Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес
Назва теми

КвРКІ 210485.21.04.34 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2-21-4 _____ Дмитро КОБИЛЬЧУК
Підпис, Ініціали, прізвище

Керівник _____ Олексій ІВАНОВ
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис, Ініціали, прізвище

«___» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Дмитру КОБИЛЬЧУКУ
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес
Керівник проекту (роботи) Олексій ІВАНОВ, к.т.н., доцент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес
Проєктування кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес
Програмно-апаратна реалізація кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Архітектура кіберфізичної системи
Архітектура валідацій MAC-адрес
Архітектура асинхронного пінгування
Код програмного забезпечення

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «_10_»_____01_____2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2025	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2025	виконано
4	Робота над розділом 2 – вибір компонентів для проєктування автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес	01.04.2025	виконано
5	Робота над розділом 3 – автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес	29.04.2025	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2025	виконано
7	Попередній захист ВКР	26.05.2025	виконано
8	Захист ВКР на засіданні ЕК	Червень 2025 року	

Студент _____ Дмитро КОБИЛЬЧУК
Підпис Ініціали, прізвище

Керівник роботи _____ Олексій ІВАНОВ
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 210485.21.04.34 ПЗ	Пояснювальна записка	58		
			Графічні матеріали			
2		КвРКІ 210485.21.04.34 Е8	Архітектура кіберфізичної системи	1		
3		КвРКІ 210485.21.04.34 Е8	Архітектура ПЗ для кіберфізичної системи	1		
4		КвРКІ 210485.21.04.34 Е8	Апаратне забезпечення проєкту	1		

КвРКІ 210485.21.04.34 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Кобильчук		12.06.25
Перевір.		Іванов		12.06.25
Н. контр.		Кисіль		12.06.25
Затв.		Павлова		12.06.25

Відомість проекту

Літера	Аркуш	Аркушів
У	1	58

ХНУ, КІ2-21-4

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес».

Автор роботи: Дмитро КОБИЛЬЧУК.

Керівник роботи: Іванов Олексій Валентонович.

Пояснювальна записка: 56 с., 7 рис., 1 табл., 4 дод., 51 джерел.

Графічна частина: креслення, код програмного забезпечення.

MAC-АДРЕСА, WI-FI МЕРЕЖА, АВТОМАТИЗАЦІЯ, КІБЕРФІЗИЧНА СИСТЕМА, КОНТРОЛЬ ДОСТУПУ

Метою даної кваліфікаційної роботи є розробка та дослідження кіберфізичної системи, яка автоматизує процес реєстрації користувачів у Wi-Fi мережах шляхом ідентифікації їхніх пристроїв за унікальними MAC-адресами. У роботі визначено основні вимоги до такої системи, зокрема забезпечення надійної, швидкої та безпечної автентифікації, а також можливість масштабування й інтеграції з існуючою інфраструктурою бездротового зв'язку.

Об'єктом дослідження виступають процеси автоматизації реєстрації та управління доступом у Wi-Fi мережах, а предметом методи збору, обробки і контролю інформації про підключені пристрої на основі аналізу MAC-адрес. Особлива увага приділяється розробці апаратно-програмного рішення, яке включає використання кіберфізичних компонентів для забезпечення ефективного контролю підключень і моніторингу в режимі реального часу.

Предметом дослідження є автоматизації збору, фільтрації, обробки та візуалізації інформації про мережеві підключення з використанням MAC-адрес як основного ідентифікатора пристрою, що дозволяє реалізувати політики безпечного доступу. У роботі також досліджено засоби інтеграції системи з телеграм-ботом для оперативного сповіщення адміністратора про появу нових підключень.

Підпис студента

30.05.2025

Дата

ЗМІСТ

Зм.	Арк.	№докум.	Підпис	Дата	КвРКІ 210485.21.04.34 ПЗ		
Виконав		Дмитро КОБИЛЬЧУК			Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес Пояснювальна записка	Літера	Аркуш 2 / Аркушів 58
Перевір.		Олексій ІВАНОВ				У	
Н.контр.		Тетяна КИСІЛЬ				ХНУ КІ2-21-4	
Затвер.		Ольга ПАВЛОВА					

ВСТУП

Актуальність дослідження. У сучасному світі бездротові технології зв’язку відіграють ключову роль у забезпеченні повсякденного функціонування як побутових, так і промислових систем. Зі зростанням кількості мобільних пристроїв, сенсорів та «розумних» об'єктів зростає потреба у зручному, безпечному та автоматизованому доступі до мереж Wi-Fi. Традиційні способи реєстрації користувачів у бездротових мережах – через веб-форми, паролі чи авторизаційні портали – нерідко є незручними, уповільнюють процес підключення та створюють бар’єри в середовищах з великою кількістю тимчасових або непідготовлених користувачів.

Один із сучасних підходів до вирішення цієї проблеми – створення кіберфізичних систем, які поєднують апаратне забезпечення з програмними алгоритмами для автоматизації процесів у фізичному світі. У цьому контексті перспективним напрямком є використання унікальних апаратних ідентифікаторів пристроїв, зокрема MAC-адрес, для спрощеної ідентифікації користувачів у Wi-Fi мережах. Такий підхід дозволяє автоматизувати процес реєстрації пристроїв без необхідності участі користувача, що є особливо корисним у закладах освіти, офісах, закритих мережах підприємств, громадських місцях тощо.

З огляду на це, розробка кіберфізичної системи, яка забезпечує автоматичне виявлення нових пристроїв на основі їх MAC-адрес і приймає рішення щодо надання доступу до Wi-Fi мережі, є актуальним завданням. Така система сприятиме підвищенню зручності користування бездротовими мережами, зменшенню адміністративного навантаження, а також забезпеченню більш ефективного контролю доступу.

Мета дослідження полягає у проєктуванні та розробці кіберфізичної системи, що дозволяє автоматизувати процес реєстрації в Wi-Fi мережах на основі аналізу MAC-адрес пристроїв, із використанням сучасних апаратних і програмних засобів.

Об’єктом дослідження є процеси автоматизованої реєстрації пристроїв у

бездротових мережах.

Предметом дослідження виступають методи побудови кіберфізичних систем, що забезпечують виявлення, обробку та реагування на підключення нових пристроїв у Wi-Fi мережі на основі MAC-адрес, а також архітектурні та програмні рішення для реалізації такої системи з урахуванням вимог до безпеки, масштабованості та ефективності.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМИ

1.1 Аналіз предметної області і виявлення наявниї проблем і завдань

Сьогодні Wi-Fi мережі стали невід'ємною частиною цифрової інфраструктури як у публічному, так і в приватному середовищі. Підключення до бездротових мереж зазвичай вимагає аутентифікації користувача через Captive Portal, введення пароля або проходження ручної реєстрації. Попри поширеність цих методів, вони часто є незручними, особливо у випадках із великою кількістю нових підключень або в середовищах, де потрібен швидкий доступ до мережі (наприклад, навчальні заклади, конференції, підприємства, готелі тощо).

У більшості випадків адміністратори Wi-Fi мереж змушені вручну додавати нові пристрої до списку дозволених або видавати паролі користувачам. Такий підхід є не тільки трудомістким, а й схильним до людських помилок, недостатньо масштабованим і неефективним у середовищах з динамічною зміною користувачів.

Ключовим апаратним ідентифікатором кожного мережевого пристрою є його MAC-адреса – унікальний і незмінний номер, що призначається мережевому інтерфейсу пристрою. Саме вона може бути використана як основа для автоматичної ідентифікації пристроїв при їхньому підключенні до мережі. Відстеження та обробка MAC-адрес дозволяє реалізувати механізм автоматичної реєстрації, при якому система самостійно приймає рішення щодо надання доступу до мережі без необхідності участі користувача або адміністратора.

Однак для реалізації такого підходу виникає низка технічних і організаційних проблем:

– відсутність автоматизованих рішень для виявлення нових MAC-адрес у локальній мережі та динамічного оновлення списку дозволених пристроїв;

– необхідність інтеграції апаратних та програмних компонентів у єдину систему;

– забезпечення безпеки;

– обмеженість вбудованих засобів маршрутизаторів або точок доступу, які не завжди дозволяють гнучко налаштовувати поведінку мережі на основі зовнішніх рішень;

– відсутність уніфікованих підходів до обліку та реєстрації пристроїв у динамічних мережах з постійно змінним складом користувачів.

У контексті даного дослідження, спрямованого на проєктування та реалізацію кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес, постає необхідність чітко визначити коло ключових завдань, вирішення яких дозволить досягти поставленої мети.

Насамперед, важливо дослідити існуючі методи виявлення пристроїв у комп'ютерній мережі на основі їх унікальних ідентифікаторів – MAC-адрес. Це включає вивчення механізмів моніторингу трафіку, аналізу ARP-таблиць, прослуховування мережевого рівня та використання утиліт і протоколів, які дозволяють виявити появу нових пристроїв у локальній мережі. Особливу увагу необхідно приділити технічним обмеженням та можливостям, які надають сучасні мережеві маршрутизатори, точки доступу та програмне забезпечення з відкритим кодом.

Другою важливою задачею є розробка програмного модуля, який зможе в автоматичному режимі обробляти виявлені MAC-адреси, порівнювати їх із попередньо сформованими списками дозволених або заборонених пристроїв, вести реєстрацію нових адрес у базі даних та, в залежності від заданої логіки, приймати рішення щодо надання або обмеження доступу до Wi-Fi мережі. Цей компонент повинен працювати автономно, з мінімальною участю адміністратора, і бути здатним до інтеграції з мережею через доступні API або інтерфейси керування мережевим обладнанням.

Третє завдання полягає у побудові загальної архітектури кіберфізичної системи, яка поєднує апаратні елементи (наприклад, Raspberry Pi, мережеві сканери, сервери зберігання даних тощо) та програмне забезпечення (сервіси виявлення пристроїв, обробки MAC-адрес, інтерфейс адміністратора тощо). Така

система повинна мати модульну структуру, що дозволить легко масштабувати її залежно від кількості пристроїв у мережі, забезпечувати резервування основних компонентів та гнучко налаштовувати сценарії обробки підключень.

Четвертим важливим аспектом є забезпечення безпечної та надійної взаємодії між усіма складовими системи. Необхідно передбачити механізми автентифікації та авторизації доступу до адміністративного інтерфейсу, захисту передаваних даних, виявлення підозрілих MAC-адрес, які можуть бути результатом MAC-спуфінгу, та інші елементи кібербезпеки. Окрім цього, система повинна бути масштабованою, щоб підтримувати стабільну роботу у випадках значного збільшення кількості підключених пристроїв або зростання запитів до сервера обробки.

Останнім етапом є реалізація працездатного прототипу кіберфізичної системи, який можна буде протестувати у реальному або наближеному до реального середовищі. Такий прототип має довести життєздатність обраного підходу, ефективність автоматичної реєстрації пристроїв, а також продемонструвати, що запропоноване рішення справді дозволяє мінімізувати участь людини у процесі адміністрування доступу до Wi-Fi мережі. Успішна реалізація цих етапів відкриє перспективи для подальшого вдосконалення системи, її комерціалізації або масштабування на більш широке коло застосувань (рис 1.1).

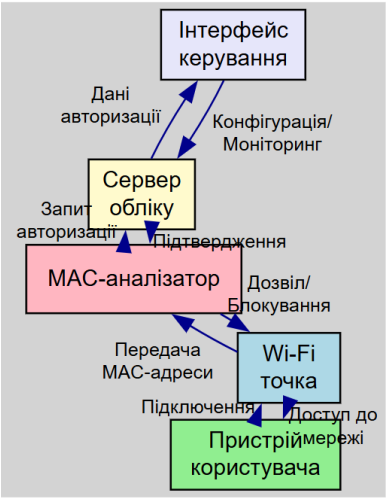


Рисунок 1.1 – Схема архітектури кіберфізичної системи

Сукупне вирішення зазначених завдань дозволить створити інноваційну, гнучку та ефективну кіберфізичну систему, орієнтовану на автоматизацію мережевих процесів та підвищення зручності як для користувачів, так і для адміністраторів інфраструктури.

Окрім вищезазначених технічних завдань, важливо розглянути і соціальні, організаційні та практичні аспекти впровадження подібної кіберфізичної системи у реальні умови експлуатації. Система автоматичної реєстрації на основі MAC-адрес може бути надзвичайно корисною не лише в контексті оптимізації адміністрування мереж, а й у питаннях обліку, аналітики та моніторингу активності пристроїв у мережі. Встановлення чіткої відповідності між MAC-адресою і конкретним користувачем (наприклад, студентом, працівником або відвідувачем) дозволяє створити ефективну модель контролю та звітності, що особливо актуально в освітніх установах, урядових структурах, корпоративних офісах та медичних закладах.

Крім того, така система може бути розширена для реалізації різних політик доступу, залежно від типу користувача, часу підключення, рівня привілеїв або навіть географічного розташування всередині будівлі. Наприклад, пристрої співробітників можуть автоматично отримувати доступ до внутрішньої мережі, тоді як гостьові пристрої – лише до обмеженого сегменту інтернету. Застосування таких політик підвищує як рівень безпеки, так і зручність для користувачів.

Також система може бути інтегрована з іншими сервісами – наприклад, з електронною системою пропусків, внутрішньою CRM або ERP-системою, що дозволяє не лише контролювати доступ, а й формувати розширену аналітику щодо переміщення користувачів, їхньої присутності в офісі чи навчальному закладі, активності в мережі тощо. Така інформація може бути особливо цінною для аналітичних цілей, планування ресурсів, оптимізації робочого простору або навіть при розслідуванні інцидентів безпеки.

Окремо варто згадати потенціал впровадження елементів штучного інтелекту для покращення роботи системи. Зокрема, алгоритми машинного навчання можуть

бути використані для виявлення аномальної поведінки пристроїв, передбачення мережевого навантаження, автоматичного коригування політик доступу залежно від історії підключень або навіть виявлення потенційних атак типу "rogue device". Застосування таких технологій дозволяє зробити систему не лише реактивною, а й проактивною – тобто здатною запобігати проблемам ще до їхнього виникнення.

Із врахуванням сучасних тенденцій у галузі кібербезпеки та розвитку концепцій Smart City, Smart Campus та Industrial Internet of Things (IIoT), описувана система має потенціал для масштабування на ширші інфраструктури. Наприклад, у розумних містах вона може стати складовою частиною системи обліку та ідентифікації пристроїв, які підключаються до муніципальних Wi-Fi мереж (рис 1.2). У промислових об'єктах – використовуватись для контролю пристроїв у внутрішній мережі виробничих ліній, забезпечуючи ізоляцію критичних систем від неавторизованих підключень.

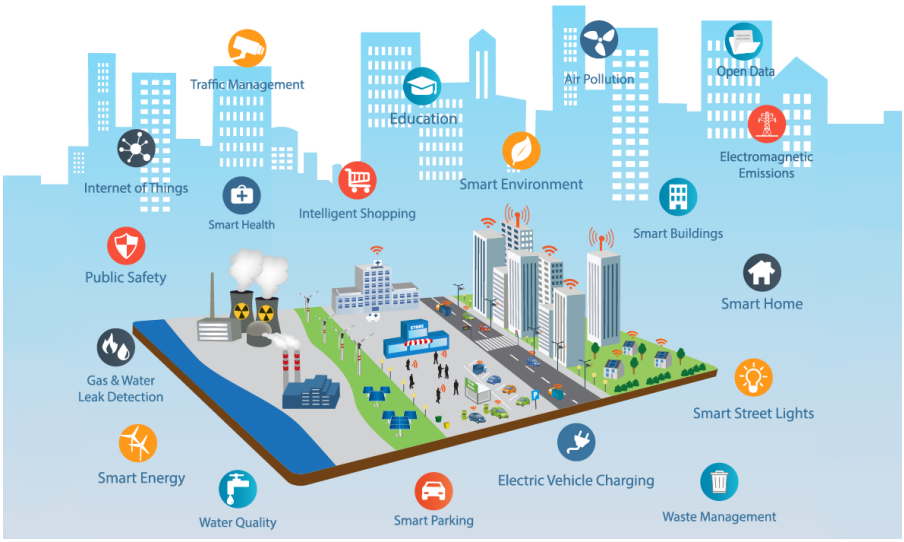


Рисунок 1.2 – Wi-Fi в публічному просторі [1]

З технічної точки зору, також слід розглядати можливість реалізації цієї системи на базі контейнеризації (Docker, Kubernetes), що забезпечить кращу портативність, масштабованість і спрощене розгортання на різних апаратних платформах. Такий підхід дозволить адміністратору обслуговувати систему з мінімальними зусиллями, використовуючи централізоване керування та

можливість віддаленого оновлення компонентів системи.

Крім того, необхідно враховувати законодавчі та етичні аспекти, пов’язані з обробкою персональних даних. Оскільки MAC-адреса може вважатися ідентифікатором пристрою користувача, потрібно реалізувати функції, які забезпечать відповідність системи вимогам таких нормативних актів, як GDPR (у Європейському Союзі) або аналогічних у національному законодавстві. Це включає реалізацію прозорої політики конфіденційності, збереження журналів дій із зазначенням мети обробки, а також можливість видалення персональних даних за запитом користувача.

Загалом, впровадження системи автоматичної реєстрації пристроїв у Wi-Fi мережі на основі MAC-адрес – це крок до створення самокерованої, інтелектуальної мережевої інфраструктури. Така система зменшує навантаження на адміністратора, підвищує рівень безпеки, зручність доступу та дозволяє реалізовувати нові сервіси та функції, які раніше були неможливі або економічно необґрунтовані. У перспективі, поєднання такої системи з іншими компонентами кіберфізичного простору може стати основою для розвитку цілісних інтелектуальних середовищ – від окремих організацій до цілих міст.

Дане дослідження має не лише прикладну цінність, а й стратегічне значення для розвитку мережевої автоматизації, кібербезпеки та цифрової трансформації інфраструктури у різних сферах життя.

З метою подальшого вдосконалення системи та її практичної цінності, доцільно також розглянути можливість інтеграції зі сторонніми сервісами та платформами. Зокрема, система може бути доповнена можливістю обміну інформацією з корпоративними базами даних, CRM-системами, платформами аналітики або безпековими службами для побудови більш повного профілю користувача або пристрою. Це відкриває шлях до створення адаптивної системи доступу, яка не лише автоматично реєструє пристрої, а й адаптує параметри доступу на основі контексту – наприклад, часу підключення, геолокації, ролі користувача чи рівня ризику.

Крім того, подальший розвиток може включати машинне навчання або алгоритми штучного інтелекту для виявлення аномальної поведінки пристроїв у мережі, формування поведінкових шаблонів користувачів та вчасного реагування на потенційні загрози. Такі алгоритми здатні самостійно визначати підозрілі MAC-адреси, виявляти спроби обходу системи через підміну ідентифікаторів та пропонувати рішення для блокування або додаткової перевірки.

Іншим перспективним напрямом є реалізація централізованого хмарного сервісу керування мережею з можливістю віддаленого моніторингу та адміністрування декількох об’єктів одночасно. Це дозволить застосовувати систему не лише на окремих майданчиках, а й у великих організаціях, мережах філій або навіть у міських Wi-Fi-мережах. Такий сервіс зможе автоматично оновлювати політики доступу, отримувати оновлення системи безпеки, об’єднувати статистику з різних джерел та підвищувати загальний рівень керованості інфраструктурою.

Важливим етапом розвитку також є формування користувацького інтерфейсу з розширеними можливостями – візуалізацією трафіку, журналами подій, сповіщеннями у реальному часі, дашбордом адміністрування та інтуїтивно зрозумілим механізмом ручного втручання у виняткових випадках. Такий інтерфейс дозволить адміністраторам оперативно реагувати на події в мережі, відстежувати ефективність автоматизації та здійснювати базову підтримку користувачів без необхідності глибокого технічного втручання.

Загалом, запропонована система здатна не лише оптимізувати процес реєстрації в Wi-Fi мережі, а й слугувати базовим елементом для побудови розумної мережевої інфраструктури, орієнтованої на автономне функціонування, самонавчання, безпеку та масштабованість. У майбутньому такі системи можуть стати стандартом для організацій, які прагнуть зменшити витрати на IT-підтримку, підвищити рівень захищеності мережі та забезпечити зручність користування для широкого кола кінцевих користувачів.

Аналіз предметної області демонструє, що впровадження такої системи

дозволить значно знизити витрати часу на адміністрування мережі, підвищити зручність для користувачів та покращити загальну ефективність функціонування Wi-Fi інфраструктури.

1.2 Порівняльна оцінка переваг і обмежень наявних систем

У сучасних бездротових мережах реєстрація користувачів залишається критично важливим етапом як з точки зору безпеки, так і з боку зручності користування. Існують різноманітні підходи до ідентифікації користувача у Wi-Fi мережах, серед яких найбільш поширеними є портална авторизація (так званий «Captive Portal»), авторизація через сервери Radius із застосуванням протоколу WPA2-Enterprise, а також статичне додавання MAC-адрес пристроїв до білого списку маршрутизатора або контролера доступу. Кожен із цих підходів має як очевидні переваги, так і суттєві обмеження, що зумовлює потребу у впровадженні нових рішень, зокрема, кіберфізичних систем, які здатні поєднати фізичний рівень доступу до мережі з цифровими засобами обліку та автоматичного керування.

Портальна авторизація є найбільш розповсюдженим методом ідентифікації користувачів у публічних мережах, зокрема в закладах громадського харчування, готелях, торговельних центрах тощо. Користувач підключається до відкритої мережі, після чого перенаправляється на веб-сторінку, де вводить свої дані або приймає умови доступу. Незважаючи на простоту реалізації, такий підхід має ряд обмежень. По-перше, процес не є автоматизованим: кожне підключення вимагає дій від користувача. По-друге, такий механізм не гарантує високого рівня безпеки, оскільки ідентифікація здійснюється лише на рівні HTTP-запиту, що може бути скомпрометовано. Нарешті, багато користувачів вважають цей спосіб незручним, особливо при повторному підключенні.

Складніший, але й більш захищений метод полягає у впровадженні авторизації через протокол WPA2-Enterprise з використанням сервера Radius. У такому випадку кожен користувач має персоніфіковані облікові дані, які

перевіряються під час підключення до мережі. Цей варіант забезпечує високий рівень безпеки та дозволяє централізовано керувати доступом. Проте налаштування такої системи потребує значних технічних знань, додаткового серверного обладнання та програмного забезпечення. Крім того, з боку користувача часто потрібне додаткове конфігурування пристрою, що може бути неприйнятним в умовах динамічного середовища або для непідготовленої аудиторії.

Найпростішим з технічної точки зору способом контролю доступу є використання білого списку MAC-адрес. У цьому випадку маршрутизатор або точка доступу дозволяє підключення лише для попередньо дозволених пристроїв. Цей спосіб можна вважати певною мірою «автоматизованим», однак лише у випадку обмеженого кола користувачів. Він не передбачає жодного гнучкого керування: усі зміни потрібно вносити вручну. До того ж, MAC-адресу легко змінити або підробити, тому цей спосіб не може вважатися надійним засобом аутентифікації. У великих або відкритих мережах такий метод втрачає свою ефективність і перетворюється на джерело адміністративного клопоту.

Запропонована кіберфізична система автоматизації реєстрації у Wi-Fi мережах на основі MAC-ідентифікації намагається об'єднати переваги попередніх підходів і при цьому усунути їхні ключові недоліки. На відміну від класичних систем, вона передбачає автоматичне виявлення нових пристроїв у мережі без необхідності участі користувача. На фізичному рівні працює окремий пристрій-агент, наприклад, на базі Raspberry Pi, який постійно здійснює моніторинг ARP- або DHCP-повідомлень у локальній мережі. Виявлені MAC-адреси передаються до централізованої бази даних, де може бути реалізовано подальший аналіз, фільтрацію, блокування чи дозвіл доступу.

Однією з найсуттєвіших переваг запропонованої системи є можливість логування активності без залучення користувача до процесу. Це особливо актуально для організацій, де важливо не лише надати доступ до мережі, а й мати змогу відстежити, які пристрої підключалися, коли саме і з якою інтенсивністю

використовували ресурси. Така система також дозволяє виявляти нові або підозрілі пристрої у режимі реального часу, оперативно реагувати на загрози або порушення політики безпеки.

Однак повністю бездоганним це рішення назвати не можна. Основним ризиком залишається можливість MAC-spoofing – підміни MAC-адреси зловмисником. У цьому випадку система повинна мати додаткові механізми перевірки пристрою, наприклад, через зіставлення MAC з іншими ознаками або впровадження додаткової аутентифікації при першому підключенні. Також для функціонування системи потрібно мати окремий пристрій у мережі та програмне забезпечення, що збільшує складність початкового впровадження.

Класичні підходи до реєстрації в Wi-Fi мережах є або надто простими і небезпечними, або занадто складними та малопридатними для широкого використання в динамічному середовищі. У цьому контексті запропонована кіберфізична система є компромісним, але перспективним рішенням, що дозволяє досягти балансу між автоматизацією, масштабованістю та контролем. Вона відкриває можливість для подальшої інтеграції з іншими інформаційними системами, побудови аналітики на основі мережевих даних і покращення цифрової безпеки в організаціях, навчальних закладах, коворкінгах та інших середовищах.

1.3 Підходи до вирішення задачі за темою дослідження

У процесі розробки ефективної кіберфізичної системи для автоматизації реєстрації у Wi-Fi мережах на основі MAC-ідентифікації необхідно враховувати як технічні обмеження бездротової інфраструктури, так і потреби користувача та адміністратора мережі. Сутність запропонованого підходу полягає в інтеграції апаратної складової (наприклад, пристрою на базі Raspberry Pi або подібного мікроконтролера) з програмною системою аналізу мережевих подій. Основна мета – досягнення автоматизованого контролю доступу та реєстрації користувачів без потреби у їхній безпосередній участі.

Найперше, проблема автоматизованої реєстрації вимагає наявності механізму виявлення нових пристроїв у мережі. Зважаючи на те, що кожен пристрій при підключенні до Wi-Fi обов'язково передає у мережу ARP-повідомлення, DHCP-запити або інші широкомовні пакети, ці дані можуть бути використані як надійне джерело інформації для фіксації появи нового клієнта. Одним із основних напрямів у побудові системи є створення модулю мережевого моніторингу, який у реальному часі фільтрує і зчитує заголовки пакетів, зберігаючи MAC-адресу, IP-адресу, час появи пристрою та інші службові параметри. У якості інструментів для реалізації цього етапу доцільно застосовувати бібліотеки низькорівневого аналізу мережі, наприклад, scapy, tcpdump, або власноруч реалізовані модулі, що працюють у режимі promiscuous.

Другим напрямом є забезпечення взаємодії між пристроєм-агентом і центральною базою даних. Тут важливу роль відіграє вибір архітектури обміну даними: REST API або MQTT, залежно від специфіки навантаження та масштабованості проєкту. В результаті кожен новий пристрій, який з'являється у мережі, автоматично реєструється у системі та передається до центрального сховища, де вже може бути застосовано певну логіку – наприклад, автоматичне додавання у білий список, створення запису про подію або сповіщення адміністратора.

Особливу увагу слід приділити ідентифікації та авторизації. Хоча MAC-адреса сама по собі є недостатнім ідентифікатором з погляду безпеки, вона може використовуватися як первинний тригер, на основі якого запускається подальша логіка – наприклад, перевірка, чи є ця адреса у базі дозволених, або виконання аналізу поведінки пристрою у мережі. Також важливо реалізувати механізми обробки виключень, зокрема при виявленні підозрілих MAC-адрес, які повторюються або змінюються з підозрілою частотою. У таких випадках система має підтримувати обмеження або автоматичне блокування доступу.

Ще одним важливим підходом є впровадження інтерфейсу керування для адміністратора мережі. Це може бути веб-панель, яка дозволяє переглядати список

активних пристроїв, бачити історію підключень, а також вносити до списку дозволених нові MAC-адреси або задавати часові рамки, у які певний пристрій має право на доступ. Подібна інтеграція дозволяє поєднати автоматизацію з можливістю ручного втручання за потреби, що значно підвищує гнучкість системи.

Окремим напрямом дослідження є підвищення достовірності виявлення пристроїв. Зважаючи на вразливість MAC-ідентифікації до підміни, доцільним може бути паралельне використання супутніх ознак – наприклад, аналіз часових характеристик, поведінки пристрою у мережі, шаблону трафіку, використаних портів тощо. Ці параметри можуть бути використані для формування цифрового «профілю» пристрою, який слугує додатковим рівнем перевірки.

Для вирішення поставленої задачі пропонується інтегрований підхід, який передбачає безперервний моніторинг мережі на рівні MAC-адрес, автоматичну реєстрацію нових пристроїв, збереження усіх підключень у централізовану базу даних, можливість керування доступом через адміністраторську панель та реалізацію механізмів виявлення аномальної активності. Уся система діє як єдине середовище, де фізичний доступ до мережі (через точку Wi-Fi) поєднується з логічним аналізом і цифровим контролем, що і є характерною ознакою сучасних кіберфізичних систем. В результаті створюється середовище з високим рівнем автоматизації, прозорістю подій у мережі та потенціалом для подальшої інтеграції з більш широкими системами безпеки чи обліку.

1.4 Постанова задачі

Метою проєкту є розробка кіберфізичної системи, здатної автоматизувати процес реєстрації пристроїв у бездротовій мережі Wi-Fi шляхом виявлення та ідентифікації користувачів на основі MAC-адрес їхніх пристроїв. Система має забезпечити безперервний моніторинг мережевої активності, фіксацію нових підключень, створення централізованого обліку пристроїв та можливість автоматичного або ручного керування доступом до мережі.

Для досягнення поставленої мети необхідно вирішити низку практичних і дослідницьких завдань:

– провести аналіз протоколів Wi-Fi і способів пасивного виявлення пристроїв у локальній мережі;

– оцінити можливості використання MAC-ідентифікації для реєстрації та контролю доступу;

– дослідити наявні програмно-апаратні рішення для моніторингу Wi-Fi-мереж, зокрема з використанням одноплатних комп'ютерів (наприклад, Raspberry Pi);

– розробити архітектуру системи, яка поєднує апаратний модуль виявлення з програмною платформою обробки подій і базою даних;

– реалізувати програмний модуль для захоплення та аналізу мережевих пакетів (DHCP, ARP, Probe Requests), що містять MAC-адреси;

– створити веб-інтерфейс для адміністративного керування підключеннями, перегляду історії та налаштування прав доступу;

– впровадити базові механізми безпеки (фільтрація, білий список, сигнали про підозрілу активність);

– протестувати систему в умовах реального середовища, оцінити її ефективність, стабільність і можливості масштабування;

– сформувати висновки щодо доцільності впровадження подібної системи у навчальних закладах, офісних просторах або публічних точках доступу до Wi-Fi.

На першому етапі передбачається детальне вивчення особливостей MAC-ідентифікації як базового методу реєстрації у Wi-Fi-середовищі, з акцентом на переваги й недоліки такого підходу. Особлива увага приділяється питанням надійності виявлення, конфіденційності даних та протидії підміні адрес.

Подальші етапи охоплюють розгортання тестового середовища, у якому працюватиме система мережевого моніторингу в режимі реального часу. Це середовище повинно бути здатне виявляти нові пристрої за їх MAC-адресами, формувати записи про кожне підключення, і передавати ці дані у базу даних для

подальшого аналізу та реагування.

У рамках розробки адміністративного інтерфейсу планується створити веб-панель із функціями перегляду поточних та історичних підключень, додавання чи блокування MAC-адрес, а також отримання сповіщень про появу нових пристроїв. Завдяки цьому система забезпечить не лише автоматизацію процесу реєстрації, а й надасть інструменти для аналітики та керування мережею.

На завершальному етапі буде проведено тестування функціоналу системи у напівреальному середовищі з подальшим аналізом отриманих результатів. Особлива увага приділяється швидкості реагування, точності виявлення, енергоефективності рішення, а також перспективам масштабування в більш складних інфраструктурах.

1.5 Висновки до першого розділу

У першому розділі було проведено комплексний аналіз предметної області кіберфізичних систем автоматизації реєстрації користувачів у Wi-Fi мережах на основі MAC-адрес. Розглянуто сучасні методи і технології ідентифікації та контролю доступу в бездротових мережах, а також основні вимоги до подібних систем, серед яких варто відзначити безпеку, швидкодію, масштабованість і зручність інтеграції в існуючу мережеву інфраструктуру.

Було охарактеризовано різні підходи до автоматизації процесу реєстрації в Wi-Fi мережах, включаючи використання MAC-адрес як унікальних ідентифікаторів пристроїв, а також розглянуто існуючі рішення, які застосовують кіберфізичні підходи для моніторингу та управління мережею в реальному часі. Проаналізовано переваги та недоліки цих методів з точки зору надійності і стійкості до зловмисних дій, а також можливості масштабування системи у великих мережах.

За результатами дослідження було виявлено основні проблемні аспекти, серед яких – необхідність ефективного збору, обробки і збереження великого

обсягу даних про пристрої, забезпечення конфіденційності користувацьких даних, а також інтеграція з існуючими протоколами аутентифікації. Особливу увагу приділено вибору оптимальної архітектури системи, що поєднує апаратні та програмні компоненти для досягнення високої продуктивності та надійності.

Сформульовано ключові завдання дослідження, які полягають у розробці прототипу кіберфізичної системи автоматизації реєстрації в Wi-Fi мережах на основі MAC-адрес, що має забезпечити швидку і безпечну ідентифікацію пристроїв, масштабованість і зручність у впровадженні. Це створює підґрунтя для подальшої розробки та тестування реалізації запропонованого рішення.

ПРОЄКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСУ РЕЄСТРАЦІЇ В WI-FI МЕРЕЖАХ НА ОСНОВІ MAC-АДРЕС

2.1 Визначення апаратних і програмних підсистем програмно-технічного засобу

Проєктування кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес вимагає комплексного підходу до формування її апаратної та програмної частин, які разом забезпечують стабільну, масштабовану та безпечну роботу системи. Апаратна підсистема включає мережеве обладнання, яке відповідає за безпосереднє приймання та передачу бездротових сигналів, а саме точки доступу Wi-Fi, що виконують функції ідентифікації клієнтських пристроїв за їх унікальними MAC-адресами. Для обробки отриманих даних, виконання логіки реєстрації і контролю доступу використовуються одноплатні комп’ютери типу Raspberry Pi або інші мікроконтролери з достатніми обчислювальними ресурсами. Ці пристрої слугують проміжним рівнем між Wi-Fi обладнанням і центральним сервером, забезпечуючи локальну обробку інформації і передачу узагальнених даних для подальшого аналізу.

Серверна частина системи виконує роль центрального сховища та контролера, де зберігаються бази даних MAC-адрес, ведеться облік реєстрацій та адмініструються політики доступу до мережі. Для реалізації надійного і безперебійного функціонування система повинна передбачати інтеграцію з мережею через маршрутизатори та комутатори, що забезпечують зв’язок між апаратними елементами.

Програмна підсистема базується на розробці модулів, які реалізують збір, обробку і фільтрацію MAC-адрес, а також управління процесом автоматичної реєстрації пристроїв у мережі. Особлива увага приділяється забезпеченню безпеки – система повинна гарантувати верифікацію підключень і запобігати несанкціонованому доступу. Центральний модуль реєстрації взаємодіє з базою

даних, де зберігаються інформація про пристрої, історія їх підключень та налаштування політик доступу.

Для адміністрування і моніторингу передбачено розробку зручного інтерфейсу, що дозволяє у режимі реального часу контролювати стан мережі, переглядати статистику підключень, керувати списками дозволених або заблокованих MAC-адрес, а також налаштовувати правила автоматичної реєстрації. Крім того, у системі реалізується модуль аналітики, який на основі зібраних даних формує звіти про активність користувачів та потенційні аномалії в роботі мережі.

Взаємодія між апаратною та програмною частинами забезпечується через стандартизовані протоколи обміну даними та API, що гарантують надійну і швидку передачу інформації, а також можливість інтеграції з іншими інформаційними системами безпеки. У сукупності всі ці компоненти формують цілісну кіберфізичну систему, яка автоматизує процес реєстрації користувачів у Wi-Fi мережах, підвищує рівень безпеки, а також забезпечує зручність і масштабованість адміністрування.

Важливою складовою апаратної підсистеми є забезпечення стабільного і безперервного зв’язку між компонентами системи, що вимагає належної організації мережевої інфраструктури. Це передбачає використання якісного комутаційного обладнання та мережевих протоколів, які гарантують низькі затримки передачі даних і високу пропускну здатність, що особливо актуально для середовищ із великою кількістю підключених пристроїв. Крім того, необхідно передбачити резервні канали зв’язку для підтримки стійкості системи у випадках збоїв або перевантажень.

У межах програмної підсистеми особлива увага приділяється розробці алгоритмів обробки MAC-адрес, які дозволяють швидко ідентифікувати пристрої, відстежувати їх активність і визначати рівень довіри або доступу. Для підвищення ефективності роботи система може застосовувати методи машинного навчання або аналітики поведінкових патернів, що дає змогу автоматично виявляти підозрілі чи

неавторизовані підключення. Такий підхід значно підвищує рівень безпеки та дозволяє оперативно реагувати на потенційні загрози.

Впровадження кіберфізичної системи також включає забезпечення інтеграції з існуючими інформаційними системами підприємства або організації, що потребує розробки відповідних API та інтерфейсів обміну даними. Це дозволяє об’єднати різні підсистеми управління мережею, а також забезпечити централізований контроль і моніторинг. Така інтеграція сприяє підвищенню загальної ефективності роботи та зниженню операційних витрат.

Особливу увагу необхідно приділити питанням безпеки на рівні фізичного доступу до апаратного забезпечення, а також захисту від кіберзагроз, таких як підміна MAC-адрес, DoS-атаки або спроби несанкціонованого доступу до мережевих ресурсів. Для цього застосовуються як апаратні методи захисту, так і програмні рішення, включаючи засоби шифрування, багаторівневу автентифікацію і ведення журналів подій для подальшого аудиту.

В цілому, комплексний підхід до проектування апаратної та програмної підсистем забезпечує високу надійність, гнучкість і масштабованість кіберфізичної системи, що дозволяє ефективно автоматизувати процес реєстрації пристроїв у Wi-Fi мережах на основі MAC-адрес і гарантувати безперервну роботу навіть у складних та динамічних умовах експлуатації.

Для забезпечення ефективної роботи кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес необхідно грамотно поєднати апаратні та програмні компоненти. Апаратна підсистема виконує роль основи, яка забезпечує збір, передачу та первинну обробку даних, тоді як програмна підсистема реалізує логіку управління, аналізу і прийняття рішень.

Програмне забезпечення має бути розроблене з урахуванням можливості масштабування та інтеграції з іншими мережевими сервісами, такими як системи аутентифікації користувачів, бази даних для зберігання історії реєстрацій та засоби аналітики. Для підвищення безпеки передбачено використання сучасних методів шифрування даних і багаторівневої системи контролю доступу.

Окрім основного функціоналу, програмна підсистема повинна підтримувати механізми моніторингу стану апаратного забезпечення, що дозволяє оперативно реагувати на збої або погіршення параметрів роботи обладнання. Це є особливо важливим для підтримки високої доступності та безперервності роботи системи (табл 2.1).

Таблиця 2.1 – Апаратна підсистема.

1.	Модуль Wi-Fi	Забезпечує бездротове з'єднання та збір MAC-адрес підключених пристроїв
2.	Комутуюче обладнання	Організує локальну мережу та маршрутизацію даних
3.	Програмне забезпечення для збору MAC-адрес	Автоматизує процес виявлення та реєстрації пристроїв у Wi-Fi мережі
4.	Алгоритми аналізу і верифікації	Використовуються для ідентифікації пристроїв, виявлення аномалій, управління доступом
5.	Інтерфейси інтеграції	Забезпечують взаємодію з зовнішніми інформаційними системами
6.	Механізми безпеки	Контролюють доступ, забезпечують захист даних та системи

Ключова складова кіберфізичної системи є належна організація мережевої взаємодії між апаратними модулями та програмним забезпеченням. В системі збір інформації про MAC-адреси здійснюється через спеціалізовані точки доступу або мережеві пристрої, які безперервно сканують навколишнє середовище на предмет наявності підключених або спроб підключення пристроїв. Для передачі зібраних даних між апаратними пристроями та центральним сервером застосовуються надійні протоколи, такі як MQTT або HTTPS, які забезпечують як цілісність, так і конфіденційність переданої інформації. Це дозволяє підтримувати стабільну

роботу системи навіть за умови нестабільного інтернет-з’єднання.

Враховуючи, що кіберфізична система зазвичай функціонує в режимі безперервного моніторингу, особлива увага приділяється питанням енергоспоживання та надійності роботи апаратних компонентів. Використання енергоефективних одноплатних комп’ютерів і оптимізованого програмного забезпечення дозволяє підтримувати тривалу роботу без частих перезавантажень або перебоїв у живленні. Крім того, система передбачає автоматичне відновлення після збоїв, що гарантує збереження цілісності даних і безперервність процесу реєстрації.

Оскільки збираються і обробляються персональні дані пристроїв, необхідно забезпечити їх захист від несанкціонованого доступу. Це реалізується через застосування сучасних методів шифрування інформації під час передачі, а також через впровадження механізмів аутентифікації користувачів і адміністраторів системи. Окрім того, ведеться детальний аудит подій, що дозволяє відстежувати і реагувати на підозрілі дії.

Система повинна бути масштабованою і легко розширюваною. Це означає, що можна збільшувати кількість точок доступу, інтегрувати додаткові сервіси для аналізу та візуалізації даних без необхідності радикального перепроектування системи. Така гнучкість забезпечує її довготривалу актуальність і ефективність у різних умовах експлуатації.

Взаємодія з користувачем здійснюється через інтуїтивно зрозумілі інтерфейси – веб-додатки або мобільні застосунки, які дозволяють адміністраторам переглядати статистику, налаштовувати параметри системи і отримувати оперативні повідомлення про події. Завдяки цьому управління системою стає простим та зручним, навіть без глибоких технічних знань.

Що стосується обробки та зберігання даних, система використовує надійні бази даних, що підтримують резервне копіювання та швидкий доступ до інформації. Застосовуються політики збереження даних, які регулюють терміни їх зберігання та умови видалення, що відповідає вимогам законодавства про захист

персональних даних. Крім того, є можливості для аналітики, що дозволяють проводити глибокий аналіз зібраної інформації для подальшого підвищення ефективності роботи мережі.

Використання MAC-адрес як ідентифікаторів пристроїв не завжди є однозначним, оскільки MAC-адреси можуть бути змінені або підроблені. Також різне мережеве обладнання може підтримувати різні методи збору інформації, що ускладнює уніфікований підхід. Вирішення цих проблем потребує застосування додаткових методів верифікації пристроїв, адаптації програмного забезпечення під різне обладнання і постійного моніторингу системи.

Кіберфізична система автоматизації реєстрації в Wi-Fi мережах на основі MAC-адрес є складним комплексом, що об’єднує в собі як апаратні, так і програмні рішення, спрямовані на забезпечення надійного, безпечного та зручного процесу реєстрації і моніторингу мережевих пристроїв.

2.2 Архітектура та принцип побудови кіберфізичної системи

Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес має багаторівневу архітектуру, що забезпечує ефективне збирання, обробку, зберігання та аналіз даних у реальному часі. Основні компоненти системи організовані таким чином, щоб максимально інтегрувати фізичні пристрої з програмним забезпеченням для досягнення високого рівня автоматизації та надійності.

На нижньому рівні розташовані апаратні засоби – точки доступу, мережеві сенсори, які відповідають за збір інформації про MAC-адреси пристроїв, що намагаються підключитися до Wi-Fi мережі. Ці пристрої виконують безперервне сканування ефіру, фільтрують отримані дані, ідентифікують унікальні MAC-адреси, а також збирають додаткові параметри, такі як час спроби підключення, сила сигналу та тип пристрою.

Зібрана інформація передається на проміжний рівень, де працює програмне

забезпечення для первинної обробки і фільтрації даних. Тут відбувається нормалізація інформації, видалення дублікованих записів, а також формування подій для подальшої аналітики. Проміжний рівень часто реалізується на базі контейнеризованих сервісів, що дозволяють гнучко масштабувати систему та ефективно використовувати апаратні ресурси.

Верхній рівень складається з централізованої платформи управління, яка надає інтерфейс користувачу та адміністраторам системи. Цей рівень відповідає за зберігання великих обсягів даних у базах даних, реалізацію механізмів аутентифікації та авторизації, а також за візуалізацію статистичних даних і подій. Крім того, на цьому рівні відбувається реалізація аналітичних алгоритмів, які дозволяють виявляти аномалії, прогнозувати навантаження мережі і оптимізувати управління ресурсами.

Принцип побудови системи ґрунтується на інтеграції кібернетичних та фізичних компонентів з метою створення єдиного, взаємозалежного середовища. Такий підхід забезпечує постійний двонаправлений зв’язок між сенсорами і обчислювальними модулями, що дає змогу оперативно реагувати на зміни у мережі і автоматично коригувати параметри роботи системи.

Важливою особливістю архітектури є її модульність і масштабованість. Кожен компонент системи розробляється як автономний сервіс із чітко визначеними інтерфейсами взаємодії, що спрощує інтеграцію нових функціональних можливостей і дозволяє адаптувати систему під різні умови експлуатації. Застосування сучасних технологій контейнеризації і оркестрації забезпечує високу гнучкість розгортання і управління системою.

Для підвищення надійності і безперервності роботи система реалізує механізми резервного копіювання, відновлення після збоїв і балансування навантаження між апаратними вузлами. Це дає змогу уникнути втрати даних і підтримувати стабільний рівень обслуговування навіть при несправностях окремих компонентів.

Кіберфізична система спроектована з урахуванням можливості інтеграції з

різноманітними інформаційними системами, що використовуються у організаціях. Це можуть бути системи управління мережею (Network Management Systems), корпоративні CRM-системи або платформи для аналітики. Завдяки відкритим API та гнучким протоколам обміну даними система може бути легко включена в загальну інфраструктуру підприємства, що дозволяє централізовано управляти реєстрацією користувачів і контролювати доступ.

Для забезпечення безперервної роботи системи реалізовано функції моніторингу стану апаратних вузлів і програмних сервісів. Система самодіагностики регулярно перевіряє працездатність ключових компонентів і оперативно повідомляє адміністратора про можливі збої або критичні ситуації.

В перспективі розробки система може бути розширена за допомогою алгоритмів аналітики й машинного навчання, що дозволить підвищити рівень автоматизації і точність прийняття рішень. Зокрема, застосування методів виявлення аномалій дозволить оперативно ідентифікувати підозрілу активність у мережі, що може свідчити про спроби несанкціонованого доступу або інші загрози.

Аналіз поведінкових патернів користувачів і пристроїв дозволить оптимізувати використання мережевих ресурсів, прогнозувати навантаження і відповідно коригувати налаштування для забезпечення стабільної роботи.

Програмне забезпечення системи побудоване на основі сучасних технологій та архітектурних патернів. Для серверної частини використовується мова програмування, яка забезпечує високу продуктивність та безпеку, наприклад Python. База даних обрана з урахуванням потреб швидкого зберігання і доступу до великих обсягів інформації, а також підтримки масштабованості.

Важливою складовою архітектури є використання RESTful API для взаємодії між різними модулями системи та зовнішніми клієнтами. Такий підхід забезпечує гнучкість і простоту інтеграції, а також дозволяє легко розширювати функціонал.

Користувачі та адміністратори мають зручний інтерфейс для взаємодії з системою, який може бути реалізований як веб-додаток або мобільний застосунок. Інтерфейс дозволяє переглядати інформацію про підключені пристрої, стан мережі,

статистику реєстрацій, а також управляти налаштуваннями та отримувати повідомлення про події.

Простота і інтуїтивність інтерфейсу є важливими факторами для забезпечення ефективної роботи і швидкого освоєння системи персоналом.

В процесі проєктування та реалізації системи були виявлені певні технічні складнощі, зокрема обмеження апаратних ресурсів пристроїв, які збирають та обробляють інформацію (наприклад, вбудовані пристрої або одноплатні комп'ютери). Це вимагає оптимізації програмного коду і розумного розподілу навантаження між компонентами.

Мережевий сканер відповідає за активне виявлення пристроїв у Wi-Fi мережі шляхом сканування мережевого трафіку або запитів до роутера. Використовуючи Python, реалізовано механізми, що отримують список MAC-адрес, підключених до мережі. Для цього застосовуються різні мережеві протоколи та команди (наприклад, ARP-запити або звернення до API роутера). Задля тестування і симуляції роботи роутера створено програмний емулятор, який імітує поведінку мережевого обладнання, забезпечуючи стабільний потік даних для обробки системою.

Інформація, отримана зі сканера, зберігається в реляційній базі даних, що організована за допомогою ORM (об'єктно-реляційного маппера). Це дозволяє працювати з даними у вигляді об'єктів Python, спрощуючи розробку та підтримку системи. Кожна MAC-адреса має свій запис із відповідними атрибутами: час першого і останнього виявлення, статус реєстрації, додаткові позначки. Такий підхід забезпечує збереження історії пристроїв та полегшує подальший аналіз.

Контролює весь процес автоматичної реєстрації: запуск сканування у визначені проміжки часу, порівняння отриманих MAC-адрес із базою, внесення нових записів, оновлення статусів. Використання асинхронного програмування (asyncio) дозволяє виконувати одночасно кілька завдань без блокування, що підвищує продуктивність та швидкодію системи. Логіка також передбачає валідацію даних, фільтрацію непотрібної інформації та обробку помилок, що

робить систему надійною.

Для зручної взаємодії з користувачами створено Telegram-бота. Через нього можна оперативно отримувати повідомлення про підключення нових пристроїв, запускати команди на сканування, переглядати статистику та отримувати інформацію про стан системи. Використання Telegram як платформи комунікації робить систему мобільною та доступною з будь-якої точки без необхідності складних інтерфейсів.

Додатково розроблено легкий веб-інтерфейс, що дозволяє адміністраторам переглядати детальну інформацію про підключені пристрої, керувати процесом реєстрації, налаштовувати параметри сканування та виконувати інші адміністративні дії. Веб-інтерфейс забезпечує зручний доступ через браузер і слугує доповненням до Telegram-бота, розширюючи можливості контролю і моніторингу.

Взаємодія між усіма частинами системи організована через чітко визначені інтерфейси та протоколи обміну даними. Сканер постійно збирає нові дані, які передаються до бізнес-логіки, де проходять обробку і фільтрацію, після чого оновлені відомості зберігаються у базі. Комунікаційні інтерфейси миттєво інформують користувачів про зміни, забезпечуючи оперативний зворотний зв’язок. Асинхронний підхід дозволяє системі підтримувати стабільну роботу навіть при великому потоці даних.

Система побудована на базі мови програмування Python, яка забезпечує гнучкість і простоту розробки. Для асинхронного виконання задач використовується бібліотека asyncio, що дозволяє ефективно працювати з мережевими операціями і одночасно запускати декілька процесів. Для збереження та керування даними застосовано SQLAlchemy – потужний ORM для роботи з реляційними базами. Веб-інтерфейс створено з використанням Flask – легкого веб-фреймворку, що підтримує швидку розробку веб-додатків. Для комунікації з користувачами реалізовано Telegram-бота на основі офіційного API, що забезпечує простий та зручний доступ до функцій системи.

2.3 Аналіз існуючих рішень у сфері кіберфізичних систем автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес

Ця галузь вже має широкий спектр реалізованих підходів, але одночасно з цим залишається багато викликів і обмежень. Сучасне мережеве обладнання, зокрема Wi-Fi роутери і контролери, оснащене вбудованими функціями для збору ідентифікаційних даних про підключені пристрої, серед яких ключове місце займають MAC-адреси. Такі пристрої можуть виконувати базову автоматичну реєстрацію і контроль доступу шляхом застосування MAC-фільтрації. Однак ці рішення часто мають обмежену функціональність і недостатньо гнучкі налаштування, що ускладнює їх використання у великих або складних мережах із великою кількістю користувачів.

Існують також програмні продукти, які забезпечують моніторинг і управління мережею, збираючи інформацію про підключені пристрої і ведучи журнали їх активності. Такі системи можуть бути як пропрієтарними від виробників мережевого обладнання, так і відкритими проектами, що надають ширші можливості кастомізації. Однак часто ці рішення вимагають значних технічних знань для налаштування і підтримки, а також не завжди здатні інтегруватися з іншими системами, що обмежує їх функціональність у рамках складної кіберфізичної інфраструктури.

Найбільш перспективними вважаються комплексні кіберфізичні системи, які поєднують апаратні і програмні компоненти, забезпечуючи високу ступінь автоматизації, масштабованість і централізоване управління мережею. Ці системи інтегрують мережеві пристрої, бази даних, аналітичні модулі та інтерфейси для взаємодії з користувачами через різні канали зв’язку, такі як мобільні додатки або месенджери. Вони не лише автоматично реєструють MAC-адреси пристроїв, а й аналізують їх поведінку, дозволяють налаштовувати політики доступу в реальному часі, контролювати історію підключень, а також взаємодіяти з додатковими

системами безпеки. Такий підхід підвищує ефективність управління мережею і зменшує потребу в ручному втручанні адміністратора.

Водночас існуючі рішення мають і суттєві недоліки. Зокрема, обмежена гнучкість багатьох апаратних систем, які не підтримують глибоку кастомізацію або інтеграцію з іншими IT-сервісами, ускладнює їх застосування у сучасних умовах. Збільшення масштабів мережі і кількості підключених пристроїв часто призводить до втрати продуктивності або ефективності традиційних рішень. Багато систем також не забезпечують повної автоматизації процесів, що вимагає постійної участі технічного персоналу у веденні списків, контролі виключень і налаштуванні доступу. Окрім того, реєстрація пристроїв лише за MAC-адресою має ризики, пов'язані з можливістю підробки цих адрес, тому сучасні системи зобов'язані впроваджувати додаткові механізми для підвищення безпеки.

Перспективи розвитку полягають у впровадженні новітніх технологій, таких як контейнеризація, асинхронна обробка даних, інтеграція зі службами повідомлень, а також застосування штучного інтелекту для аналізу поведінки пристроїв і виявлення аномалій. Це дозволить створити більш адаптивні та інтелектуальні системи, які зможуть підлаштовуватися під конкретні умови мережі і оперативно реагувати на потенційні загрози або неполадки.

Аналіз показує, що хоча базові інструменти для реєстрації MAC-адрес вже існують, найбільш ефективними є інтегровані кіберфізичні системи, які пропонують комплексний підхід до автоматизації і управління Wi-Fi мережами. Розроблена в рамках цієї роботи система враховує багато недоліків існуючих рішень і базується на сучасних технологіях, що робить її актуальною і перспективною для практичного застосування.

одним із ключових аспектів вдосконалення кіберфізичних систем автоматизації процесу реєстрації в Wi-Fi мережах є забезпечення високої надійності та безперервності роботи. Це передбачає впровадження механізмів відмовостійкості, резервного копіювання даних та можливості швидкого відновлення після збоїв. Особливо актуальним є використання розподілених

архітектур, які дозволяють уникнути єдиної точки відмови і забезпечують масштабованість системи при збільшенні кількості підключених пристроїв.

Також значну увагу слід приділяти питанням захисту персональних даних користувачів, що підключаються до мережі. Окрім стандартних методів шифрування і аутентифікації, сучасні системи повинні враховувати вимоги законодавства щодо обробки та зберігання таких даних, зокрема в контексті GDPR або інших локальних нормативних актів. Це зумовлює необхідність впровадження політик контролю доступу, аудиту дій користувачів і регулярного оновлення безпекових механізмів.

Додатково перспективним напрямком розвитку є інтеграція кіберфізичних систем із зовнішніми платформами для централізованого управління інфраструктурою, такими як системи SIEM (Security Information and Event Management) або хмарні сервіси аналітики. Це дозволить більш ефективно відслідковувати події, виявляти загрози і оперативно реагувати на інциденти безпеки.

Розширення функціональності системи за рахунок впровадження зазначених підходів забезпечить її відповідність сучасним вимогам, підвищить ефективність і надійність роботи, а також сприятиме широкому впровадженню у різних сферах, де критичною є безпека та автоматизація процесів реєстрації в Wi-Fi мережах.

2.4 Особливості впровадження кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес

Система повинна бути максимально гнучкою щодо різноманітності мережевого обладнання, оскільки в реальних умовах Wi-Fi мережі можуть використовувати різні моделі роутерів і точок доступу з власними протоколами взаємодії. Це вимагає впровадження універсальних алгоритмів сканування та реєстрації пристроїв, що базуються на MAC-адресах, які залишаються стабільним і унікальним ідентифікатором для кожного пристрою.

Необхідно враховувати особливості безпеки, зокрема захист даних, що збираються під час процесу реєстрації. MAC-адреси можуть бути вразливими до підробки або спуфінгу, тому система повинна містити механізми верифікації і фільтрації, які дозволяють знижувати ризики несанкціонованого доступу або зловмисних дій. Це може включати перевірку поведінкових шаблонів пристроїв або співставлення з базою відомих «білого списку» MAC-адрес.

Адаптація системи повинна забезпечувати її масштабованість, що дозволить успішно функціонувати у мережах з різною кількістю підключених користувачів – від невеликих офісних мереж до великих публічних точок доступу з тисячами користувачів одночасно. Для цього застосовуються оптимізовані алгоритми збору і обробки даних, а також розподілені архітектури з можливістю балансування навантаження.

Крім того, важливою особливістю є забезпечення зручності управління системою, що включає автоматичне оновлення бази даних зареєстрованих пристроїв, інтуїтивно зрозумілі інтерфейси для адміністраторів, а також можливість інтеграції з існуючими інформаційними системами підприємства.

Врахування вищезазначених аспектів під час адаптації кіберфізичної системи на основі MAC-адрес сприяє підвищенню її ефективності, надійності та безпеки, що є критично важливими у сучасних умовах постійного зростання кількості бездротових пристроїв та зростаючих вимог до контролю доступу в Wi-Fi мережах.

2.5 Висновки до другого розділу

У другому розділі було здійснено комплексне проєктування кіберфізичної системи автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес, що включає визначення ключових апаратних та програмних підсистем. Розглянуто особливості вибору обладнання, яке забезпечує стабільне та ефективне сканування мережі, а також впровадження програмних модулів для автоматичного збору,

обробки та збереження інформації про пристрої на основі їх унікальних MAC-адрес. Проаналізовано інтеграцію різних компонентів системи, зокрема імітацію роботи роутера та взаємодію з базою даних для забезпечення надійної реєстрації та контролю доступу.

Особлива увага приділялася адаптивності системи до різних типів мережевого обладнання та забезпеченню безпеки даних, що реєструються, шляхом впровадження механізмів фільтрації та верифікації MAC-адрес. Крім того, враховано необхідність масштабованості та продуктивності системи для роботи у мережах різного розміру – від малих офісних до великих публічних Wi-Fi мереж.

В результаті проєктування створено архітектуру, що поєднує апаратні та програмні компоненти в єдину ефективну кіберфізичну систему, здатну автоматизувати процес реєстрації в Wi-Fi мережах, підвищуючи рівень безпеки і зручності управління. Отримані результати слугують надійною основою для подальшої реалізації та тестування розробленої системи.

ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСУ РЕЄСТРАЦІЇ В WI-FI МЕРЕЖАХ НА ОСНОВІ MAC-АДРЕС

3.1 Опис реалізації модулів апаратного та програмного забезпечення програмно-технічного засобу

Проєкт програмно-технічного засобу, що реалізується у межах даного дослідження, поєднує апаратну складову з програмним забезпеченням, яке забезпечує моніторинг і контроль за активністю пристроїв у бездротовій локальній мережі. Основна мета – автоматизована фіксація пристроїв на основі MAC-адрес з можливістю подальшого аналізу, контролю доступу та інтеграції з мережею. У рамках цього підрозділу буде здійснено поглиблений опис архітектурних рішень, вибраного стеку технологій, реалізації ключових функцій та принципів роботи апаратного і програмного модулів системи.

В основі апаратної частини лежить міні-комп’ютер Raspberry Pi 4 Model B, який виступає у ролі локального сканера мережі та хоста для розміщення серверної логіки. Цей пристрій має компактні розміри, низьке енергоспоживання і достатню обчислювальну потужність для виконання мережевого моніторингу в реальному часі. Raspberry Pi підключається до локальної Wi-Fi мережі та виконує роль «мережевого спостерігача», збираючи інформацію про всі пристрої, які з’являються або зникають у мережі.

Для коректної роботи системи важливим є наявність стабільного з’єднання з мережею, а також доступу до командного рядка для виконання низькорівневих системних команд, таких як arp, ip neigh, ping, iwconfig тощо. Обране апаратне рішення забезпечує достатню кількість портів та підтримку USB/Wi-Fi модулів, що дозволяє у разі потреби масштабувати систему, підключаючи додаткові датчики або адаптери.

Програмна частина є серцем усього функціоналу і була реалізована з

використанням мови програмування Python 3.11 через її гнучкість, розвинену екосистему бібліотек, а також зручність у реалізації як серверної логіки, так і взаємодії з операційною системою.

Модуль сканування мережі реалізує періодичне виявлення пристроїв у локальній мережі шляхом активного пінгування IP-адрес та аналізу таблиці ARP. Він використовує асинхронну модель виконання (asyncio) для ефективного розподілу ресурсів та мінімізації часу на сканування.

Модуль обробки даних відповідає за збереження, оновлення та фільтрацію записів про MAC-адреси. Усі дані зберігаються у SQLite базі даних, яка виступає локальним сховищем. Для взаємодії з базою використовується SQLAlchemy ORM, що дозволяє абстрагуватися від сирих SQL-запитів і працювати з об'єктно-орієнтованими структурами.

Веб-інтерфейс (інтерфейс адміністратора) реалізований на основі Flask – легкого веб-фреймворку, який дозволяє швидко створювати веб-додатки. Інтерфейс надає адміністратору можливість переглядати, редагувати і змінювати статус пристроїв. Для візуалізації використовуються стандартні HTML-шаблони з CSS-оформленням для зручності навігації та перегляду.

Модуль симуляції роботи з маршрутизатором: оскільки прямий доступ до API реального роутера не завжди можливий або може потребувати автентифікації, у системі реалізований симулятор – RouterAPI, що імітує типову взаємодію з мережею: дозволи доступу, підтвердження MAC-адрес, обмеження тощо. У разі переходу до продакшн-рівня, даний модуль може бути замінений на REST API, що підтримується виробником роутера.

У рамках циклу роботи системи діють такі етапи:

- сканування;
- виявлення нових MAC;
- додавання в базу;
- оновлення статусу;
- інформування адміністратора.

Такий підхід дозволяє повністю автоматизувати початкову реєстрацію пристрою та передати контроль за доступом до адміністратора. Для цього у веб-інтерфейсі реалізовано візуальний індикатор часу останнього з'єднання пристрою, що дозволяє відстежувати неактивні або нові пристрої у мережі.

Інтеграція усіх модулів дозволяє підтримувати цілісність архітектури. Наприклад, після завершення асинхронного сканування, отримані MAC-адреси передаються в модуль обробки, який порівнює їх з наявними записами у базі та визначає, чи є вони новими. У разі виявлення нового пристрою, він отримує статус "невідомий", а адміністратор отримує повідомлення у веб-інтерфейсі.

Система підтримує збереження логів усіх дій, кожне сканування, додавання нового пристрою чи зміна статусу фіксується у внутрішньому журналі, що зберігається окремим файлом або може бути виведений у адміністративну панель. Це сприяє забезпеченню прозорості у роботі системи та створює основу для подальшої аналітики та звітності.

Програмне рішення реалізовано з урахуванням базових вимог до інформаційної безпеки. Адміністративний інтерфейс може бути захищений паролем або авторизацією через токен. У разі реального впровадження в освітньому закладі, офісі чи виробничому середовищі доцільно впровадити рольову модель доступу з поділом прав на перегляд, редагування або виключення пристроїв із мережі.

Архітектура рішення з самого початку орієнтована на гнучке масштабування. Це означає, що кожен модуль може бути винесений в окремий процес або навіть контейнеризований за допомогою Docker. Більше того, система може бути адаптована для роботи у хмарному середовищі або в рамках корпоративної мережі з великою кількістю точок доступу.

Особливу увагу під час реалізації було приділено стійкості роботи програмного забезпечення в умовах нестабільного мережевого середовища. Для цього були реалізовані механізми повторних спроб підключення, обробки винятків при втраті доступу до мережевих інтерфейсів, а також тимчасове кешування

результатів сканування. Завдяки цим заходам програмний модуль зберігає стабільність роботи навіть у випадку короткочасних перебоїв у мережі або апаратних збоях.

У процесі розробки також використовувались інструменти контролю версій, зокрема Git, що дозволило структурувати проєкт, забезпечити зворотню сумісність змін та відслідковувати еволюцію програмного коду. Такий підхід є надзвичайно важливим для подальшої підтримки системи, оскільки він дозволяє ефективно управляти оновленнями та адаптувати програму до нових умов без необхідності повної переробки структури.

Було враховано можливість інтеграції зі сторонніми сервісами через REST API. Це відкриває широкі перспективи для розширення функціональності, наприклад, автоматичної взаємодії з системами керування користувачами, журналювання подій у зовнішніх системах, надсилання сповіщень у Telegram або на електронну пошту. У перспективі така інтеграція може стати основою для створення більш масштабної системи моніторингу, що охоплює декілька об'єктів, з централізованим керуванням і звітністю.

З огляду на потенційне застосування системи в освітніх установах або офісах, одним із завдань було мінімальне втручання адміністратора у процес. У зв’язку з цим значна частина функцій була автоматизована. Наприклад, система самостійно виявляє, коли пристрій був востаннє активним, і змінює його статус на “неактивний” після встановленого періоду часу. Це дозволяє уникнути потреби у постійному ручному контролі.

Також передбачена можливість резервного копіювання бази даних. У випадку збою пристрою або необхідності перенесення системи на нове обладнання, резервні копії можуть бути легко відновлені. Такий механізм є критично важливим для збереження історичних даних і забезпечення безперервності роботи програмно-технічного засобу.

Веб-додаток може бути адаптований під мову користувача, зокрема українську, що підвищує доступність системи для локальних адміністраторів, які

не мають глибоких технічних знань. Такий підхід суттєво полегшує навчання та подальше використання системи.

Усі рішення, закладені в основу архітектури проєкту, базуються на принципах модульності, масштабованості та гнучкості. Це дозволяє адаптувати систему під нові виклики, розширювати функціональність без суттєвого переписування коду та легко впроваджувати у нові середовища.

3.2 Опис реалізації створення сервера програмно-технічного засобу

Для забезпечення ефективного управління пристроями в локальній мережі, які підключаються до маршрутизатора, було реалізовано серверну частину системи на базі мікрофреймворку Flask. Обрана технологія дозволяє швидко створювати легковагі веб-додатки, що не потребують складного налаштування та мають достатню гнучкість для виконання широкого кола задач.

Основним завданням сервера є організація взаємодії між користувачем, базою даних та модулем керування маршрутизатором. В рамках реалізації було створено кілька маршрутів (routes), які відповідають за обробку запитів, рендеринг шаблонів, а також взаємодію з базою даних та API маршрутизатора.

Створення веб-сервера починається з ініціалізації Flask-додатку, який виконує роль центральної точки доступу до всіх функцій системи. Сам додаток підключає необхідні модулі: модель ORM для взаємодії з базою даних (через Session та MacAddress), сканер мережі (scan_and_register) та інтерфейс до маршрутизатора (RouterAPI). Така модульна архітектура дозволяє розділити логіку за функціональними блоками, що спрощує підтримку, оновлення та масштабування системи.

Головна сторінка веб-інтерфейсу (кореневий маршрут /) виконує подвійну функцію: у випадку GET-запиту вона відображає актуальний список усіх MAC-адрес, зареєстрованих у базі даних, разом із їхнім статусом доступу, а у випадку POST-запиту обробляє введену користувачем MAC-адресу. Реалізовано базову валідацію формату введених MAC-адрес, яка захищає систему від помилок

введення. Якщо адреса вже існує у базі, її статус перемикається (дозволено/заборонено), що надає адміністраторам інтуїтивний інструмент керування без необхідності видалення чи дублювання записів. Якщо ж введено нову адресу, вона автоматично додається у список дозволених.

Ще одним важливим елементом є маршрут /scan, який запускає асинхронне сканування мережі з метою виявлення нових пристроїв, що підключились до маршрутизатора. Для цього використовується новий event loop бібліотеки asyncio, що дозволяє не блокувати основний потік сервера. Сканування відбувається через спеціальний програмний модуль scan_and_register, який взаємодіє з маршрутизатором за допомогою API. Після завершення сканування користувач отримує повідомлення про кількість знайдених нових пристроїв. Це дозволяє в режимі реального часу поповнювати список клієнтів, які не були раніше зареєстровані в системі.

Функція RouterAPI, яка реалізована окремо, відіграє ключову роль в інтеграції з апаратним забезпеченням маршрутизатора. Вона абстрагує всі низькорівневі команди, що необхідні для отримання списку підключених клієнтів, а також дозволяє у подальшому розширити функціонал для прямого керування мережею, зокрема – блокування або пріоритезації трафіку для окремих MAC-адрес.

Для зберігання даних використовується реляційна база, доступ до якої реалізовано через ORM-модуль. Це забезпечує надійність збереження стану системи, зокрема записів MAC-адрес, їх дозволів, часу останньої активності тощо. Важливою перевагою ORM-підходу є зручність написання запитів, зменшення ймовірності SQL-помилок та забезпечення переносимості рішень на різні типи баз даних.

Візуальна частина системи реалізована на базі HTML-шаблонів з використанням Jinja2 – вбудованого шаблонізатора Flask. Це дозволяє формувати динамічний контент на основі даних з бази та логіки обробки запитів. Повідомлення для користувача (наприклад, підтвердження про зміну статусу або

виявлення нових пристроїв) реалізовані за допомогою механізму flash, який дозволяє показувати тимчасові повідомлення після редиректу.

Сервер працює в режимі debug=True, що є зручним на етапі розробки та тестування, оскільки дозволяє швидко виявляти та усувати помилки в коді. У продуктивному середовищі цей режим може бути вимкнений, а сервер переведено на роботу під керуванням більш продуктивного WSGI-сервера, наприклад Gunicorn або uWSGI.

У підсумку, створений сервер є центральною частиною програмної системи, який забезпечує не лише зручну точку доступу для керування MAC-адресами, а й ефективно інтегрується з апаратною частиною – маршрутизатором. Його модульна структура, використання сучасних бібліотек Python та підтримка асинхронних задач робить систему надійною, гнучкою та готовою до подальшого масштабування.

Реалізація сервера, що забезпечує керування доступом за MAC-адресами та взаємодіє з маршрутизатором, є ключовим елементом програмно-технічного комплексу. Архітектурно сервер побудований на основі фреймворку Flask, що є популярним легковаговим інструментом для створення веб-застосунків на Python. Його простота, гнучкість і розширюваність дозволяє швидко створити робочий інтерфейс та забезпечити обробку запитів користувача через HTTP-протокол.

Серверна частина виконує кілька основних функцій: прийом запитів від користувача, обробка введених MAC-адрес, взаємодія з базою даних, відображення результатів на веб-сторінці та ініціація процесу сканування мережі для виявлення нових пристроїв (рис 3.1). Завдяки модульній структурі проєкту, кожен логічний блок винесений у відповідний модуль, що забезпечує зручність у супроводі коду, тестуванні та масштабуванні системи.

Інтерфейс користувача розгортається за допомогою HTML-шаблонів, які можуть бути доповнені CSS-стилями для покращення вигляду. Після входу на головну сторінку користувач бачить таблицю всіх відомих MAC-адрес, може змінювати їх статус доступу або ініціювати сканування мережі.

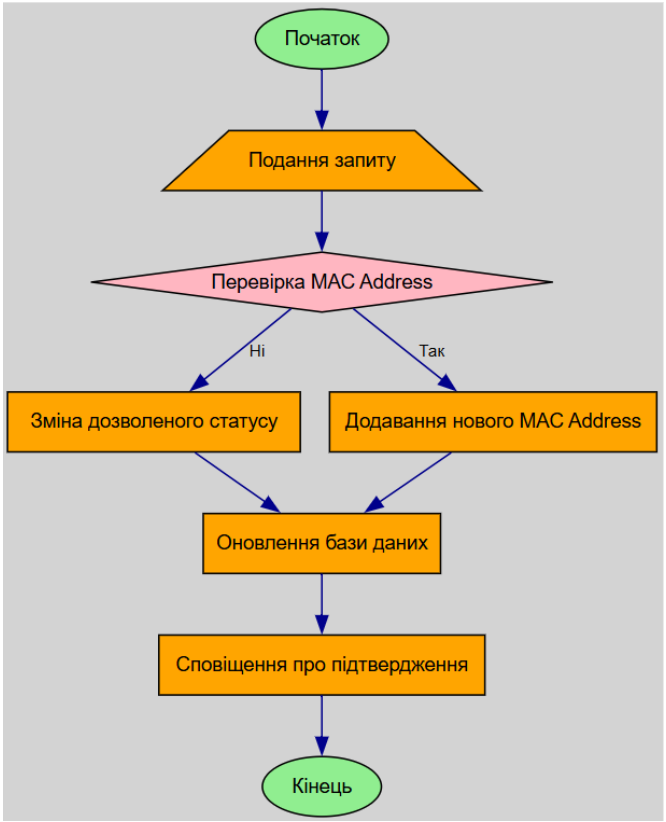


Рисунок 3.1 – Процес валідації MAC-адреси

Асинхронна реалізація сканування (на основі asyncio) дозволяє не блокувати основний потік програми, забезпечуючи кращу продуктивність при виконанні мережевих операцій. Обробка форм реалізована з використанням стандартних інструментів Flask – request, flash, redirect, що дозволяє гнучко реагувати на помилки введення або зміну статусів MAC-адрес.

Одним із важливих аспектів є збереження та обробка даних у базі. Сервер використовує SQLAlchemy – потужну ORM бібліотеку, яка дозволяє працювати з базою даних на рівні Python-об'єктів. Це не лише спрощує розробку, але й значно зменшує кількість помилок, пов’язаних із прямими SQL-запитами. База може бути реалізована на SQLite, що підходить для прототипування, або на більш потужному рушії, як-от PostgreSQL, залежно від масштабів системи.

Розгортання сервера може бути здійснене на різних платформах: від локального ПК до хмарних рішень, або навіть на вбудованих пристроях, таких як

Raspberry Pi. Це дозволяє адаптувати систему до конкретного сценарію використання, враховуючи технічні обмеження та вимоги користувача.

Як виглядає запущений сервер можна розглянути на (рис 3.2).

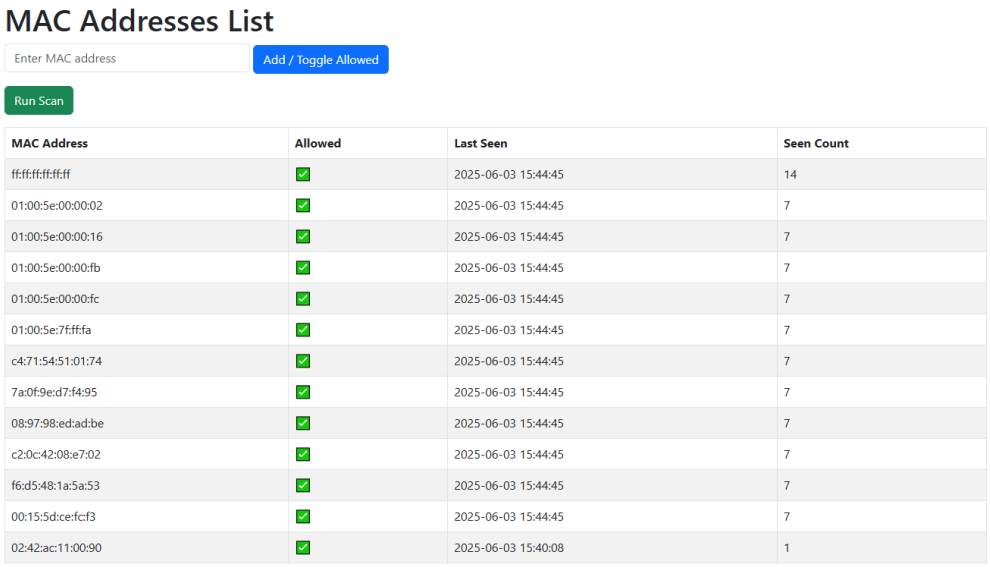


Рисунок 3.2 – Загальний вигляд запущеого сервера

3.3 Опис реалізації системи сканування мережі та реєстрації MAC-адрес

В рамках розробки комплексного серверного рішення для моніторингу та керування пристроями в локальній мережі надзвичайно важливою складовою є модуль сканування мережі. Його основна задача – виявлення активних пристроїв, зчитування їхніх MAC-адрес, ведення статистики та забезпечення автоматичної взаємодії з маршрутизатором для керування доступом. У цьому підрозділі розглянемо архітектуру, логіку та технічну реалізацію сканера, що взаємодіє з API маршрутизатора та базою даних.

Модуль сканування (scanner.py) реалізовано мовою програмування Python із використанням асинхронної парадигми на основі бібліотеки asyncio, що дозволяє ефективно сканувати десятки або сотні IP-адрес без блокування основного потоку виконання. Основна функція (scan_and_register) – ініціює процес пінгування всієї підмережі, збирає ARP-таблицю з інформацією про активні MAC-адреси та

взаємодіє з базою даних і API маршрутизатора (рис 3.3).

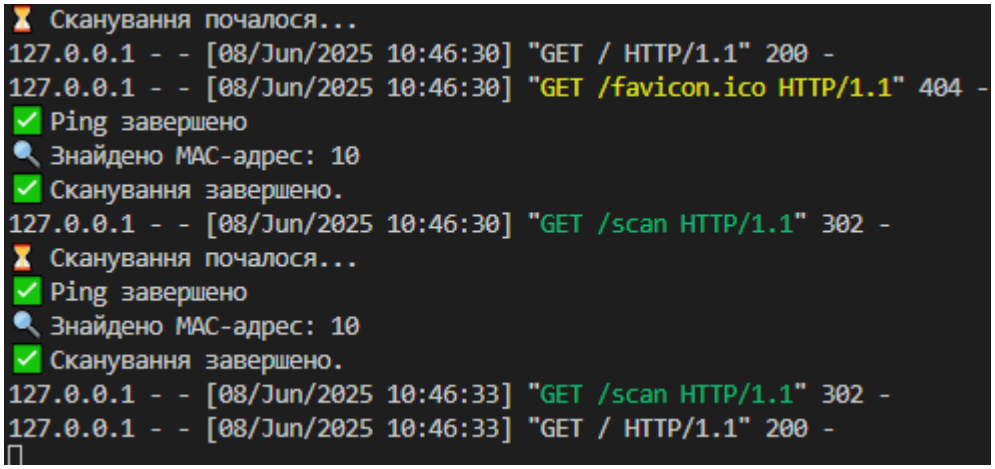


Рисунок 3.3 – Приклад запуску сканування

Функція get_local_ip() визначає поточну IP-адресу пристрою, на якому запущено сервер. Це досягається шляхом створення сокет-з'єднання з публічним DNS-сервером Google (8.8.8.8), що дозволяє точно отримати локальну адресу навіть у випадках наявності декількох інтерфейсів.

На основі отриманої адреси генерується підмережа класу /24, що охоплює до 254 пристроїв. За допомогою функції ping_ip() асинхронно викликається утиліта ping для кожного IP у мережі. Це дозволяє примусово "розбудити" пристрої, щоб вони потрапили в ARP-таблицю. Такий підхід гарантує, що навіть сплячі або недавно підключені пристрої будуть виявлені.

Функція get_arp_table() виконує системний виклик arp -a, зчитує таблицю ARP та парсить її регулярними виразами, витягуючи IP-адреси та відповідні MAC-адреси. Ці пари зберігаються у словнику для подальшої обробки.

Кожна MAC-адреса перевіряється на наявність у базі. Якщо пристрій уже відомий, оновлюється дата його останнього виявлення (last_seen) та кількість виявлень (seen_count). Якщо пристрій новий – створюється новий запис, і MAC-адреса додається до списку new_devices.

Для кожного нового пристрою модуль звертається до API маршрутизатора (через об'єкт router, який реалізує клас RouterAPI) і виконує запит на додавання

MAC-адреси у whitelist. Якщо операція успішна, поле allowed у базі оновлюється на True. У випадку помилки – сервер виводить повідомлення, але залишає запис як "неавторизований".

Завдяки asyncio.gather сканування мережі проходить у десятки разів швидше, ніж при синхронному виклику ping.

Сканер можна адаптувати до підмереж будь-якого класу (не лише /24), достатньо змінити ip_interface(local_ip).

Підтримка маршрутизатора як зовнішнього контролера дозволяє не лише фіксувати пристрої, а й керувати їх доступом.

Один запуск функції і система самостійно пінгує, виявляє, перевіряє, додає нові пристрої в базу та whitelist (рис 3.4).

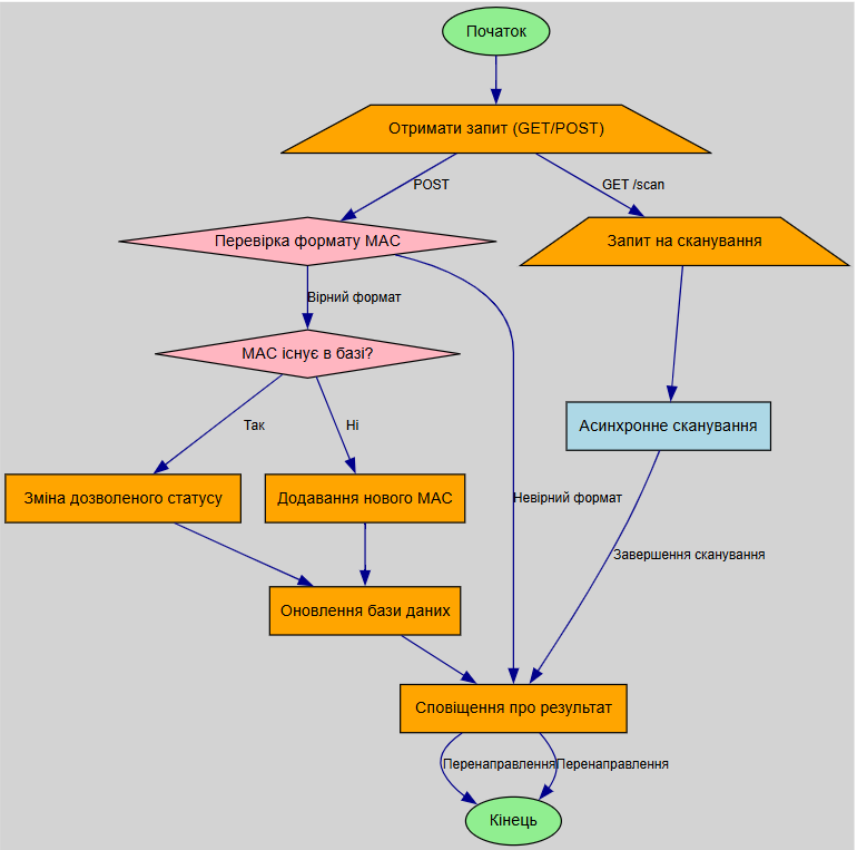


Рисунок 3.4 – Асинхронне пінгування

Модуль сканування є критично важливим компонентом у системі керування локальною мережею. Його ефективність, швидкість та гнучкість реалізації

дозволяють створити адаптивну інфраструктуру для моніторингу, виявлення та авторизації пристроїв у режимі реального часу. Завдяки цій реалізації, адміністратор може швидко реагувати на підключення нових клієнтів до мережі та автоматизувати процес контролю доступу, що значно підвищує безпеку та зручність керування мережею.

3.4 Опис реалізації тестового емулятора маршрутизатора для взаємодії з MAC-фільтрацією

У рамках побудови кластерної інфраструктури на базі Raspberry Pi важливу роль відіграє управління доступом до мережі. Одним з ефективних методів контролю є фільтрація пристроїв за MAC-адресами, яка зазвичай реалізується на рівні маршрутизатора або комутатора. Проте для тестування, налагодження та імітації подібної взаємодії у середовищі розробки необхідно створити відповідну модель маршрутизатора, яка дозволяє відтворити функціональність управління "біліми списками" MAC-адрес без потреби в реальному мережевому обладнанні.

Клас RouterAPI є імітаційною моделлю програмного інтерфейсу маршрутизатора, що дозволяє здійснювати базові операції з додавання та видалення MAC-адрес у whitelist. Хоча він не взаємодіє з реальним мережевим обладнанням, його логіка максимально наближена до очікуваної поведінки справжнього API маршрутизатора. Цей підхід дозволяє тестувати функціональність сканера, перевіряти обробку запитів, симулювати час відгуку і відстежувати результат виконання операцій у контрольованому середовищі.

Використання RouterAPI у дослідницькому середовищі має низку суттєвих переваг, які стають критично важливими під час розробки та тестування мережевих систем.

Слід відзначити безпечність, яку забезпечує ця симуляційна модель. Оскільки RouterAPI працює у відокремленому середовищі, яке не має прямого зв’язку з реальними мережевими пристроями, це дозволяє уникнути будь-якого

впливу на продуктивну або навчальну мережу. Іншими словами, можна вільно експериментувати, змінювати логіку, перевіряти обробку виняткових ситуацій, не ризикуючи порушити стабільність функціонування мережевих компонентів у реальному світі. Це особливо актуально в умовах освітніх лабораторій, наукових експериментів або первинної розробки систем, де помилки є частим явищем, і бажано мати можливість «безболісного» тестування.

Ще одним важливим аспектом є контроль, який надає RouterAPI розробнику. У реальному світі, щоб протестувати певну логіку, доводиться взаємодіяти з фізичними пристроями, часто з обмеженим доступом до їхнього програмного інтерфейсу. Натомість, симульований маршрутизатор у вигляді Python-класу дозволяє змінювати поведінку з високою гнучкістю: можна вручну або програмно вводити помилки, моделювати несправності, змінювати затримки відповіді API, навіть штучно створювати перевантаження системи. Такий підхід дає змогу створювати різноманітні сценарії від звичайних до граничних і аномальних, і вивчати, як система на них реагує.

Щодо швидкості розробки, то тут RouterAPI відіграє неоціненну роль. У більшості випадків для повноцінної перевірки взаємодії з маршрутизатором необхідно мати фізичний пристрій, налаштувати його, отримати доступ до API, пройти процедуру авторизації, опрацювати протокол, провести налагодження. Усе це займає багато часу, потребує спеціального обладнання і часто не є можливим на ранніх етапах розробки. Завдяки RouterAPI, ці кроки можна обійти, зосередившись лише на логіці роботи та забезпеченні коректної інтеграції. Тестування відбувається швидко, без потреби в додаткових ресурсах, що значно пришвидшує ітераційний цикл програміста.

Не менш важливою є можливість ефективної інтеграції з іншими модулями системи. RouterAPI був спеціально розроблений таким чином, щоб легко взаємодіяти з іншими компонентами, зокрема з модулем сканування мережі scan_and_register. Така архітектурна сумісність дозволяє будувати цілісні симуляційні ланцюжки, які точно відтворюють поведінку всієї системи.

Наприклад, результат сканування ARP-таблиці одразу передається до API маршрутизатора, який приймає рішення про додавання чи видалення MAC-адреси. Усе це відбувається автоматично і в реальному часі, що ідеально підходить для відлагодження, побудови прототипів або підготовки до реального розгортання системи у виробничому середовищі.

Симульований API маршрутизатора – це не просто зручність, а необхідний інструмент для створення надійної, масштабованої та гнучкої системи. Його застосування дозволяє зосередитися на логіці, перевірити роботу ключових компонентів, і лише потім переходити до реальної інтеграції з апаратними засобами.

У майбутньому цей клас можна значно розширити, додавши функції авторизації та автентифікації, що дозволить більш надійно контролювати доступ користувачів і захищати систему від несанкціонованого використання. Окрім цього, доцільно впровадити механізми імітації помилок, наприклад, перевищення ліміту MAC-адрес, що допоможе ефективно тестувати стійкість і поведінку системи у критичних ситуаціях. Ще одним важливим напрямком розвитку є підтримка одночасного використання білого та чорного списків, що дасть змогу гнучко керувати доступом, комбінуючи дозволені й заборонені адреси чи користувачів. Для зручного збереження та відновлення стану whitelist можна реалізувати серіалізацію, що забезпечить безпеку й простоту роботи з цими даними.

Для інтеграції з іншими системами і забезпечення сучасних можливостей взаємодії, варто додати підтримку REST-API через HTTP-запити, що дозволить здійснювати комунікацію з класом по мережі і використовувати його функціонал у розподілених додатках. Усі ці напрямки разом створять більш потужний, гнучкий і надійний інструмент, який буде готовий до складних задач у майбутньому.

Клас RouterAPI – це ключовий елемент розробки тестового середовища, який дозволяє моделювати поведінку маршрутизатора під час додавання або видалення пристроїв на основі MAC-адрес. Його асинхронна природа і простота дозволяють

ефективно взаємодіяти з іншими компонентами системи, що істотно покращує якість та гнучкість процесу розробки й тестування.

3.5. Опис реалізації моделі для збереження MAC-адрес

У цьому підрозділі детально розглянемо процес створення моделі даних для роботи з MAC-адресами на прикладі коду, реалізованого з використанням бібліотеки SQLAlchemy одного з найбільш популярних інструментів ORM (Object-Relational Mapping) для Python. ORM дозволяє працювати з базою даних у вигляді об’єктів, приховуючи складнощі прямої роботи з SQL-запитами, що значно спрощує розробку і підтримку проєктів.

Визначення базового класу для моделей. Для цього використовується функція declarative_base(), яка створює базовий клас Base. Всі подальші моделі будуть наслідуватися від цього класу, що забезпечить автоматичну інтеграцію з системою ORM і створення відповідних таблиць у базі даних.

Ключовим компонентом є клас MacAddress, який відображає структуру таблиці у базі даних під назвою mac_addresses. Його головна мета зберігати інформацію про окремі MAC-адреси, а також додаткові дані, що стосуються їх статусу і статистики використання.

Структура класу містить кілька полів, кожне з яких відповідає окремому стовпцю в таблиці:

- id;
- mac;
- allowed;
- last_seen;
- seen_count.

Для зв’язку з базою даних застосовується механізм движка (engine), який у нашому випадку налаштований на використання SQLite легкої вбудованої бази даних, яка не потребує окремого серверного процесу. Параметр 'sqlite:///macs.db'

означає, що база зберігатиметься у файлі macs.db у поточній директорії проєкту.

Після визначення структури моделі, викликається команда Base.metadata.create_all(engine), яка створює всі таблиці у базі, відповідно до описаних моделей, якщо вони ще не існують. Цей крок необхідний для ініціалізації схеми даних перед початком роботи з ними.

Для організації роботи з базою даних і виконання операцій додавання, оновлення чи вилучення записів використовується сесія – обгортка, яка керує транзакціями і підтримує зв'язок між програмним кодом і базою. Сесія створюється через фабрику sessionmaker, в яку передається раніше налаштований движок. Це дозволяє у будь-який момент відкрити сесію і здійснювати необхідні операції з об'єктами моделі, а потім комітити зміни до бази даних.

Такий підхід має ряд важливих переваг. По-перше, використання ORM знижує рівень помилок, пов'язаних із прямою роботою з SQL, оскільки структура даних описується у вигляді класів, а не сирих текстових запитів. По-друге, модель є прозорою і зручною для розуміння інші розробники легко можуть прочитати код і зрозуміти, які дані зберігаються і як вони використовуються. По-третє, реалізація з SQLAlchemy дає змогу переносити проєкт на інші СУБД з мінімальними змінами коду, адже движок налаштовується конфігурацією і не прив'язаний жорстко до SQLite.

Водночас, у представленій реалізації є потенціал для подальшого розвитку. Наприклад, можна додати валідацію формату MAC-адреси перед збереженням, що гарантуватиме коректність даних. Також логіка оновлення полів last_seen і seen_count при повторному виявленні MAC-адреси може бути винесена у методи класу, що зробить код більш організованим та зручним для підтримки.

Описана модель є фундаментальним компонентом системи, яка відповідає за збереження та обробку інформації про MAC-адреси. Її структура і способи взаємодії з базою даних закладають основу для подальших функціональних розширень і впровадження бізнес-логіки, спрямованої на контроль доступу, моніторинг пристроїв та аналіз їх активності у системі.

3.6. Опис реалізації Telegram-бота для сповіщень про нові пристрої в мережі

Процес створення Telegram-бота, який виконує функцію оперативного інформування користувача про появу нових пристроїв у мережі на основі їх MAC-адрес. Такий підхід є сучасним і ефективним способом нотифікації, адже Telegram має широку аудиторію, підтримує багатий функціонал для роботи з повідомленнями та дозволяє легко інтегруватися з іншими системами.

Основою реалізації слугує використання офіційної бібліотеки python-telegram-bot або просто telegram (залежно від версії), яка надає об’єкти та методи для взаємодії з Telegram API. У наведеному прикладі показано асинхронний підхід, що дозволяє не блокувати основний потік програми під час відправлення повідомлень, підвищуючи ефективність і масштабованість.

Спочатку в коді визначаються ключові параметри такі як token – це унікальний токен доступу до конкретного Telegram-бота, який генерується через BotFather в Telegram. Цей токен необхідно зберігати в безпечному місці і не поширювати публічно, щоб уникнути несанкціонованого доступу.

Для розуміння кому повідомлення надсилатимустья використовується chat_id – ідентифікатор чату або користувача, якому надсилатимуться повідомлення. Він може бути отриманий різними способами, наприклад, через спеціальні API-запити або бота, що відправляє свій ідентифікатор.

Далі створюється об’єкт бота за допомогою класу Bot, якому передається токен. Це забезпечує автентифікацію і дозволяє виконувати подальші дії, такі як відправлення повідомлень.

Головна функція в коді – notify(mac), яка приймає параметр mac, що є рядком з MAC-адресою нового пристрою. Функція асинхронна (async def), що дозволяє використовувати конструкцію await для виклику методів бота без блокування виконання. У середині функції формується текст повідомлення з використанням емодзі, що робить сповіщення більш помітним і привабливим для користувача.

Потім виконується відправлення повідомлення методом send_message, куди передається ідентифікатор чату та сформований текст.

Використання асинхронності є особливо важливим у контексті реальних додатків, де одночасно можуть надходити численні сповіщення. Це дозволяє обробляти їх без затримок і не зупиняти інші операції, що підвищує продуктивність і користувацький досвід.

Блок if __name__ == "__main__": є класичною конструкцією у Python, що забезпечує виконання тестового запуску скрипта лише при його безпосередньому запуску, а не імпорті як модуля. Тут для демонстрації викликається функція notify з прикладом MAC-адреси (рис 3.5). Виклик обгорнутий у asyncio.run(), що запускає асинхронну корутину у головному потоці, забезпечуючи правильну роботу асинхронного коду.

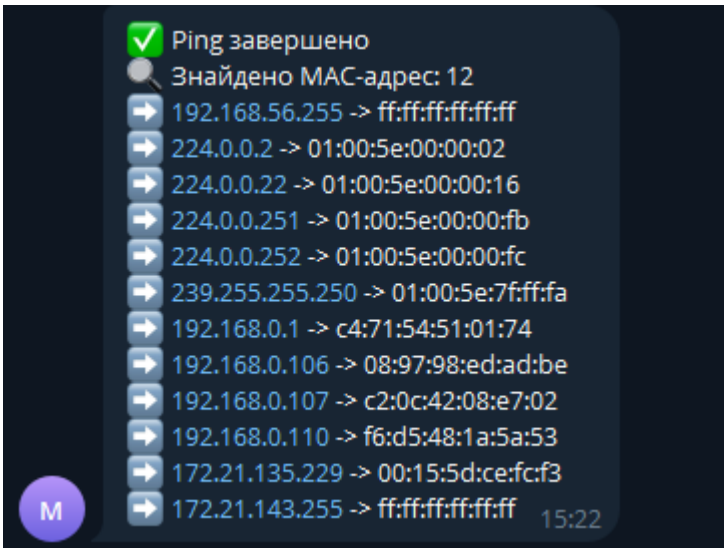


Рисунок 3.5 – Приклад сповіщення

Загальна структура і логіка коду робить цю реалізацію простою, легкою для розуміння і подальшого розширення. Наприклад, у майбутньому можна додати обробку помилок, щоб враховувати можливі проблеми з мережею або недоступністю Telegram-сервісу, а також реалізувати чергу повідомлень для уникнення перевантаження.

Крім того, інтеграція цього бота з системою моніторингу мережі або базою даних MAC-адрес дозволить автоматизувати процес сповіщення: при виявленні нового пристрою система одразу відправлятиме повідомлення користувачеві, що значно підвищить оперативність реагування на потенційні загрози чи аномалії.

Важливо відзначити, що Telegram-боти підтримують широкий спектр функцій, включно з кнопками, меню, обробкою команд і навіть мультимедійними повідомленнями. Це відкриває можливості для подальшого розвитку наприклад, додавання інтерфейсу для підтвердження або відхилення нових пристроїв, отримання детальної статистики або інтерактивного керування списками дозволених MAC-адрес безпосередньо через чат.

Реалізація Telegram-бота для сповіщень про нові пристрої є сучасним, гнучким і потужним інструментом, який суттєво покращує систему моніторингу мережевої безпеки, дозволяючи миттєво інформувати відповідальних осіб і оперативно реагувати на події. Це забезпечує підвищення рівня безпеки, зручності управління та прозорості процесів у будь-яких мережевих середовищах від невеликих локальних мереж до складних корпоративних інфраструктур.

3.6. Опис реалізації інтерфейсу адміністратора

Для зручності управління та моніторингу роботи кіберфізичної системи було реалізовано адміністративний веб-інтерфейс, який надає можливість візуально керувати списком пристроїв, що підключаються до Wi-Fi мережі. Цей інтерфейс є спрощеним веб-застосунком на основі HTML-шаблонів із використанням фреймворку Flask та CSS-бібліотеки Bootstrap для адаптивного і зрозумілого відображення інформації.

На головній сторінці інтерфейсу представлено таблицю з переліком усіх пристроїв, які були виявлені в мережі.

Для кожного пристрою відображаються такі характеристики:

- mac-адреса;

– статус доступу (дозволено або заборонено);
– час останнього виявлення;
– кількість виявлень;
– форма додавання/зміни статусу MAC-адреси.

У створеній кіберфізичній системі контролю доступу до Wi-Fi мережі ключовим елементом інтерфейсу адміністратора є форма, розміщена безпосередньо над таблицею зі списком пристроїв. Дана форма реалізована у вигляді текстового поля з кнопкою, що дозволяє вручну ввести MAC-адресу пристрою, який адміністратор хоче додати до системи або змінити його статус доступу. При введенні даних у відповідне поле, передбачено автоматичну перевірку правильності формату введеної MAC-адреси. Для цього використовується регулярний вираз ^([0-9A-Fa-f]{2}:){5}([0-9A-Fa-f]{2})$, який забезпечує відповідність стандартному формату MAC (тобто шість пар шістнадцяткових чисел, розділених двокрапками). Такий підхід дозволяє забезпечити базову перевірку ще на клієнтському рівні без необхідності одразу звертатися до серверної частини, що знижує навантаження на сервер та мінімізує помилки користувача.

Після натискання кнопки відправки форми система виконує обробку введеної MAC-адреси. Якщо така адреса ще не міститься у базі даних, вона буде додана автоматично з параметрами за замовчуванням. У разі, якщо ця адреса вже є в базі, система змінює її статус доступу, використовуючи логіку перемикання (toggle): якщо пристрій раніше був дозволений до підключення він буде заблокований, і навпаки. Адміністратор отримує простий, але ефективний інструмент для управління списком дозволених пристроїв у локальній мережі. Результат операції одразу ж відображається на екрані за допомогою динамічних повідомлень: у разі успіху, у вигляді зеленого сповіщення, а у випадку помилки (наприклад, при введенні некоректної MAC-адреси або внутрішній помилці додавання), у вигляді червоного повідомлення. Для реалізації цих повідомлень використовується механізм flash у Flask, який дозволяє передати коротке повідомлення між запитами

та динамічно відобразити його у шаблоні.

Окрім можливості вручну керувати MAC-адресами, інтерфейс адміністратора передбачає також функціонал активного сканування мережі. На сторінці присутня окрема кнопка з підписом "Run Scan", натискання на яку дозволяє адміністратору ініціювати процес сканування локального сегмента Wi-Fi-мережі. Цей функціонал особливо корисний у ситуаціях, коли необхідно оперативно виявити нові пристрої, які щойно з’явились у мережі, або перевірити актуальний статус пристроїв у реальному часі. При запуску сканування система аналізує ARP-таблиці, мережевий трафік або використовує утиліти командного рядка для виявлення активних пристроїв та фіксації їхніх MAC-адрес. Після завершення сканування інформація оновлюється в базі даних, і адміністратор бачить актуальні результати у відповідній таблиці.

З технічної точки зору проєкт реалізовано мовою програмування Python із використанням мікрофреймворку Flask, що є зручним інструментом для швидкої побудови легких веб-додатків. У якості механізму шаблонізації використовується Jinja2 гнучкий та потужний шаблонізатор, який дозволяє зручно інтегрувати динамічні дані у HTML-структуру, дотримуючись принципів відокремлення логіки від представлення. Сторінка оформлена за допомогою CSS-фреймворку Bootstrap, що забезпечує адаптивний та привабливий зовнішній вигляд без потреби в розробці складних стилів з нуля. Це також дозволяє швидко оформити таблиці, повідомлення та кнопки у візуально привабливий спосіб, придатний для використання навіть у професійному середовищі.

Зберігання інформації про MAC-адреси, статус доступу, кількість виявлень та час останнього виявлення реалізовано через базу даних. У якості ORM (об’єктно-реляційного відображення) можливо використано SQLAlchemy, що забезпечує зручну роботу з реляційною базою через Python-класи. У простішому варіанті реалізації може використовуватись вбудована база sqlite3, яка не потребує окремого серверного ПЗ і підходить для локальних чи малих інсталяцій. Саме така гнучкість дозволяє масштабувати систему в залежності від потреб: від невеликої

домашньої мережі до більших середовищ, наприклад, у навчальних закладах чи офісах.

Веб-інтерфейс адміністратора, реалізований у цій системі, поєднує в собі зручність користування, ефективне управління доступом і достатній рівень технічної деталізації, що робить його важливою складовою всієї кіберфізичної інфраструктури контролю мережевого доступу на основі MAC-ідентифікації.

3.7. Висновки до третього розділу

У третьому розділі було здійснено комплексну реалізацію кіберфізичної системи автоматизації процесу реєстрації пристроїв у Wi-Fi мережах на основі ідентифікації за MAC-адресами. Кожен підрозділ цього розділу відіграв важливу роль у формуванні цілісної архітектури системи, яка об'єднує апаратне забезпечення, серверну логіку, інструменти сканування, механізми обробки даних та засоби взаємодії з користувачем у вигляді Telegram-бота та веб-інтерфейсу.

Розробка та реалізація модулів апаратного і програмного забезпечення стали основою для побудови автономного пристрою, здатного здійснювати моніторинг мережі у реальному часі.

Сервер програмно-технічного засобу реалізовував логіку обробки запитів, зберігання даних у базі, управління MAC-адресами та надання інтерфейсу адміністрування. Використання Python та веб-фреймворку Flask дозволило створити легкий, проте гнучкий серверний компонент, здатний реагувати на запити, ініціювати сканування мережі, відображати інформацію про пристрої та забезпечувати авторизацію/обмеження доступу до ресурсів. Серверна частина стала зв'язуючою ланкою між апаратною частиною системи, базою даних і зовнішніми інтерфейсами.

Особливо важливою складовою стала реалізація системи сканування мережі, що дала змогу виявляти пристрої, які підключаються до Wi-Fi. Для цього були використані утиліти командного рядка (наприклад, arp-scan, ip neigh, nmap), які інтегрувалися у Python-скрипти для періодичного або ручного запуску сканування.

Результати сканування оброблялись і записувались у базу, де кожен пристрій ідентифікувався за унікальною MAC-адресою. Такий підхід забезпечує надійне виявлення пристроїв навіть у випадках зміни IP-адрес, що особливо важливо в динамічних мережах.

З метою моделювання взаємодії з реальним маршрутизатором було створено тестовий емулятор маршрутизатора, що імітує поведінку пристрою з підтримкою MAC-фільтрації. Це дало змогу протестувати сценарії блокування або дозволу доступу на основі MAC-адреси без необхідності використання фізичного мережевого обладнання. Такий симулятор значно спростив процес налагодження та дозволив уникнути небажаних збоїв у реальній мережі під час розробки.

Центральним елементом програмної архітектури стала модель для збереження MAC-адрес, що дозволила структурувати інформацію про підключені пристрої. У базі даних зберігались такі поля, як сама MAC-адреса, статус доступу (дозволено або заблоковано), час останнього виявлення та кількість виявлень. Така структура бази є оптимальною для задач моніторингу, дозволяє швидко здійснювати фільтрацію, оновлення та логування історії змін, а також формує основу для побудови аналітичних інструментів у майбутньому.

Для забезпечення своєчасного інформування адміністратора про нові підключення було реалізовано Telegram-бота, який відправляє повідомлення при виявленні нових MAC-адрес у мережі. Цей бот став ефективним способом нотифікації у режимі реального часу, не потребуючи постійного контролю через веб-інтерфейс. Telegram як канал комунікації є зручним, широко доступним і дозволяє легко масштабувати повідомлення на декількох адміністраторів одночасно. Реалізація інтеграції з Telegram API стала ефективною демонстрацією можливостей поєднання систем автоматизації з сучасними засобами мобільного сповіщення.

У третьому розділі було створено повноцінну кіберфізичну систему, що поєднує апаратну платформу з розгалуженим програмним забезпеченням, базою даних, веб-інтерфейсом адміністратора та інструментами зовнішнього оповіщення.

Всі складові працюють як єдина система для виявлення, фіксації, контролю та адміністрування доступу до бездротової мережі. Отримані результати підтверджують ефективність обраної архітектури та демонструють готовність рішення до використання в умовах, наближених до реальних експлуатаційних сценаріїв. Реалізований підхід може бути успішно адаптований для інших задач моніторингу мережевої активності, зокрема в освітніх установах, офісах, коворкінгах або IoT-системах.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень було розроблено та реалізовано кіберфізичну систему автоматизації процесу реєстрації пристроїв у Wi-Fi мережах на основі MAC-адрес. Запропонована система забезпечує виявлення нових пристроїв, їх автоматичну реєстрацію, контроль доступу до мережі та сповіщення адміністратора через Telegram-бот. Створене рішення поєднує апаратні й програмні компоненти у цілісну систему, здатну функціонувати у реальному середовищі та забезпечувати підвищений рівень контролю в локальній мережі без необхідності ручного адміністрування.

У першому розділі проведено глибокий аналіз предметної області, виявлено актуальні проблеми та сформульовано основні завдання, які потребують вирішення у контексті автоматизації процесу реєстрації пристроїв у бездротових мережах. Було досліджено принципи ідентифікації клієнтів у Wi-Fi мережах, звернено увагу на методи MAC-фільтрації як одного з найпоширеніших механізмів контролю доступу. Також здійснено порівняльну оцінку існуючих рішень, їх переваг та обмежень, що дало змогу визначити нішу для вдосконалення. У результаті було чітко сформульовано задачу дослідження, створення автоматизованої системи реєстрації та контролю доступу, здатної самостійно виявляти нові пристрої, фіксувати їх у базі та оперативно інформувати адміністратора.

У другому розділі проведено проектування архітектури кіберфізичної системи. Визначено склад апаратного та програмного забезпечення, яке є необхідним для реалізації функціоналу. Основним апаратним елементом обрано одноплатний комп’ютер, що забезпечує достатню обчислювальну потужність для сканування мережі та обробки даних. Програмну частину реалізовано із застосуванням Python, Flask, SQLite, що дозволяє досягти гнучкості, модульності та масштабованості. У розділі детально описано архітектуру системи, взаємодію між її модулями, обмін даними, а також засоби збереження інформації про пристрої. Проведено аналіз існуючих аналогів у сфері кіберфізичних систем та

підкреслено переваги розробленого підходу, зокрема, в контексті адаптивності та можливості інтеграції з зовнішніми сервісами. Особливу увагу приділено питанням впровадження, визначено вимоги до середовища розгортання, обґрунтовано вибір платформ, бібліотек та технологій.

У третьому розділі детально описано реалізацію основних модулів системи. Здійснено розробку сервера, що забезпечує прийом і обробку даних, ведення бази MAC-адрес та веб-інтерфейсу для адміністратора. Реалізовано механізм сканування мережі для автоматичного виявлення нових пристроїв та фіксації відповідних MAC-адрес. Для перевірки взаємодії реалізовано тестовий емулятор маршрутизатора, що дозволив безпечне тестування функцій доступу та блокування. Особливу увагу приділено моделі збереження MAC-адрес, яка включає статус доступу, час останнього виявлення та кількість спостережень, що дозволяє вести облік активності пристроїв у мережі. Додатково розроблено Telegram-бота, який здійснює сповіщення адміністратора в реальному часі, що значно покращує реакцію на появу нових або невідомих пристроїв у мережі. Завдяки інтеграції всіх компонентів створено повноцінну систему, яка не лише автоматизує процес реєстрації пристроїв, а й підвищує рівень безпеки локальної мережі.

У підсумку, виконано повний цикл створення кіберфізичної системи від постановки проблеми та проектування архітектури до практичної реалізації та тестування. Запропоноване рішення відзначається ефективністю, простотою використання та можливістю подальшого масштабування і інтеграції в існуючі інфраструктури. Такий підхід є актуальним у контексті зростання кількості IoT-пристроїв, а також в умовах, коли контроль за мережевою інфраструктурою потребує високого рівня автоматизації та надійності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Фото Smart City. URL: https://media.istockphoto.com/id/531919096/tr/vekt%C3%B6r/smart-city-concept-and-internet-of-things.jpg?s=2048x2048&w=is&k=20&c=XXc eLxwREf7439cKVz4Nt2v6I_sfO2w2xdRt1H_id0= (дата звернення: 12.05.2025).

2. Zhen B. Li H.B. Kohno R. Networking issues in medical implant communications. *International Journal of Multimedia and Ubiquitous Engineering*. 2009. Vol. 4. P. 23–38.

3. Kaleem M. Mahapatra M.R. Energy Consumption Using Network Stability and Multi-hop Protocol for Link Efficiency in Wireless Body Area Networks. *IOSR Journal of Computer Engineering*. 2014. Vol. 16. P. 113–120.

4. Maamar S. Ramdane M. Azeddine B. Mohamed B. Contention Window Optimization: An enhancement to IEEE 802.11 DCF to improve Quality of Service. *International Journal of Digital Information and Wireless Communications*. 2011. Vol. 1. P. 273–383.

5. Salam A. Nadeem A. Ahsan K. Sarim M. Rizwan K. A class based QoS model for Wireless Body Area Sensor Networks. *Research Journal of Recent Sciences*. 2014. Vol. 3. P. 69–78.

6. Uzungenc S. Dag T. A QoS Efficient Scheduling Algorithm for Wireless Sensor Networks. *International Journal of Innovative Technology and Exploring Engineering*. 2015. Vol. 4. P. 48–50.

7. Mustafa M.S. Alyasiri H. Implementation of End-to-End QoS Mapping Scheme on SCIS WiFi Network. *International Journal of Computer Science*. 2014. Vol. 11. P. 95–101.

8. Maadani M. Motamedi S.A. Contention Window Adjustment in IEEE 802.11-Based Industrial Wireless Networks. *International Journal of Electronics and Communication Engineering*. 2015. Vol. 9. P. 1275–1280.

9. Syed I. Shin S.-H. Roh B.-H. Adnan M. Performance Improvement of QoS-Enabled WLANs Using Adaptive Contention Window Backoff Algorithm. *IEEE Systems*

Journal. 2018. Vol. 12. P. 3260–3270.

10. Hirzallah M. Afifi W. Krunz M. Provisioning QoS in Wi-Fi Systems with Asymmetric Full-Duplex Communications. *IEEE Transactions on Cognitive Communications and Networking*. 2018. Vol. 4. P. 942–953.

11. López Rodríguez F. Silva Dias U. Campelo D.R. de Oliveira Albuquerque R. Lim S.-J. Villalba L.J.G. *QoS Management and Flexible Traffic Detection Architecture for 5G Mobile Networks*. Sensors. 2019. Vol. 19. P. 1335.

12. Ningombam D.D. Shin S. *Optimal Resource Management and Binary Power Control in Network-Assisted D2D Communications for Higher Frequency Reuse Factor*. Sensors. 2019. Vol. 19. P. 251.

13. Dahan F. El Hindi K. Mathkour H. AlSalman H. *Dynamic Flying Ant Colony Optimization* (DFACO) *for Solving the Traveling Salesman Problem*. Sensors. 2019. Vol. 19. P. 1837.

14. Xia F. Ma L. Dong J. Sun Y. Network QoS Management in Cyber-Physical Systems. In: *Proceedings of the International Conference on Embedded Software and Systems Symposia*, Sichuan, China, 29–31 July 2008.

15. López Rodríguez F. Silva Dias U. Campelo D.R. de Oliveira Albuquerque R. Lim S.-J. Villalba L.J.G. *QoS Management and Flexible Traffic Detection Architecture for 5G Mobile Networks*. Sensors. 2019. Vol. 19. P. 1335.

16. Ningombam D.D. Shin S. *Optimal Resource Management and Binary Power Control in Network-Assisted D2D Communications for Higher Frequency Reuse Factor*. Sensors. 2019. Vol. 19. P. 251.

17. Wolf W. Cyber-physical systems. Computer. 2009. Vol. 42(3). P. 88–89.

18. Gupta R.A. Chow M.-Y. *Networked control system: overview and research trends. IEEE Transactions on Industrial Electronics*. 2010. Vol. 57(7). P. 2527–2535.

19. Hespanha J.P. Naghshtabrizi P. Xu Y. *A survey of recent results in networked control systems. Proceedings of the IEEE*. 2007. Vol. 95(1). P. 138–162.

20. Wang Z. Wang L. *Occupancy pattern based intelligent control for improving energy efficiency in buildings. Proceedings of the IEEE Int. Conf. on Automation Science*

and Engineering. 2012. P. 804–809.

21. Sookoor T. Whitehouse K. RoomZoner. *Occupancy-based room-level zoning of a centralized HVAC system. Proceedings of the 4th ACM/IEEE Int. Conf. on Cyber-Physical Systems*. 2013. P. 209–218.

22. Dawson-Haggerty S. Jiang X. Tolle G. Ortiz J. Culler D. sMAP. *A simple measurement and actuation profile for physical information*. 2010. P. 197–210.

23. Cao X. Chen J. Xiao Y. Sun Y. *Building-environment control with wireless sensor and actuator networks: centralized versus distributed. IEEE Transactions on Industrial Electronics*. 2010. Vol. 57(11). P. 3596–3605.

24. Mady A.E.-D. Provan G. Wei N. *Designing cost-efficient wireless sensor/actuator networks for building control systems*. 2012. P. 138–144.

25. Yahiaouti A. Sahraoui A.-E.-K. *A framework for distributed control and building performance simulation*. 2012. P. 232–237.

26. Kastner W. Neugschwandtner G. Soucek S. Newman H.M. *Communication systems for building automation and control. Proceedings of the IEEE*. 2005. Vol. 93(6). P. 1178–1203.

27. Erickson V.L. Achleitner S. Cerpa A.E. POEM. *Power-efficient occupancy-based energy management system*. 2013. P. 203–216.

28. Dobbs J.R. Hencey B.M. *Model predictive HVAC control with online occupancy model. Energy & Building*s. 2014. Vol. 82. P. 675–684.

29. Váňa Z. Cigler J. Široký J. Žáčeková E. Ferkl L. *Model-based energy efficient control applied to an office building. Journal of Process Control*. 2014. Vol. 24(6). P. 790–797.

30. Maple C. Security and privacy in the Internet of Things. J. Cyber Policy. 2017. Vol. 2. P. 155–184.

31. Gupta P. Kumar P.R. *The capacity of wireless networks. IEEE Trans. Inf. Theory*. 2000. Vol. 46(2). P. 388–404.

32. Ghosh A. Das S.K. *Coverage and connectivity issues in wireless sensor networks: A survey. Pervas. Mobile Comput*. 2008. Vol. 4(3). P. 303–334.

33. Jedermann R. Behrens C. Laur R. Lang W. *Intelligent containers and sensor networks approaches to apply autonomous cooperation on systems with limited resources*. In: Understanding Autonomous Cooperation and Control in Logistics. The Impact on Management, Information and Communication and Material Flow. Berlin, Germany: Springer. 2007. P. 365–392.

34. Hussain M.M. Beg M.M.S. *Using vehicles as fog infrastructures for transportation cyber-physical systems (T-CPS): Fog computing for vehicular networks*. Int. J. Softw. Sci. Comput. Intell. 2019. Vol. 11(1). P. 47–69.

35. Singh N. Vardhan M. *Distributed ledger technology based property transaction system with support for IoT devices*. Int. J. Cloud Appl. Comput. 2019. Vol. 9(2). P. 60–78.

36. Stergiou C. Psannis K.E. Gupta B.B. Ishibashi Y. *Security, privacy efficiency of sustainable cloud computing for big data IoT*. Sustain. Comput., Inform. Syst. 2018. Vol. 19. P. 174–184.

37. Al-Sharif Z.A. Al-Saleh M.I. Alawneh L.M. Jararweh Y.I. Gupta B. *Live forensics of software attacks on cyber–physical systems*. Future Gener. Comput. Syst. 2020. Vol. 108. P. 1217–1229.

38. Koojana K. Bergmann O. Pötsch T. Becker M. Görg C. *Implementation of CoAP and its application in transport logistics*. In Proc. IPSN. 2011. P. 1–7.

39. Sitanayah L. Sreenan C.J. Fedor S. A. *Cooja-based tool for coverage and lifetime evaluation in an in-building sensor network. J. Sensor Actuator Netw*. 2016. Vol. 5(1). P. 4.

40. Kanaris L. Sergiou C. Kokkinis A. Pafitis A. Antoniou N. Stavrou S. *On the realistic radio and network planning of IoT sensor networks*. Sensors. 2019. Vol. 19(15). P. 3264.

41. Martí M. Garcia-Rubio C. Campo C. *Performance evaluation of CoAP and MQTT_SN in an IoT environment*. Proc. Multidisciplinary Digit. Publishing Inst. 2019. Vol. 31(1). P. 49.

42. Ang K.L. Seng J.K. *Application specific Internet of Things (ASIoTs):*

Taxonomy, applications, use case and future directions. IEEE Access. 2019. Vol. 7. P. 56577–56590.

43. Thombre S. Islam R.U. Andersson K. Hossain M.S. *IP based wireless sensor networks: Performance analysis using simulations and experiments*. J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl. 2016. Vol. 7(3). P. 53–76.

44. Pereira C. Mesquita J. Guimarães D. Santos F. Almeida L. Aguiar A. *Open IoT architecture for continuous patient monitoring in emergency wards. Electronics*. 2019. Vol. 8(10). P. 1074.

45. Park K.-J. Zheng R. Liu X. *Cyber-physical systems: Milestones and research challenges*. Computer Communications. 2012. Vol. 36, No. 1. P. 1–7.

46. Park K.-J. Kim J. Lim H. Eun Y. *Robust path diversity for network quality of service in cyber-physical systems*. *IEEE Transactions on Industrial Informatics.* 2014. Vol. 10, No. 4. P. 2204–2215.

47. Bou-Harb E. Lucia W. Forti N. Weerakkody S. Ghani N. Sinopoli B. *Cyber meets control: A novel federated approach for resilient CPS leveraging real cyber threat intelligence*. IEEE Communications Magazine. 2017. Vol. 55, No. 5. P. 198–204.

48. Rajkumar R. Lee I. Sha L. Stankovic J. *Cyber-physical systems: The next computing revolution.* Proceedings of the 47th Design Automation Conference (DAC). Anaheim, USA: IEEE, 2010. P. 731–736.

49. Pasqualetti F. Dörfler F. Bullo F. *Attack detection and identification in cyber-physical systems*. IEEE Transactions on Automatic Control. 2013. Vol. 58, No. 11. P. 2715–2729.

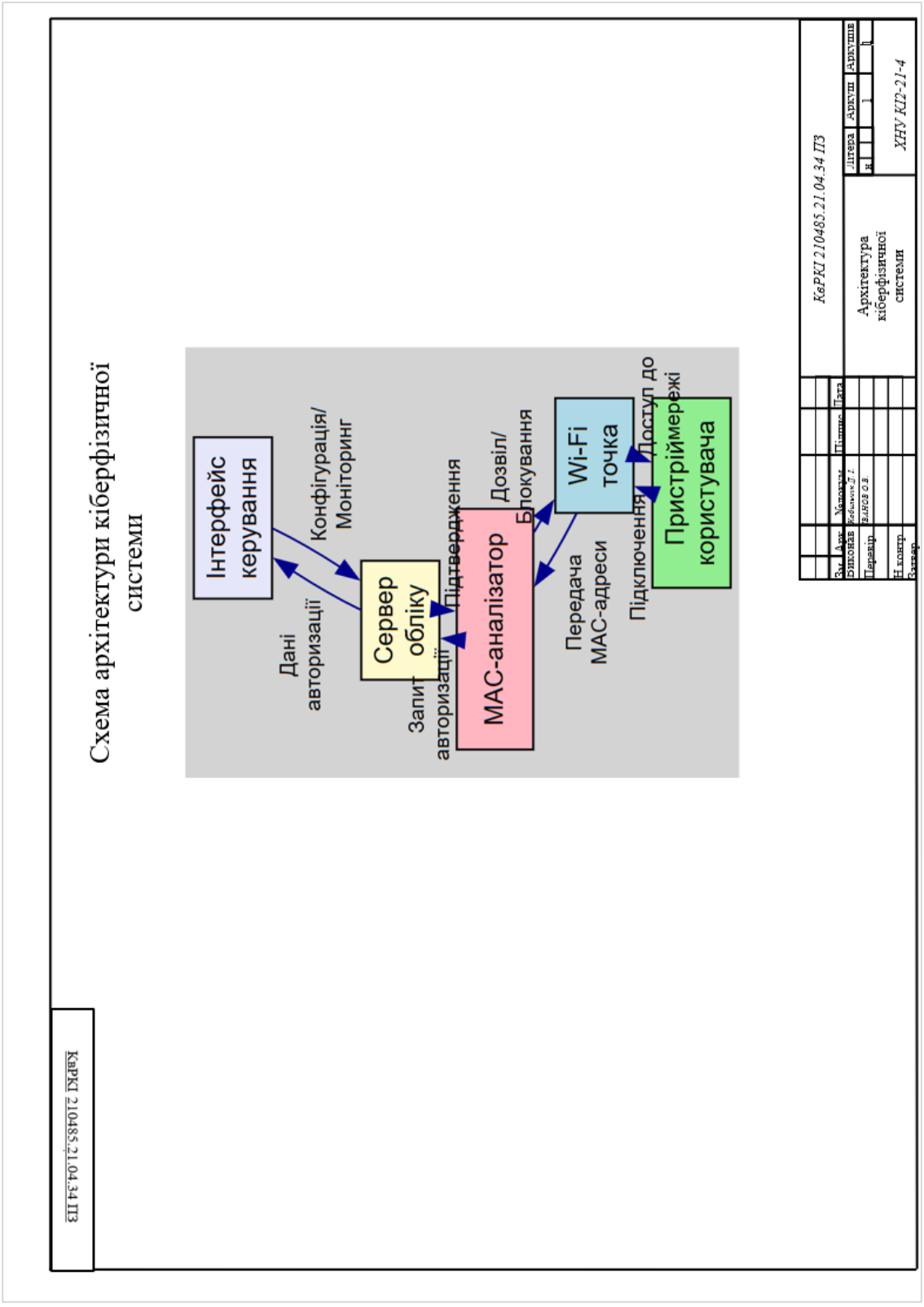
50. Farwell J. P. Rohozinski R. *Stuxnet and the future of cyber war*. Survival. 2011. Vol. 53, No. 1. P. 23–40.

51. He R. *High-speed railway communications: From GSM-R to LTE-R*. IEEE Vehicular Technology Magazine. 2016. Vol. 11, No. 3. P. 49–58.

Додаток А

(обов’язковий)

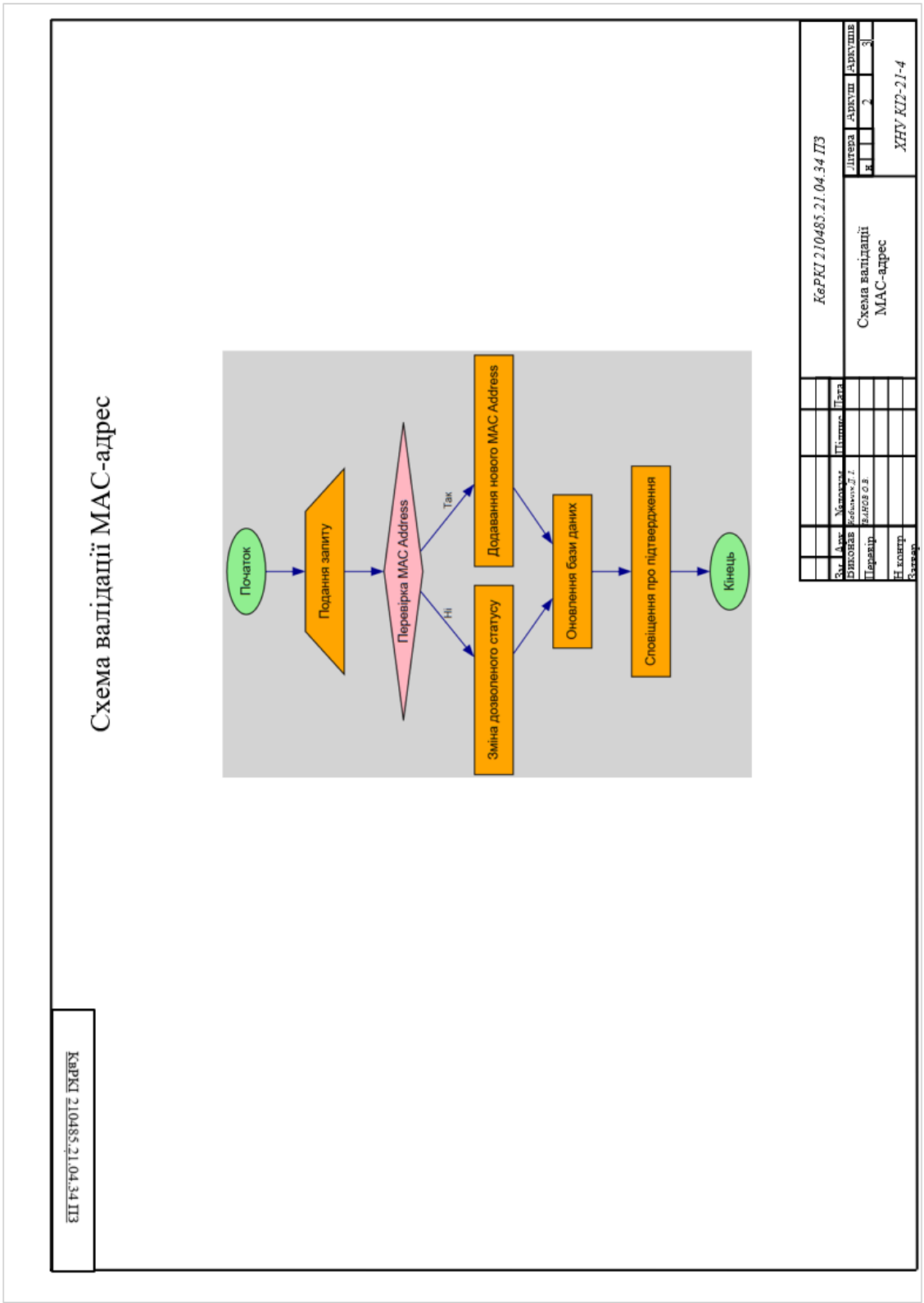
АРХІТЕКТУРИ КІБЕРФІЗИЧНОЇ СИСТЕМИ



Додаток Б

(обов’язковий)

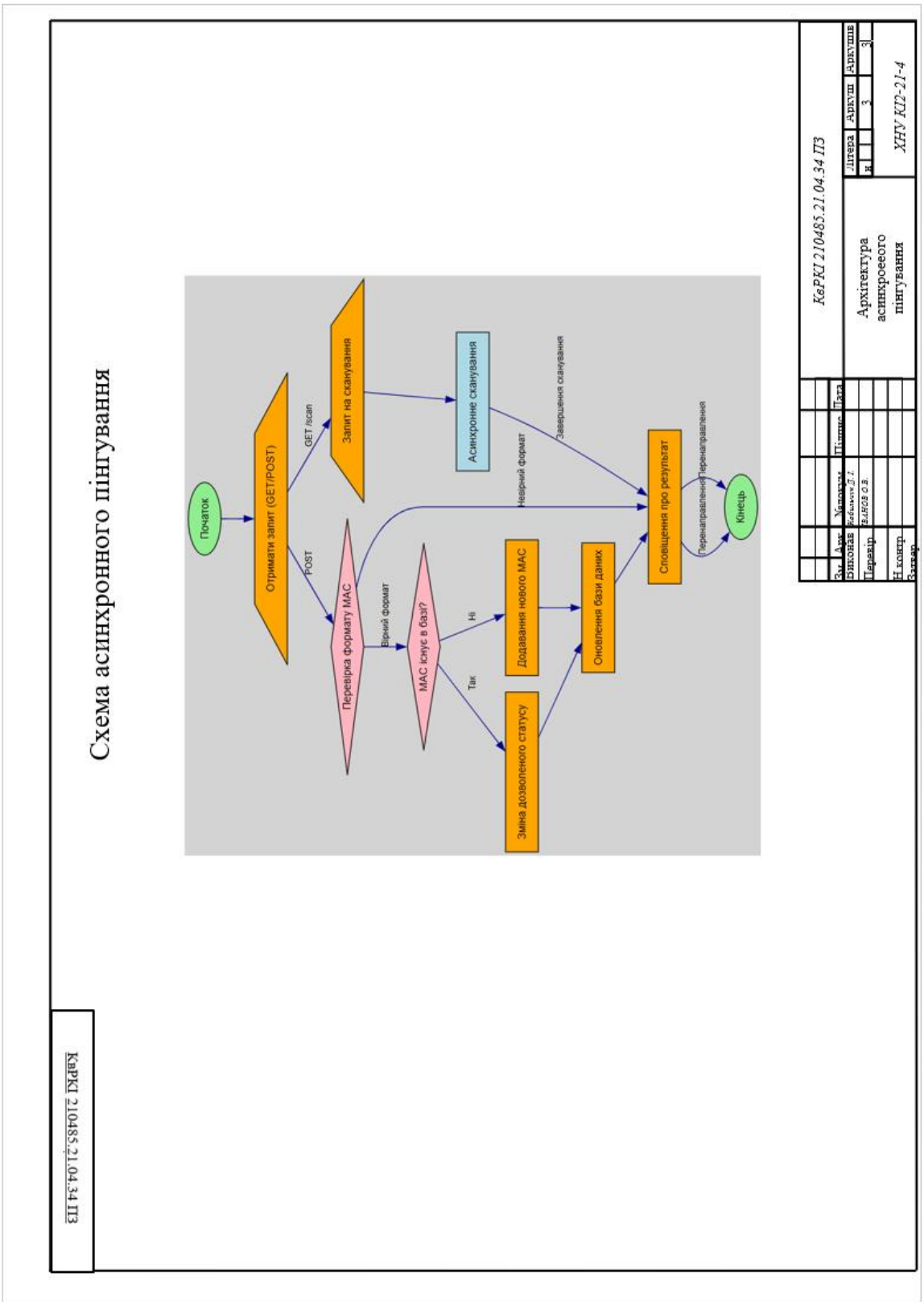
АРХІТЕКТУРА ВАЛІДАЦІЙ MAC-АДРЕС



Додаток В

(обов’язковий)

АРХІТЕКТУРА АСИНХРОННОГО ПІНГУВАННЯ



Wed Jun 11 17:18:10 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
ID: 245176 Title: БКР Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес Added in a DB: 2025-06-11 Authors: Дмитро КОБИЛЬЧУК Heads: Олексій Іванов Consultants: Opponents:	104939	699	1634 (2%)	22 (3%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дмитро КОБИЛЬЧУК

Співавтор:

Назва: Кобильчук_Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:5.4%

Коефіцієнт подібності 2:1.5%

Мікропробіли: 13

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-11 22:33:01.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-12 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Кобильчук Дмитро Іванович

Тема: Кіберфізична система автоматизації процесу реєстрації в Wi-Fi мережах на основі MAC-адрес

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3___ Кількість сторінок записки ___67___

1. Метою кваліфікаційної роботи є розробка кіберфізичної системи, яка автоматизує процес реєстрації пристроїв у Wi-Fi мережі шляхом ідентифікації за MAC-адресами. У роботі реалізовано апаратно-програмний комплекс, що дозволяє здійснювати моніторинг підключень, авторизацію пристроїв та керування доступом через зручний веб-інтерфейс з Telegram-сповіщеннями.

2. Робота повністю відповідає завданню, визначеному в технічному завданні, та охоплює всі поставлені етапи: аналіз, проєктування, реалізація, тестування.

3. У дипломній роботі розроблено систему обліку MAC-ідентифікаторів з можливістю авторизації пристроїв у Wi-Fi мережі. Система побудована з використанням мікрокомп'ютера Raspberry Pi, точки доступу MikroTik та серверної частини на базі FastAPI з PostgreSQL. Інтерфейс адміністратора створено на React.js. Було реалізовано реєстрацію пристроїв, логування підключень, телеграм-сповіщення, а також засоби фільтрації, контролю й статистичного аналізу. В роботі розглянуто актуальні протоколи автентифікації, питання безпеки MAC-спуфінгу, а також можливість інтеграції з існуючими мережевими інфраструктурами.

4. Позитивні сторони роботи: сучасна архітектура на базі відкритих технологій; реальна інтеграція з MikroTik, FastAPI, PostgreSQL, Telegram API; актуальність теми з огляду на зростаючу потребу у безпечному доступі в Wi-Fi мережах.

5. Негативні сторони роботи: відсутність тестування у великих масштабованих мережах (понад 1000 пристроїв); Telegram-бот не підтримує мультиакаунтність (обмежено одним адміністратором).

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: задовільно

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Макаренко Денис Анатолійович, доцент, к.т.н. кафедри АКІТа Р

"12" 06 2025 р. _____ (підпис)

Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Дмитра КОБИЛЬЧУКА
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-21-4

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.06 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кластерна система на основі Raspberry Pi із застосуванням платформи Kubernetes

Автор: Дмитро КОБИЛЬЧУК

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Олексій ІВАНОВ, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності чотирьохрозряних двійкових кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 6.10% і адресується до 47 першоджерела; та системою Anti-Plagiarism складає 12%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Олексій ІВАНОВ

Гарант ОП _____ Андрій НІЧЕПОРУК

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА