%)= 84938511 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.19)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,25;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$ПП =$

37909830/(1+0,25)^1+64036875/(1+0,25)^2+84938511/(1+0,25)^3=114799981,63грн.

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$ВВ = k_{інв} \cdot \quad , \tag{4.20}$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=3;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 1253447,88 грн.

$ВВ = k_{інв} \cdot$ = 3 · 1253447,88= 3726400,779грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{4.21}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 114799981,63грн;

PV – теперішня вартість початкових інвестицій, 3726400,779грн.

$E_{абс} = ПП - PV$ = 114799981,63- 3726400,779= 111073580,85грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 \quad , \tag{4.22}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 111073580,85 грн;

PV – теперішня вартість початкових інвестицій, 3726400,779грн;

$T_{ж}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 3 роки.

$$E_{в} = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+111073580,85/3726400,779)^{1/3}= 2,13.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \tag{4.23}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,11;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,18.

$\tau_{мін}$ = 0,11+0,18 = 0,29 < 2,13 свідчить про те, що внутрішня економічна дохідність інвестицій $E_{в}$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_{в}}, \tag{4.24}$$

де $E_{в}$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 2,13 = 0,47 року.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

4.5 Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу» становить 36,7 балів, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вищий середнього).

Також термін окупності становить 0,478 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу».

ВИСНОВОК

В цій роботі було проведено детальний аналіз систем контролю та управління доступом, включаючи їх структурні особливості, персональні системи контролю доступу, можливості дистанційного управління, моніторинг та існуючі аналоги сучасних замків. Було визначено можливості підвищення захищеності від несанкціонованого доступу на основі вдосконаленої системи моніторингу управління доступом.

В роботі було розроблено алгоритм роботи вдосконаленої системи контролю та управління доступом, вибрано технології резервного каналу та алгоритм шифрування даних для підвищення захищеності системи. Також було вибрано елементну базу апаратної частини системи.

В результаті було розроблено вдосконалену систему моніторингу управління доступом, включаючи інтеграцію апаратної частини резервного каналу у систему контролю доступу, розробку програмної частини резервного каналу, інтеграцію шифрування даних у резервний канал системи моніторингу та тестування вдосконаленої системи контролю та управління доступом з резервним каналом та шифруванням даних.

Ця робота відкриває нові можливості для підвищення захищеності систем контролю та управління доступом. Вона може слугувати основою для подальших досліджень в цій області.

Додатково, важливо зазначити, що ця робота не тільки досліджує існуючі системи контролю та управління доступом, але й пропонує конкретні шляхи їх вдосконалення. Вона включає в себе розробку нового алгоритму роботи, вибір технологій резервного каналу, алгоритму шифрування даних та елементної бази апаратної частини системи. Ці елементи, в свою чергу, сприяють підвищенню захищеності системи від несанкціонованого доступу.

Розробка вдосконаленої системи моніторингу управління доступом є ключовим елементом цієї роботи. Це включає інтеграцію апаратної частини резервного каналу у систему контролю доступу, розробку програмної частини

резервного каналу, інтеграцію шифрування даних у резервний канал системи моніторингу та тестування вдосконаленої системи контролю та управління доступом з резервним каналом та шифруванням даних.

Всі ці елементи разом створюють сильну основу для подальшого вдосконалення систем контролю та управління доступом. Ця робота є важливим кроком у напрямку розробки більш надійних та безпечних систем, які можуть відігравати ключову роль у захисті від несанкціонованого доступу. Вона також відкриває нові можливості для подальших досліджень в цій області.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: навч. посіб. Київ: Видавництво НА СБ України, 2020. 256 с.

2. Сучасні інформаційні технології та системи в управлінні: збірн. матеріалів. Київ: КНЕУ, 2017. 213 с.

3. Система контролю і управління доступом. Вікіпедія: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC (дата звернення 15.10.2023).

4. Яку СКУД вибрати: огляд систем безпеки. iXBT.com: веб-сайт. URL: https://www.ixbt.com/live/sw/kakuyu-skud-vybrat-obzor-sistem-bezopasnosti.html (дата звернення 15.10.2023).

5. Системи контролю і управління доступом. ВалТек: веб-сайт. URL: https://valtek.com.ua/ua/system-integration/security-control-system/accesscontrol/access-control-review (дата звернення 15.10.2023).

6. Системи контролю і управління доступом від А до Я. deps: веб-сайт. URL: https://deps.ua/ua/knowegable-base/reference-information/7824.html (дата звернення 15.10.2023).

7. Системи контролю та керування доступом. видеокамеры.com.ua: вебсайт. URL: https://xn--80adgeboqrpy5j.com.ua/kontrol_dostypy/ (дата звернення 15.10.2023).

8. СКУД. ТЗІ: веб-сайт. URL: https://tzi.ua/ua/skud.html (дата звернення 15.10.2023).

9. Система контролю і управління доступом (СКУД). VIST+IT: веб-сайт. URL: https://vistplus.com/it-poslugi/skud/ (дата звернення 15.10.2023).

10. Об’єкти та процедури, що є системою контролю і управління доступом. ua-referat.com: веб-сайт. URL:

https://uareferat.com/%D0%9E%D0%B1%60%D1%94%D0%BA%D1%82%D0%B8_%D1%
82%D0%B0_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B8_%D1%97%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BE%D1%8E_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC (дата звернення 15.10.2023).

11. Хоріщенко Я.В., Перекрест А.Л. Система віддаленого керування та моніторингу технічних об’єктів з використанням веб-технологій та динамічних сторінок. Проблеми вищої школи. Інновації в освіті та виробництві. Комп’ютерні технології в освіті та виробництві. 2020. С. 49-50.

12. Євтушенко К.В., Перекрест А.Л. Обґрунтування структури мережевої лабораторії з дистанційним доступом через Internet. Збірка наукових праць VII Всеукраїнської науково-технічної конференції молодих учених і спеціалістів «Електромеханічні та енергетичні системи, методи моделювання та оптимізації». Кременчук, КрНУ, 2010. С. 55-56.

13. Веб-технології віддаленого керування. Луцький національний технічний університет: веб-сайт. URL: https://elib.lntu.edu.ua/sites/default/files/elib_upload/APS%20i%20K/page29.html (дата звернення 15.10.2023).

14. Розроблення системи керування віддаленими об’єктами. allbest: вебсайт. URL: https://revolution.allbest.ru/programming/00706696_0.html (дата звернення 15.10.2023).

15. Кращі програми для віддаленого доступу до комп’ютера. VIST+IT: веб-сайт. URL: https://vistplus.com/stati/krashhi-programi-dlya-viddalenogodostupu-do-komp-yutera/ (дата звернення 15.10.2023).

16. Макаренко А.Ю., Парфенова А.О., Могильний С.Б. Бездротові технології передачі даних Wi-Fi, Bluetooth та ZigBee. Вісник національного технічного університету України «КПІ». Серія Радіотехніка. Радіоапаратобудування. 2010. Вип. 41. С. 171-181.

17. Азаров О., Богомолов С., Крупельницький Л. Використання бездротових мереж у системах опрацювання біомедичних сигналів. ВНТУ. С. 146-150.

18. Бездротові технології. Вікіпедія: веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%B4%D1%80%D0%BE%D1%82%D0%BE%D0%B2%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97 (дата звернення 15.10.2023).

19. Дистанційне управління зі смартфона з WI-FI, Bluetooth, LTE, GSM. DTB-GROUP: веб-сайт. URL: https://dtb.com.ua/ua/g91671568-upravleniesmartfona-kanalam (дата звернення 15.10.2023).

20. Z-Wave vs ZigBee, WiFi, Thread, Bluetooth BLE. SuperHome.pro: вебсайт. URL: https://superhome.pro/z-wave-vs-zigbee-wifi-thread-Bluetooth-blevybiraem-protokol-upravleniya-umnym-domom/ (дата звернення 16.10.2023).

21. Види замків для СКУД. Dnepr Security: веб-сайт. URL: https://dneprsecurity.com/statji/vidi-zamkov-dlja-skud-.html (дата звернення 16.10.2023).

22. Електронні замки СКУД. 740: веб-сайт. URL: https://740.com.ua/catalog/elektronye-zamki-skud (дата звернення 16.10.2023).

23. Як вибрати замок для системи контролю і управління доступом. ФОРТЕР: веб-сайт. URL: https://www.forter.com.ua/experts/kak-vybrat-zamokdlja-sistemy-kontrolja-i-upravlenija-dostupom-skud/ (дата звернення 16.10.2023).

24. Замки в СКУД: основні технічні характеристики та принципи дії. Охорони в домі немає: веб-сайт. URL: http://ohranivdome.net/kontrol-iupravlnenie-dostupom/montazh-sistem-kontrolya-dostupa/zamki-v-skud-osnovnye-tekhnicheskie-kharakteristiki-i-principy-dejjstviya.html (дата звернення 16.10.2023).

25. Види замків в системах контролю і управління доступом. Power Video: веб-сайт. URL: https://www.powervideo.ru/blog/vidyi-zamkov-v-sistemaxkontrolya-bezopasnosti.html (дата звернення 16.10.2023).

26. Електронні замки і ключі: види та механіка роботи. iron Logic: вебсайт. URL: https://ironlogic.ru/il.nsf/htm/ru_new_15.09.2013 (дата звернення 16.10.2023).

27. Встановлення та розробка систем контролю доступу. ЛюксМайстер: веб-сайт. URL: https://locksmaster.ua/vstanovlennja-rozrobka-sistem-kontroljudostupu/?gclid=CjwKCAjwhCVBhB8EiwAjFEPGVRiSzrLLXXUPhVCibKWqqx7bPYF1hjpBzjWtKY6FUIDSp omq_AOxxoCxV4QAvD_BwE (дата звернення 16.10.2023).

28. Біометричні замки для систем контролю доступу. Лабораторія безпеки: веб-сайт. URL: https://securitylab.com.ua/ua/sistemy-kontrolyadostupa/biometricheskie/zamki/ (дата звернення 16.10.2023).

29. Які бувають замки в СКУД. Magazun: веб-сайт. URL: https://magazun.com/poleznye-stati-uk/pro-kontrol-dostupa/kakie-byvayut-zamkinakladnye-rigelnye-elektromagnitnye-avtonomnye-i-navesnye-uk/ (дата звернення 16.10.2023).

30. Що таке СКУД? Kibstore: веб-сайт. URL: https://kibstore.com/blog/kontrol-dostupu/ssho-take-skud (дата звернення 16.10.2023).

31. Огляд електронних замків. Електрик.Інфо: веб-сайт. URL: http://electrik.info/main/automation/1436-umnye-zamki-obzor.html (дата звернення 16.10.2023).

32. Сучасні замки для воріт. Нові ворота: веб-сайт. URL: https://novivorota.com.ua/zamki-dlia-raspashnih.html (дата звернення 16.10.2023).

33. Види замків. House Of Locks: веб-сайт. URL: https://houselock.com.ua/ua (дата звернення 16.10.2023).

34. Замки для воріт. Ворота-маркет: веб-сайт. URL: https://vorotamarket.com.ua/?gclid=Cj0KCQjwn4qWBhCvARIsAFNAMihHkzYP8i

f0mcb851WCP5IArg1CgJK2TMgvGD9SAVnJ1GboD-iI0TQaAs3SEALw_wcB (дата звернення 16.10.2023).

35. ESP32. Вікіпедія: веб-сайт. URL: https://uk.wikipedia.org/wiki/ESP32 (дата звернення 19.10.2023).

36. Плата розробника для модуля ESP32. Arduino.ua: веб-сайт. URL: https://arduino.ua/prod2151-plata-razrabotchika-dlya-modylya-esp32 (дата звернення 19.10.2023).

37. Плата розробника ESP-WROOM-32 ESP32 (Wi-Fi + Bluetooth). Ardushop: веб-сайт. URL: https://ardushop.in.ua/arduino/developer-board-espwroom-32-esp-32-Wi-Fi-Bluetooth (дата звернення 19.10.2023).

38. Advanced Encryption Standard (AES). Вікіпедія: веб-сайт. URL: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard (дата звернення 19.10.2023).

39. AES-шифрування. memory.net.ua: веб-сайт. URL: https://memory.net.ua/blog/aes-shifruvannja.html (дата звернення 19.10.2023).

40. Contributors to Wikimedia projects. Elliptic-curve cryptography - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography (дата звернення: 01.11.2023).

41. Contributors to Wikimedia projects. RSA (cryptosystem) - Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/RSA_(cryptosystem) (дата звернення: 02.11.2023).

42. Wiki - Qualcomm Linux Modems by Quectel & Co - Open Source Mobile Communications. *Open Source Mobile Communications*. URL: https://osmocom.org/projects/quectel-modems/wiki (дата звернення: 02.11.2023).

43. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с.

44. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа. Вінниця : ВНТУ, 2016. 113 с.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції "Управління інформаційною безпекою" кафедри МБІС

д.т.н., професор

Юрій ЯРЕМЧУК

"20" вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу

08-72.МКР.004.00.099.ТЗ

Керівник магістерської кваліфікаційної роботи

к.т.н., доцент Карпінець В.В.

Вінниця – 2023 р.

1. Найменування та область застосування

Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу. Область застосування: захист інформаційних ресурсів від несанкціонованого доступу у системах контролю та управління доступом.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №203 від 18. 09. 2023 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка ефективного алгоритму захисту від атаки блокуванням основних каналів зв’язку у системах контролю та управління доступом.

3.2 Призначення: розроблений програмний та апаратний алгоритм від атаки блокуванням основних каналів зв’язку у системах контролю та управління доступом.

4. Джерела розробки

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4.– С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Pentium 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 512 Mb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	25.09.2023
2	Аналіз предметної області обраної теми	26.09.2023	05.10.2023
3	Апробація отриманих результатів	06.10.2023	10.10.2023
4	Розробка алгоритму роботи	11.10.2023	22.10.2023
5	Написання магістерської роботи на основі розробленої теми	23.10.2023	16.11.2023
6	Розробка економічної частини	17.11.2023	23.11.2023
7	Передзахист магістерської кваліфікаційної роботи	24.11.2023	25.11.2023
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	26.11.2023	30.11.2023
9	Захист магістерської кваліфікаційної роботи	15.12.2023	15.12.2023

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– вдосконалений пристрій

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Кметюк О.О.

Додаток Б. Лістинг файлу Database

```
#include "database.h"
#include "storage.h"

//-------------------------------------------------------------------------//
static const char *TAG = "database";
static const char charset[] =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567
89";
static const char database_user_cnt_key[]  = "db_user_cnt";
static const char database_admin_cnt_key[] = "db_admin_cnt";
//static const char database_id_key[]         = "db_id";

//-------------------------------------------------------------------------//
static void database_change_cnt(const char* key, bool is_inc) {
esp_err_t result = ESP_OK;
uint16_t count = storage_nvs_get_u16_value(key, &result);
if (result != ESP_OK) {
        ESP_LOGE(TAG, "can't get value: %s", key);
        return;
}

is_inc == true ? count++ : count--;

result = storage_nvs_set_u16_value(key, count);
if (result != ESP_OK) {
        ESP_LOGE(TAG, "can't change counter: %s", key);
}
}

//-------------------------------------------------------------------------//
char* database_generate_new_key(void) {
char *key = malloc(DATABASE_KEY_LENGTH + 1);

if (key) {
        int charset_len = sizeof(charset) - 1;
        int index;
```

```
        for (int n = 0; n < DATABASE_KEY_LENGTH; n++) {
                index = esp_random() % charset_len;
                key[n] = charset[index];
        }
        key[DATABASE_KEY_LENGTH] = '\0';
} else {
        ESP_LOGE(TAG, "can't generate key");
}

return key;
}

//-------------------------------------------------------------------------//
bool database_add_user(uint16_t* user_id, database_add_user_t* user) {
esp_err_t result;
char id_str[16] = { 0 };
size_t size;
uint16_t id;

for (id = 1; id < MAX_ID; id++) {
        snprintf(id_str, sizeof(id_str), "%d", id);

        if (storage_nvs_check_blob(id_str, &size) != ESP_OK) {
                ESP_LOGI(TAG, "user's blob with id: %d isn't exist", id);
                break;
        }
}

*user_id = id;

database_user_t newuser;
newuser.id = id;
newuser.parent_id = user->parent_id;
memcpy(newuser.key, user->key, sizeof(newuser.key));
newuser.active = user->active;
newuser.role = user->role;
newuser.gate = user->gate;
```

```
        newuser.block = user->block;
        newuser.permission = user->permission;
        newuser.time = user->time;
        newuser.valid = user->valid;
        newuser.payment = user->payment;
        memcpy(newuser.email, user->email, sizeof(newuser.email));

        ESP_LOGI(TAG, "newuser id: %"PRIu16", parent_id: %"PRIu16", user
key: %.*s, active: %d, role: %d, gate: %d, block: %d, permission: %d, time:
%"PRIu32", valid: %"PRIu32", payment: %"PRIu32", email: %.*s",
                        newuser.id,
                        newuser.parent_id,
                        DATABASE_KEY_LENGTH,
                        newuser.key,
                        newuser.active,
                        newuser.role,
                        newuser.gate,
                        newuser.block,
                        newuser.permission,
                        newuser.time,
                        newuser.valid,
                        newuser.payment,
                        sizeof(newuser.email),
                        newuser.email);

        result = storage_nvs_set_blob(id_str, &newuser);
        if (result != ESP_OK) {
                ESP_LOGE(TAG, "can't save new user to database");
                return false;
        }

        ESP_LOGI(TAG, "user's blob with id: %d created", id);

        database_get_key_int(DATABASE_ID));

        database_change_cnt("db_user_cnt", true);
        if (user->role == ADMIN) {
                database_change_cnt("db_admin_cnt", true);
```

```
	}

	ESP_LOGI(TAG, "user count: %d, admin count: %d",
database_get_user_cnt(), database_get_admin_cnt());

	return true;
	}

	//-------------------------------------------------------------------------//
	bool database_get_user(uint16_t id, database_user_t* user) {
	esp_err_t result = ESP_OK;
	char id_str[16] = { 0 };
	size_t size = 0;

	if (id == 0) {
		ESP_LOGE(TAG, "id is 0");
		return false;
	}

	snprintf(id_str, sizeof(id_str), "%d", id);

	if (storage_nvs_check_blob(id_str, &size) != ESP_OK) {
		ESP_LOGE(TAG, "can't find user's blob by id: %d", id);
		return false;
	}

	storage_nvs_get_blob(id_str, (void *)user, &result);
	if (result == ESP_OK) {
		ESP_LOGI(TAG, "get user's blob by id: %d, size: %d", id, size);
		return true;
	}
	return false;
	}

	//-------------------------------------------------------------------------//
	bool database_edit_user(uint16_t id, database_add_user_t* user) {
	esp_err_t result = ESP_OK;
	char id_str[16] = { 0 };
```

```
	database_user_t find_user;

	snprintf(id_str, sizeof(id_str), "%"PRIu16"", id);

	if (database_get_user(id, &find_user) != true) {
		ESP_LOGE(TAG, "can't get user data");
		return false;
	}

	if (find_user.role != ADMIN && user->role == ADMIN) {
		database_change_cnt("db_admin_cnt", true);
	} else if (find_user.role == ADMIN && user->role != ADMIN) {
		if (database_check_admin_id(id, &find_user)) {
			ESP_LOGI(TAG, "change admin to user");
			database_change_cnt("db_admin_cnt", false);

		} else {
			ESP_LOGI(TAG, "can't change single admin to user");
			return false;
		}
	}

	ESP_LOGI(TAG, "user count: %"PRIu16", admin count: %"PRIu16"",
database_get_user_cnt(), database_get_admin_cnt());

	find_user.id = id;
	find_user.parent_id = user->parent_id;
	memcpy(find_user.key, user->key, sizeof(find_user.key));
	find_user.active = user->active;
	find_user.role = user->role;
	find_user.gate = user->gate;
	find_user.block = user->block;
	find_user.permission = user->permission;
	find_user.time = user->time;
	find_user.valid = user->valid;
	find_user.payment = user->payment;
	//memcpy(find_user.email, user->email, sizeof(find_user.email));
	memcpy(find_user.email, user->email, strlen(user->email)+1);
```

```
result = storage_nvs_set_blob(id_str, &find_user);
if (result == ESP_OK) {
        ESP_LOGI(TAG, "user's blob with id: %"PRIu16" edited", id);
        return true;
}
return false;
}

//-------------------------------------------------------------------------//
bool database_delete_user(uint16_t id, database_user_t* user) {

esp_err_t result = ESP_OK;
char id_str[16] = { 0 };
database_user_t find_user;

if (database_get_user(id, &find_user) != true) {
        ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"", id);
        return false;
}

if (database_check_admin_id(id, &find_user)) {
        snprintf(id_str, sizeof(id_str), "%"PRIu16"", id);
        ESP_LOGI(TAG, "delete user id: %"PRIu16"", id);

        result = storage_nvs_delete_key(id_str);
        if (result != ESP_OK) {
                ESP_LOGE(TAG, "can't delete user by id: %"PRIu16"", id);
                return false;
        }

        ESP_LOGI(TAG, "user's blob with id: %"PRIu16" deleted", id);

        database_change_cnt("db_user_cnt", false);

        if (user->role == ADMIN) {
                database_change_cnt("db_admin_cnt", false);
        }
```

```
            ESP_LOGI(TAG, "user count: %"PRIu16", admin count:
%"PRIu16"", database_get_user_cnt(), database_get_admin_cnt());

        } else {
            ESP_LOGI(TAG, "can't delete single active Admin with id:
%"PRIu16"", id);
            return false;
        }

        return true;
        }

        //-------------------------------------------------------------------------//
        uint16_t database_get_user_cnt(void) {
        esp_err_t result;
        uint16_t user_cnt = storage_nvs_get_u16_value("db_user_cnt", &result);

        if (result != ESP_OK) {
            ESP_LOGE(TAG, "can't get user counter");
            return 0;
        }

        ESP_LOGI(TAG, "user cnt: %"PRIu16"", user_cnt);

        return user_cnt;
        }

        //-------------------------------------------------------------------------//
        uint16_t database_get_admin_cnt(void) {
        esp_err_t result;
        uint16_t admin_cnt = storage_nvs_get_u16_value("db_admin_cnt",
&result);

        if (result != ESP_OK) {
            ESP_LOGE(TAG, "can't get admin counter");
            return 0;
        }
```

```
ESP_LOGI(TAG, "admin cnt: %"PRIu16"", admin_cnt);

return admin_cnt;
}

//-------------------------------------------------------------------------//
uint16_t database_get_key_int(database_keys_t key) {
esp_err_t result = ESP_OK;
char* key_str = NULL;

switch(key) {
case DATABASE_USER_CNT:
        key_str = (char *)database_user_cnt_key;
        break;
case DATABASE_ADMIN_CNT:
        key_str = (char *)database_admin_cnt_key;
        break;
}

uint16_t value = storage_nvs_get_u16_value(key_str, &result);

if (result != ESP_OK) {
        ESP_LOGE(TAG, "can't get key: %s", key_str);
        return 0;
}

return value;
}

//-------------------------------------------------------------------------//
esp_err_t database_set_admin_key(const char* key) {
return storage_nvs_set_value("DB_KEY", key);
}

//-------------------------------------------------------------------------//
char* database_get_admin_key(void) {
esp_err_t result = ESP_OK;
```

```
	return storage_nvs_get_value("DB_KEY", &result);
	}

	//-------------------------------------------------------------------------//
	uint16_t database_get_admin_id(void) {

	database_user_t find_user;
	uint16_t id = storage_nvs_get_first_id();
	ESP_LOGI(TAG, "storage_nvs_get_first_id: %"PRIu16"", id);

	if (database_get_user(id, &find_user) != true) {
		ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"", id);
		return false;
	}

	while (!(find_user.role == ADMIN && find_user.active)) {

		id = storage_nvs_get_next_id(id);

		if (database_get_user(id, &find_user) != true) {
			ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"",
id);
			return false;
		}
	}

	ESP_LOGI(TAG, "First active admin id: %"PRIu16"", id);
	return id;
	}

	uint8_t database_get_role(uint16_t id) {

	database_user_t find_user;

	if (database_get_user(id, &find_user) != true) {
		ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"", id);
		return false;
	}
```

```
	return find_user.role;
	}

	//-------------------------------------------------------------------------//
	bool database_check_admin_id(uint16_t admin_id, database_user_t*
find_user) {

	uint16_t id = storage_nvs_get_first_id();

	if (database_get_user(id, find_user) != true) {
		ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"", id);
		return false;
	}

	while (1) {
		if (find_user->role == ADMIN && find_user->active) {
			if (id != admin_id) {
				ESP_LOGI(TAG, "active admin id: %"PRIu16"", id);
				break;
			}
		}

		id = storage_nvs_get_next_id(id);
		ESP_LOGI(TAG, "next id: %"PRIu16"", id);

		if (database_get_user(id, find_user) == false) {
			ESP_LOGE(TAG, "can't get user data with id: %"PRIu16"",
id);
			return false;
		}
	}

	return true;
	}

	//-------------------------------------------------------------------------//
	esp_err_t database_check_id(uint16_t id) {
```

```
size_t size = 0;
char id_str[16] = { 0 };
snprintf(id_str, sizeof(id_str), "%"PRIu16"", id);

return storage_nvs_check_blob(id_str, &size);
}

//-------------------------------------------------------------------------//
bool database_check_active(void) {
esp_err_t result;
bool active = storage_nvs_get_u8_value("active", &result);

return ((result == ESP_OK) && active);
}

//-------------------------------------------------------------------------//
void ASC_database_init(void) {
ESP_LOGI(TAG, "init");
}
```

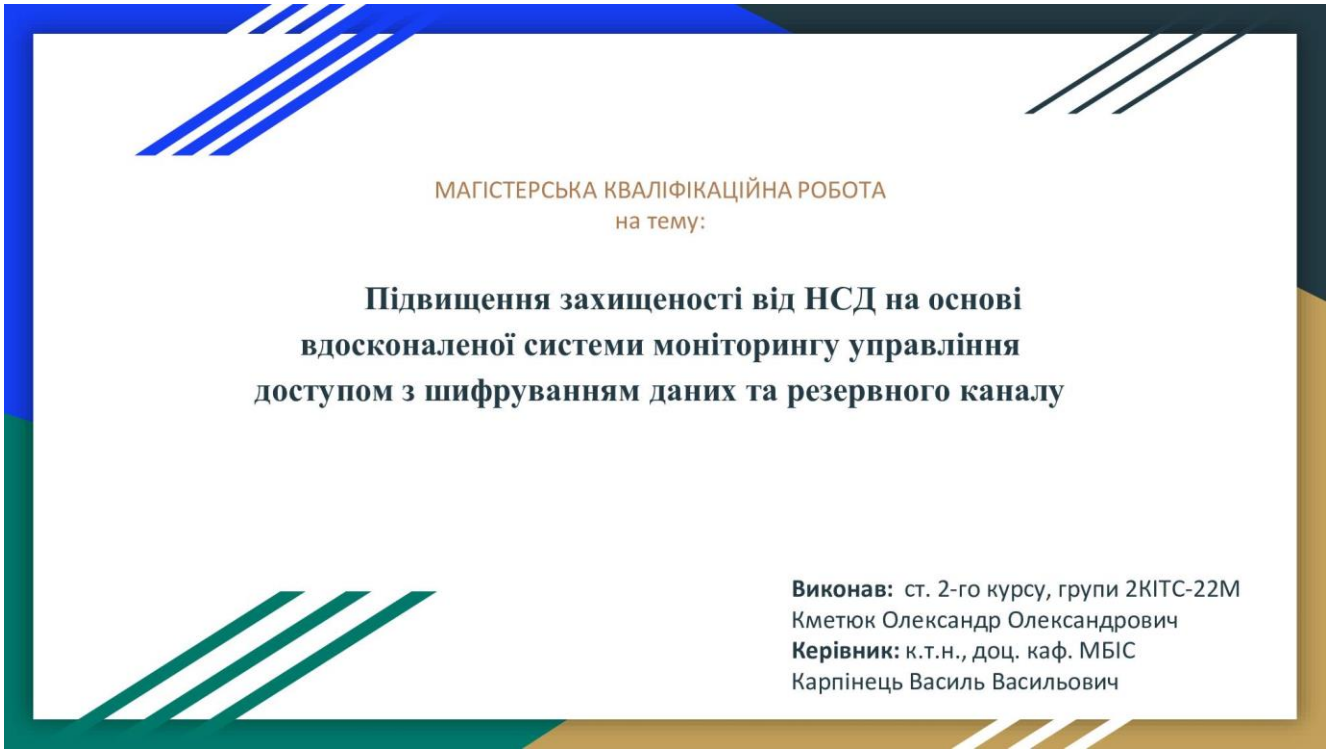
Додаток В. Лістинг файлу cmdline

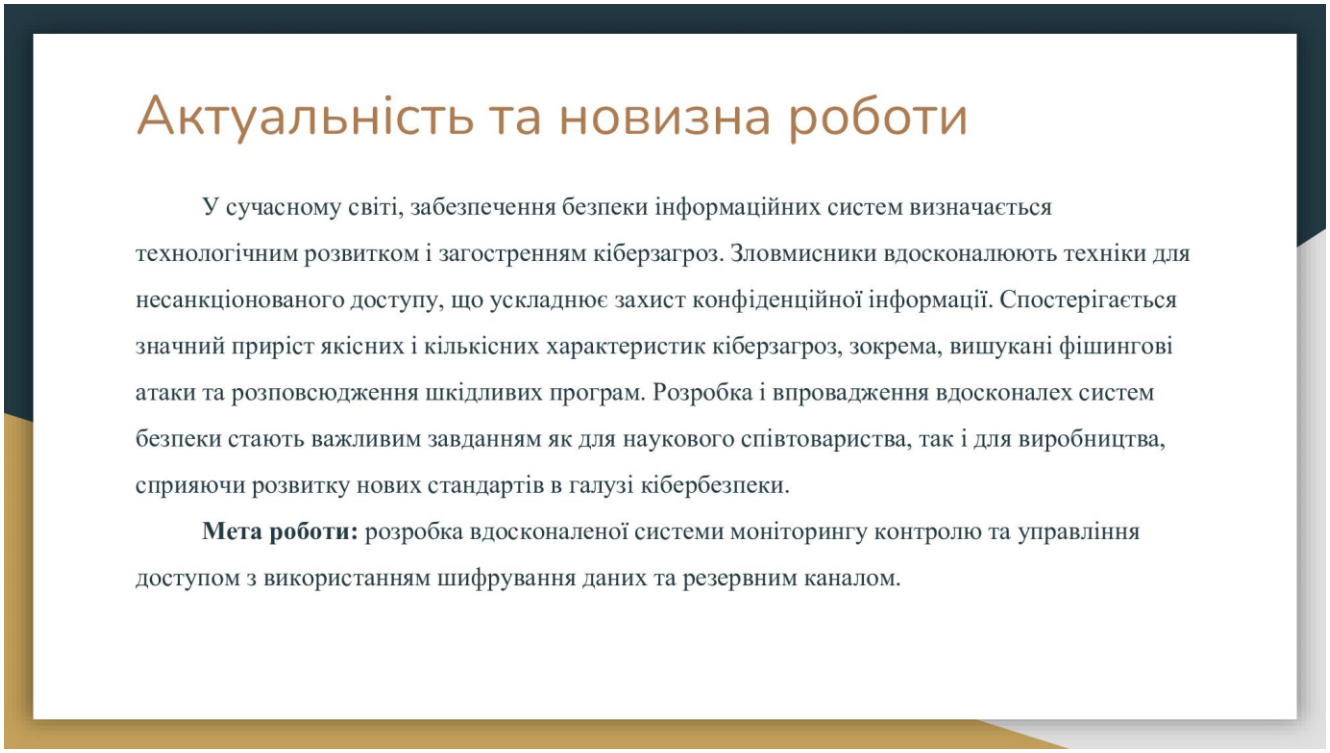
```
#include "cmdline.h"

//-------------------------------------------------------------------------//
static const char *TAG = "cmdline";

//-------------------------------------------------------------------------//
static void cmdline_commands_init(void) {
cmd_system_registr();
cmd_nvs_register();
cmd_ota_register();
cmd_proc_register();
cmd_relay_register();
}

//-------------------------------------------------------------------------//
static void cmdline_task(void *parameters) {

cmdline_commands_init();
esp_console_register_help_command();

const char *prompt = LOG_COLOR(LOG_COLOR_PURPLE) "asc> "
LOG_RESET_COLOR;

ESP_LOGW(TAG, "\n"
        "Type 'help' to get the list of commands.\n"
        "Press TAB when typing command name to auto-
complete.\n");

int probe_status = linenoiseProbe();

if (probe_status) {
    ESP_LOGW(TAG, "\n"
            "Your terminal application does not support escape
sequences.\n"
```

```
                "Line editing and history features are disabled.\n"
                "On Windows, try using Putty instead.\n");
        linenoiseSetDumbMode(1);
        prompt = "asc> ";
    }

    for (;;) {
        char *line = linenoise(prompt);
        if (line == NULL) {
            continue;
        }

        int ret;
        esp_err_t err = esp_console_run(line, &ret);
        if (err == ESP_ERR_NOT_FOUND) {
            ESP_LOGW(TAG, "Unrecognized command\n");
        } else if (err == ESP_ERR_INVALID_ARG) {
            ESP_LOGW(TAG, "Invalid argument in command\n");
        } else if (err == ESP_OK && ret != ESP_OK) {
            ESP_LOGE(TAG, "Command returned non-zero error code:
0x%x\n", ret);
        } else if (err != ESP_OK) {
            ESP_LOGE(TAG, "Internal error: 0x%x\n", err);
        }

        linenoiseFree(line);
    }
    vTaskDelete(NULL);
    }
    //-------------------------------------------------------------------------//
    void cmdline_proc(const char *cmd) {
    int ret;
    esp_err_t err = esp_console_run(cmd, &ret);
    if (err == ESP_ERR_NOT_FOUND) {
        ESP_LOGW(TAG, "Unrecognized command\n");
    } else if (err == ESP_ERR_INVALID_ARG) {
        ESP_LOGW(TAG, "Invalid argument in command\n");
    } else if (err == ESP_OK && ret != ESP_OK) {
```

```
                ESP_LOGE(TAG, "Command returned non-zero error code:
0x%x\n", ret);
        } else if (err != ESP_OK) {
                ESP_LOGE(TAG, "Internal error: 0x%x\n", err);
        }
        }

        //-------------------------------------------------------------------//
        void asc_cmdline_init(void) {
        setvbuf(stdin, NULL, _IONBF, 0);
        setvbuf(stdout, NULL, _IONBF, 0);

        esp_vfs_dev_uart_port_set_rx_line_endings(0,
ESP_LINE_ENDINGS_CR);
//esp_vfs_dev_uart_set_rx_line_endings(ESP_LINE_ENDINGS_CR); //
        esp_vfs_dev_uart_port_set_tx_line_endings(0,
ESP_LINE_ENDINGS_CRLF);//esp_vfs_dev_uart_set_tx_line_endings(ESP_LI
NE_ENDINGS_CRLF); //

        //ESP_ERROR_CHECK(uart_driver_install(CONFIG_CONSOLE_UART_
NUM, 256, 0, 0, NULL, 0));
        //esp_vfs_dev_uart_use_driver(CONFIG_CONSOLE_UART_NUM);

        ESP_ERROR_CHECK(uart_driver_install(0, 256, 0, 0, NULL, 0));
        esp_vfs_dev_uart_use_driver(0);
        esp_console_config_t console_config = {
                        .max_cmdline_args = 8,
                        .max_cmdline_length = 256,
                        .hint_color = atoi(LOG_COLOR_CYAN)
        };
        ESP_ERROR_CHECK(esp_console_init(&console_config));
        linenoiseSetMultiLine(1);
        linenoiseSetCompletionCallback(&esp_console_get_completion);
        linenoiseSetHintsCallback((linenoiseHintsCallback*)
&esp_console_get_hint);

        xTaskCreate(&cmdline_task, "cmdline", 4 * 1024, NULL, 8, NULL);
        }
```

Додаток Г. Ілюстративний матеріал





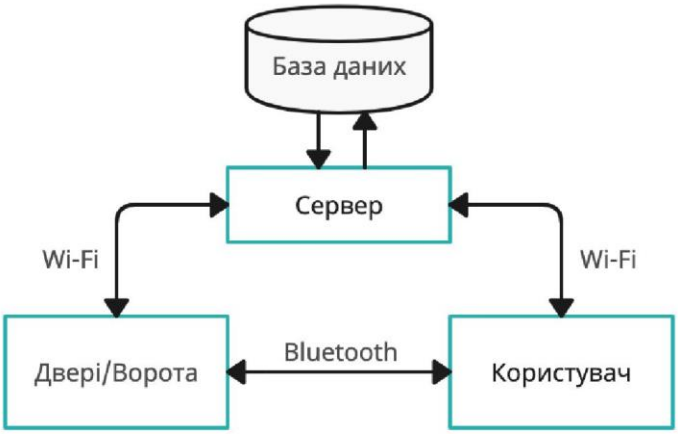
Система контролю та управління доступом

Система контролю та управління доступом (СКУД) - це комплексна система, яка забезпечує контроль та обмеження доступу осіб до певних приміщень, територій або ресурсів. Основна мета СКУД полягає в забезпеченні фізичної безпеки об'єктів або інформації, регулюванні руху людей та створенні системи моніторингу за подіями на контрольованій території.

Основні компоненти СКУД:
– Електронні замки;
– Ключ (картки/біометричні сканери/мобільний додаток/магнітні ключі);
– Датчики;
– Програмне забезпечення.

Системи контролю доступу можуть бути встановлені в офісах, промислових підприємствах, житлових будинках, банках та інших об'єктах з метою забезпечення безпеки та контролю за доступом.

Скуд із можливістю дистанційного керування за допомогою мобільного додатку



Аналіз можливостей вдосконалення

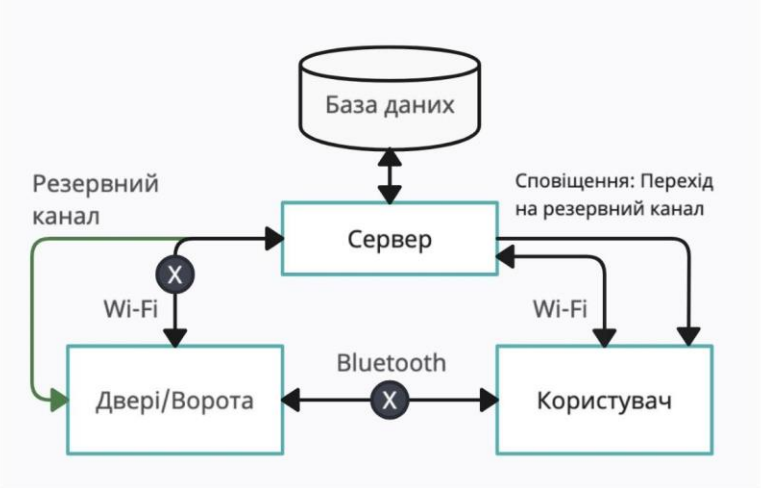
Резервний Канал:

– Розробка та імплементація надійного резервного каналу для забезпечення безперебійності роботи системи навіть при можливих викликах чи неполадках в основному каналі.

Шифрування Даних:

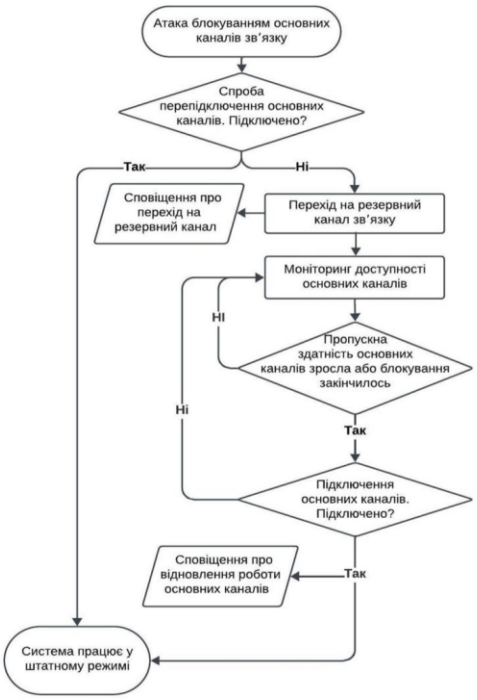
– Використання сучасних шифрувальних методів для захисту конфіденційної інформації від несанкціонованого доступу та забезпечення конфіденційності даних.

Схема роботи вдосконаленої СКУД із резервним каналом



Алгоритм роботи системи СКУД з резервним каналом

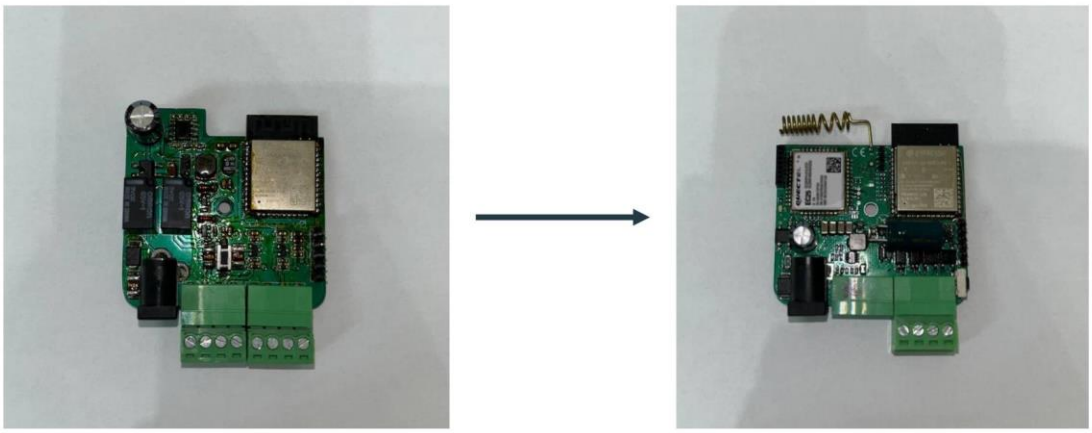
1. Виявлення блокування основних каналів;
2. Перехід на резервний канал;
3. Ініціація сповіщень та аналіз ситуації;
4. Збереження журналу інцидентів;
5. Відновлення основного зв'язку.



Реалізація апаратної частини резервного каналу

Мережева підтримка	GSM/GPRS/EDGE: 850/900/1800/1900 МГц WCDMA: B1/B2/B5/B8 LTE FDD: B1/B3/B7/B8/B20 LTE TDD: B38/B40/B41
Швидкість передачі даних	LTE Cat 4 (до 150 Мбіт/с вниз, до 50 Мбіт/с вгору) HSPA+ (до 42 Мбіт/с вниз, до 5.76 Мбіт/с вгору)
Інтерфейси	USB 2.0 High-Speed UART, I2C, GPIO, PCM, etc.
Підтримка GNSS:	GPS, GLONASS, BeiDou, Galileo
SIM-карта	1.8V/3V
Робоча температура	Від -40°C до +85°C
Розміри	32 мм × 29 мм × 2.4 мм
Підтримка ОС	Windows 7/8/8.1/10, Linux, Android, eCall
Живлення	Вхідна напруга: 3.4V - 4.2V Режим сну: менше 10 мкА
Інші особливості	Вбудований TCP/IP stack Режим віддаленого відладки Підтримка AT-команд

Інтеграція GSM модему в попередньо розроблену СКУД на основі чипу ESP32



Тестування вдосконаленої системи

```
I (2032) ble: init
I (2032) BLE_INIT: BT controller compile version [963cad4]
I (2042) phy_init: phy_version 601,98f2a71,Jun 29 2023,09:58:12
I (2072) BLE_INIT: Bluetooth MAC: 34:85:18:46:e1:ee

I (2092) ble: GATTS_REG_EVT, status 0, app_id 0
I (2092) ble: GATTS_CREATE_EVT, status 0, service_handle 40
I (2092) ble: GATTS_START_EVT, status 0, service_handle 40
I (2102) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 42, service_handle 40
I (2112) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 44, service_handle 40
I (2122) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 46, service_handle 40
I (2122) ble: GATTS_ADD_CHAR_EVT, status 0,  attr_handle 48, service_handle 40
I (2132) ble: GATTS_ADD_CHAR_DESCR_EVT, status 0, attr_handle 49, service_handle 40
```

Ініціалізація основного каналу (Bluetooth)

Тестування вдосконаленої системи

```
I (2302) wifi: init
I (2302) wifi:mode : sta (34:85:18:46:e1:ec)
I (2302) wifi:enable tsf
I (2312) wifi: started
I (4722) wifi:new:<11,2>, old:<1,0>, ap:<255,255>, sta:<11,2>, prof:1
I (5452) wifi:state: init -> auth (b0)
I (5452) wifi:state: auth -> assoc (0)
I (5462) wifi:state: assoc -> run (10)
I (5572) wifi:connected with TP-Link_30FC, aid = 1, channel 11, 40D, bssid = 0c:80:63:c0:30:fc
I (5572) wifi:security: WPA2-PSK, phy: bgn, rssi: -65
I (5592) wifi:pm start, type: 1

I (5592) wifi:set rx beacon pti, rx_bcn_pti: 14, bcn_timeout: 25000, mt_pti: 14, mt_time: 10000
I (5602) wifi:<ba-add>idx:0 (ifx:0, 0c:80:63:c0:30:fc), tid:0, ssn:2, winSize:64
I (5622) wifi:AP's beacon interval = 102400 us, DTIM period = 1
I (7092) esp_netif_handlers: sta ip: 192.168.0.109, mask: 255.255.255.0, gw: 192.168.0.1
I (7092) wifi: connect, got ip: 192.168.0.109
I (7102) lokkyy: connect to WIFI
I (7102) mqtt: other event id:7
I (7102) wifi: rssi: -64
I (7102) wifi: connected to ap SSID:TP-Link_30FC password:83738791
```

Ініціалізація основного каналу (Wi-Fi)

Тестування вдосконаленої системи

```
I (152282) wifi:<ba-del>idx:0, tid:0
I (152282) wifi:new:<11,0>, old:<11,2>, ap:<255,255>, sta:<11,2>, prof:1
E (152292) esp-tls: [sock=55] delayed connect error: Software caused connection abort
I (152292) wifi: disconnect
E (152302) transport_base: Failed to open a new connection: 32772
E (152312) mqtt_client: Error transport connect
I (152312) mqtt: MQTT_EVENT_ERROR
I (152312) mqtt: MQTT_EVENT_DISCONNECTED
I (152322) lokkyy: MQTT client not connect
E (152292) esp-tls: [sock=54] delayed connect error: Software caused connection abort
I (152302) lokkyy: not connect to WIFI
E (152332) transport_base: Failed to open a new connection: 32772
E (152352) mqtt_client: Error transport connect
I (152352) mqtt: MQTT_EVENT_ERROR
I (152362) mqtt: MQTT_EVENT_DISCONNECTED
I (152362) lokkyy: MQTT client not connect
I (152332) mqtt: disconnect
```

Атака на систему блокуванням основного каналу зв’язку

Тестування вдосконаленої системи

```
I (23767) pppos_client: Module Name=SIMCOM_SIM800C
I (23867) pppos_client: Product Name and Release information: SIM800 R14.18
I (23967) pppos_client: Product Revision information: Revision:1418B10SIM800C24_TLS12
I (24067) pppos_client: Product Serial Number: 869627034683896
I (24167) pppos_client: Voltage: 4120 mV, bcs=0, bcl=89
I (24267) pppos_client: SIM Card inserted
I (24367) pppos_client: IMSI=255011673154378
I (24467) pppos_client: IMEI=869627034683896
I (24567) pppos_client: Operator Name=UMC, 1007778424
I (24667) pppos_client: Mobile Subscriber: 255011673154378
I (24767) pppos_client: Signal quality: rssi -79dbm, rssi value 17, ber 0
I (25017) pppos_client: Waiting for IP address
I (25017) pppos_client: LED state: LED_GSM_WAITING_FOR_IP...
I (25017) gptimer: Stop gptimer
I (25027) gptimer: Start gptimer with led state: LED_GSM_WAITING_FOR_IP
I (31757) esp-netif_lwip-ppp: Connected
I (31757) pppos_client: Modem Connect to PPP Server
I (31757) pppos_client: ~~~~~~~~~~~~~~
I (31767) pppos_client: IP          : 10.142.120.9
I (31767) pppos_client: Netmask     : 255.255.255.255
I (31777) pppos_client: Gateway     : 192.168.254.254
I (31777) pppos_client: Name Server1: 80.255.64.23
I (31797) pppos_client: Name Server2: 80.255.64.24
I (31797) pppos_client: ~~~~~~~~~~~~~~
```

Успішний перехід системи на резервний канал зв’язку

Результати тестування

З виведених системних даних у терміналі видно, що в результаті атаки, яка полягала в блокуванні Wi-Fi сигналу, вдосконалена система успішно активувала резервний канал та встановила з'єднання, обходячи блокування Wi-Fi. Цей успішний сценарій свідчить про ефективність механізму резервного каналу.

З врахуванням цього результату можна зробити висновок, що система демонструє надійну працездатність та здатність вчасно реагувати на потенційні загрози, такі як блокування основного каналу зв’язку.

Результати роботи

У результаті вивчення та вдосконалення систем контролю та управління доступом, дана робота виокремила нові можливості для забезпечення високого рівня захисту від несанкціонованого доступу. Розроблена вдосконалена система моніторингу управління доступом, разом з інтеграцією резервного каналу та шифруванням даних, визначає новий стандарт у розробці безпеки, створюючи міцну платформу для подальших інновацій та досліджень в цій важливій галузі.

Додаток Д. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Підвищення захищеності від НСД на основі вдосконаленої системи моніторингу управління доступом з шифруванням даних та резервного каналу

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 97 % Схожість 3 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Коваль Н.І.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Кметюк О.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Карпінець В.В.
(підпис) (прізвище, ініціали)