Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
КЕРУВАННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ В КОРПОРАТИВНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ
08-34.МКР.008.00.000 ПЗ

Виконав: студент 2-го курсу,
групи ТКС-18м
спеціальності 172 – Телекомунікації та радіотехніка
_____ Палагнюк Д.М.

Керівник: к.т.н., доцент каф. ТКСТБ
_____ Городецька О.С.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф. БМІ
_____ Тимчик С.В.

«____» _____ 2019 р.

Вінниця ВНТУ - 2019 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
Освітньо-кваліфікаційний рівень магістр
Галузь знань 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
к.т.н., професор Г.Г. Бортник

“___” _____2019 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Палагнюку Дмитру Михайловичу .
(прізвище, ім’я, по батькові)

1. Тема роботи Керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах

керівник роботи Городецька Оксана Степанівна, канд. техн. наук, доцент,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від “02” 10 2019 року № 254
2. Строк подання студентом роботи 02 грудня 2019 року

3. Вихідні дані до роботи 1. Рівень значущості α – 0,1; 2. СКВ вимірювання рівня сигналу – 2 дБм; 3. Довірчий інтервал ε – 10^{-2} ; 4. Частота передавача – 2,4 ГГц; 5. потужність передавача +0,09 Вт; 6. Розрахунок місця розташування МАП методами трилатерації; 7. Параметри, що характеризують сигнально-перешкодну обстановку k_{λ}– 0,6, Г –14.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності; 2. Алгоритм управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог безпеки і якості послуг; 3. Система управління безпекою мобільних абонентських пристроїв.
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)
1. Типовий склад сучасного МАП; 2. Узагальнена блок-схема алгоритму управління безпекою МАП; 3. Блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП; 4. Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу; 5. Схема управління конфігурацією МАП; 6. Схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Городецька О.С., доцент кафедри ТКСТБ		
Економічна частина	Кавецький В.В., старший викладач		
Охорона праці та безпека в надзвичайних ситуаціях	Березюк О.В. к.т.н., доцент		

7. Дата видачі завдання 02 вересня 2019 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	06.09.2019р.	
2.	Модель безпеки мобільного абонентського пристрою в корпоративних інфокомунікаційних мережах з різними вимогами по захищеності	13.09.2019р.	
3.	Алгоритм управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог безпеки і якості послуг	04.10.2019р.	
4.	Система управління безпекою мобільних абонентських пристроїв	25.10.2019р.	
5.	Аналіз економічної ефективності розробки	15.11.2019р.	
6.	Охорона праці та безпека в надзвичайних ситуаціях	22.11.2019р.	
7.	Оформлення пояснювальної записки та графічної частини	29.11.2019р.	
8.	Нормоконтроль МКР	02.12.2019р.	
9.	Попередній захист МКР, рецензування МКР	06.12. 2019р.	
10.	Захист МКР ЕК	09.12. 2019р.	

Студент _____ Палагнюк Дмитро Михайлович
(підпис)

Керівник роботи _____ Городецька О. С.
(підпис)

РЕФЕРАТ

УДК 621.391

Палагнюк Д. М. Керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах. Магістерська кваліфікаційна робота зі спеціальності «Телекомунікації та радіотехніка» – Вінниця: ВНТУ, 2019. – 153 с. На українській мові.

Рисунків 28, таблиць 36, бібліографія 81.

Розглянуто основні особливості МАП, що впливають на захищеність доступу, умови функціонування МАП в корпоративних мережах з різними вимогами по захищеності і вимогами які пред'являються до них. На основі проведеного в роботі аналізу зроблено висновок, що основна проблема потребує вирішення для підвищення результативності захисту інформації при роботі з МАП.

Розглянуто модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності, і обґрунтована її коректність.

Досліджено алгоритм управління безпекою мобільного абонентського пристрою дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог щодо безпечності та якості послуг, проведена оцінка його властивостей, доведена його ефективність.

Досліджено систему управління безпекою МАП, що відрізняється можливістю віддаленого управління програмно-апаратної залежності від умов доступу, вимог політик безпеки і якості послуг, що надаються для забезпечення захищеного доступу до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності.

ABSTRACT

UDC 621.391

Palahniyk D. M. Management of Mobile Subscriber Devices Security in Corporate Information Networks. Master's qualification work in the specialty "Telecommunications and Radio Engineering" - Vinnitsa: VNTU, 2019. - 153 p. In Ukrainian language.

Figures 28, tables 36, bibliography 81.

The main features of the MAP affecting access security, the conditions of MAP functioning in corporate networks with different security requirements and requirements to them are considered. Based on the analysis, it is concluded that the main problem needs to be solved in order to improve the effectiveness of information security when working with the MAP.

The model of security of mobile subscriber device in corporate networks with different security requirements is considered, and its correctness is substantiated.

The algorithm of management of security of the mobile subscriber device allows to determine the optimal software and hardware configuration of the device taking into account the attributes of access and requirements for security and quality of services, conducted an assessment of its properties, proved its effectiveness.

The MAP security management system has been investigated, characterized by the possibility of remote management of software and hardware dependence on access conditions, requirements of security policies and quality of services provided to provide secure access to infocommunication services and information of corporate networks with different security requirements.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

АПМДЗ	апаратно-програмний модуль довіреного завантаження
АС	автоматизована система
БМПД	бездротова мережа передачі даних
ВОЛЗ	волоконно-оптична лінія зв'язку
ГЛОНАСС	глобальна навігаційна супутникова система
ЗБ	завдання з безпеки
ЗКМ	захищена корпоративна мережа
ЗІ	захист інформації
ІБ	інформаційна безпека
КС	комп'ютерна система
МАП	мобільний абонентський пристрій
ОС	операційна система
ПЗ	профіль захисту
ПЗП	постійний запам'ятовуючий пристрій
ПЗ	програмне забезпечення
ПЕОМ	персональна електронна обчислювальна машина
ЗОТ	засоби обчислювальної техніки
ЗЗІ	засіб захисту інформації
СКВ	середньоквадратичне відхилення
СУБД	система управління базою даних
ТЗ	технічний засіб
ТКВІ	технічний канал витоку інформації
УКХ	ультракороткі хвилі
УМАП	універсальний мобільний абонентський пристрій
ЦУІБ	центр управління інформаційною безпекою
ЕОТ	електронна обчислювальна техніка
ACK	Acknowledge
BYOD	Bring Your Own Device

CCA	Channel Clearance Algorithm
CTS	Clear To Send
CSMA /CA	Carrier Sense Multiple Access / Collision Avoidance
IEEE	Institute of Electrical and Electronics Engineers
GPS	Global Positioning System
GSM	Global System for Mobile Communications
LTE	Long-Term Evolution
MAC	Media Access Control
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Mobile Information Management
OFDM	Orthogonal Frequency Division Multiplexing
POA	Phase of Arrival
RFID	Radio Frequency IDentification
RSP	Received Signal Phase
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
RTS	Ready To Send
SoC	System-on-Chip
SSOTDOA	Single Sign-On- Time Difference Of Arrival

ВСТУП

Актуальність теми. Використання сучасних МАП, що володіють значними обчислювальними і комунікаційними ресурсами, для обробки конфіденціальної інформації обмежена в зв'язку з низкою суттєвих особливостей, що стосуються їх експлуатації: розмірами, мобільністю користувачів, багатофункціональністю.

Зазначені особливості визначають зовсім інший спектр загроз інформаційної безпеки при роботі з МАП в порівнянні зі стаціонарними засобами обчислювальної техніки (ЗОТ). Постійна зміна місця розташування користувачів МАП, бездротовий віддалений доступ до мереж з різними потребами по захищеності, обмежені обчислювальні можливості з одного боку і високошвидкісні комунікаційні з іншого створюють велику кількість загроз інформаційній безпеці, пов'язаних в першу чергу з погрозами порушення конфіденційності інформації [1].

Аналіз існуючих наукових досліджень, технічних і программно-апаратних рішень, а також нормативно-правової бази в області захисту інформації при роботі з МАП показав, що в даний час:

1) існуючі технічні рішення, що дозволяють управляти функціональністю (конфігурацією) МАП, не передбачають визначення ймовірності знаходження користувача МАП в спеціальних приміщеннях, до яких пред'являють підвищені вимоги щодо забезпечення інформаційної безпеки (ІБ) в корпоративній мережі, і не дозволяють завчасно запобігати роботі МАП тих режимах, які при поточному місцезнаходженню МАП заборонені;

2) доступ до мереж з різними вимогами по захищеності здійснюється або з використанням декількох зареєстрованих в корпоративній мережі МАП, відповідних необхідного рівня захисту або з використанням автоматизованого перемикання режимів роботи; відсутнє автоматичне управління МАП в залежності від вимог захищеності мережі, до якої надається доступ, а також місце розташування МАП; в разі доступу до інформаційних ресурсів сторонньої організації з використанням особистих або корпоративних МАП в даний час діють організаційно-технічні обмеження.

Перераховані фактори обумовлюють актуальність теми магістерського дослідження: "Управління безпекою мобільних абонентських пристроїв в корпоративних мережах " [2].

Об'єкт дослідження: система управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності.

Предмет дослідження: моделі та алгоритми управління безпекою МАП.

Мета дослідження: підвищення ймовірності забезпечення безпеки потрібної для доступу до інфокомунікаційних послуг та інформації в корпоративних інфокомунікаційних мережах з різними вимогами по захищеності при використанні єдиного МАП.

Наукова задача дослідження: на основі формальної моделі безпеки розробити алгоритм управління безпекою МАП, що враховує атрибути доступу користувачів і МАП, включаючи його місце розташування, вимоги за якістю послуг, що надаються, а також науково-технічні пропозиції щодо реалізації системи управління безпекою МАП, що дозволяють підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційним послугам та інформації корпоративних мереж з різними вимогами захищеності при використанні єдиного МАП.

Рішення наукової задачі грунтується на використанні теорії машинного навчання, теорії ймовірності та математичної статистики, апарату прихованих марковских моделей, теорії алгоритмів, теорії управління, теорії множин, теорії оптимізації, чисельних методів і методів математичного та імітаційного моделювання.

Основні положення, що виносяться на захист:

1. Модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності [3].

2. Алгоритм управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог по безпеки і якості послуг [4].

3. Система управління безпекою мобільних абонентських пристроїв, що забезпечує підвищення ймовірності забезпечення безпеки потрібної для доступу до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП [5].

Наукова новизна магістерської роботи полягає:

– у вдосконаленні і обґрунтуванні коректності формальної моделі безпеки МАП, що відрізняється від відомих урахуванням оцінки його місцезнаходження в спеціальному приміщенні, інших атрибутів доступу, а

також реалізацією вимог мандатної і рольової політик безпеки в корпоративних мережах з різними вимогами щодо єдиного МАП;

– у вдосконаленні нового алгоритму управління безпекою МАП, що відрізняється від відомих визначенням оптимальної, з точки зору забезпечення конфіденційності інформації та якості наданих користувачеві;

– у вдосконаленні системи управління безпекою МАП, з можливістю віддаленого управління програмно-апаратними конфігураціями, що відрізняються врахуванням впливу умов доступу, вимог політик безпеки і якості послуг які надаються для забезпечення захищеного доступу до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності.

Практична новизна магістерської роботи полягає:

– в розробці науково-технічних пропозицій щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, що дозволяє підвищити ймовірність забезпечення безпеки інформації при віддаленому доступі до інфокомунікаційних послуг і ресурсів в мережах з різними вимогами щодо захищеності при використанні єдиного МАП;

– в розробці послуг, програмно-апаратної реалізації МАП з урахуванням ймовірності його знаходження в спеціальних приміщеннях та інших атрибутів доступу;

– в розробці рекомендацій щодо формування оптимальних параметрів системи визначення місця розташування МАП, що дозволяють підвищити достовірність обчислення його місцезнаходження в спеціальних приміщеннях.

Теоретична значимість виконаних в магістерській досліджень стоїть в розробці формального апарату моделювання безпеки МАП в корпоративних мережах з урахуванням його місця розташування в спеціальних приміщеннях, а також розробці алгоритму оптимізації програмно-апаратної конфігурації (безпеки) МАП, що дозволяє підвищити вірогідність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг і інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП за рахунок врахування вимог щодо ІБ і якості надання послуг в корпоративній мережі.

Практична значимість роботи полягає:

1. в дослідженні ефективності відомих способів і систем визначення розташування МАП при їх використанні всередині будівлі в заданих приміщеннях і обгрунтуванні оптимальних параметрів алгоритмів визначення

розташування МАП, що дозволяють підвищити достовірність визначення розташування МАП в спеціальних приміщеннях;

2. в реалізації запропонованих алгоритмів у вигляді комплексу програм для ЕОМ і перевірці можливості їх застосування в корпоративної мережі;

3. в розробці науково-технічних пропозицій щодо практичної реалізації системи управління безпекою МАП, підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг і інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП.

Структурно магістерська робота складається зі вступу, пяти розділів, висновків, бібліографічного списку, що включає 81 джерело, 8 додатків. Текст магістерської викладено на 153 сторінках, включаючи 28 рисунків і 36 таблиць.

Публікації за темою магістерської роботи включають в себе 8 тез доповідей.

1 МОДЕЛЬ БЕЗПЕКИ МОБІЛЬНОГО АБОНЕНТСЬКОГО ПРИСТРОЮ В КОРПОРАТИВНИХ МЕРЕЖАХ З РІЗНИМИ ВИМОГАМИ ПО ЗАХИЩЕНОСТІ

Даний розділ присвячений розробці формальної моделі безпеки МАП. Відмінною особливістю даної моделі є облік атрибутів доступу, включаючи місцезнаходження МАП в спеціальних приміщеннях будівлі, в яких розгорнуті корпоративні мережі з різними вимогами по захищеності. Запропоновано модель безпеки МАП, обгрунтована її коректність. На основі аналізу технологій визначення місця розташування МАП в приміщеннях всередині будівель запропоновано технологічне рішення, що дозволяє підвищити достовірність визначення місця розташування МАП в приміщеннях з різними вимогами по захищеності за рахунок застосування методу статистичних випробувань. Обгрунтовано застосування запропонованого технологічного рішення для оцінення місцезнаходження МАП на території приміщень організації із заданою точністю. Розроблено імітаційну модель, що дозволяє оцінити оптимальні параметри алгоритмів визначення місця розташування, проведена оцінка його якості. Представлені результати моделювання.

1.1 Постановка завдання на розробку моделі

Вже згадана в якості об'єкта дослідження в магістерській роботі система управління безпекою МАП в корпоративних мережах з різними вимогами щодо захищеності може бути віднесена до комп'ютерної системи (КС). Відповідно до [5] при аналізі безпеки КС, які повинні володіти високим рівнем довіри, починаючи з оціночного рівня довіри 5, згідно класифікації по [5], потрібно, щоб при розробці КС була використана формальна модель політики безпеки.

Для аналізу безпеки запропонованої в роботі системи управління МАП і досягнення мети дослідження, що полягає в підвищенні ймовірності забезпечення безпеки інформації при експлуатації МАП необхідно розробити модель безпеки МАП, що відрізняється від відомих урахуванням його місця знахожденя в корпоративних мережах з різними вимогами по захищеності. Формальна постановка задачі на розробку моделі: на основі теорій множин, кінцевих автоматів, машинного навчання, математичної статистики та чисельних методів розробити модель безпеки МАП.

Пропонована в роботі модель безпеки МАП базується на класичній моделі Белла-ЛаПадули [6], елементах рольової і атрибутної моделях управління доступом, а також і моделях безпеки, що враховують місце розташування суб'єктів [7].

Початкові дані:

1) елементи класичної моделі Белла-ЛаПадули:

S - безліч суб'єктів системи;

MD - безліч МАП, при цьому $MD \subseteq S$;

O- безліч об'єктів системи, включаючи функціональні блоки МАП;

$P = \{read, write, append, execute\}$ - безліч видів доступу і видів прав доступу;

$B = \{b \subseteq S \times O \times P\}$- безліч можливих множин поточних доступів в системі;

$(L, \leq)$- решітка конфіденційності, наприклад, $L = \{$"ОІ","КІ"$\}$, де "ОІ" < "КІ";

$M = \{m_{|S|\times|O|}\}$ - безліч можливих матриць доступів, де $m_{|S|\times|O|}$ - матриця доступів, $m_{|S|\times|O|} \subseteq P$- права доступу суб'єкта s до об'єкта o;

$(f_s, f_o, f_c, f_{loc}) \in F = L^S \times L^O \times L^S$- четвірка функцій (f_s, f_o, f_c, f_{loc}), яку задають відповідно:$f_s: S \to L$ - рівень доступу суб'єктів; $f_s: O \to L$ - рівень конфіденційності об'єктів; $f_c: S \to L$ - поточний рівень доступу суб'єктів, при цьому для будь-якого $s \in S$, виконується нерівність $f_c(s) \leq f_s(s)$; $f_{loc}: LOC \to L$ - функція, що визначає рівень конфіденційності місця розташування;

$V = B \times M \times F$- безліч станів системи;

Q - безліч запитів до системи;

D - безліч відповідей на запити, наприклад $\{\text{yes}, \text{no}, \text{error}\}$;

$W \subseteq Q \times D \times V \times V$- безліч дій системи, де четвірка $(q, d, v^*, v) \in W$ означає, що система за запитом q з відповіддю d перейшла з стану v в стан v^*;

$N_0 = \{0,1,2, \dots\}$- безліч значень часу;

X- безліч функцій $x: N_0 \to Q$, які задають всі можливі послідовності запитів до системи;

Y- безліч функцій $y: N_0 \to D$, які задають всі можливі послідовності відповідей системи за запитами;

Z- безліч функцій $z: N_0 \to V$, які задають всі можливі послідовності станів системи;

2) елементи мандатної-рольового управління доступом:

R - безліч ролей;

$CONF$ - безліч можливих конфігурацій МАП, при цьому $CONF \subseteq R$;

SS - безліч сесій користувачів (суб'єктів);

$PA: R \to 2^P$ - функція, що задає для кожної ролі безліч прав доступу; при цьому для кожного права доступу $p \in P$ існує роль $r \in R$ така, що $p \in PA(r)$;

$SA: S \to 2^R$ - функція, що задає для кожного суб'єкта безліч ролей, на які він може бути авторизований, при цьому для $MD \subseteq S$ $SA: MD \to 2^{CONF}$;

$user: SS \to S$ -функція, що задає для кожної сесії суб'єкта (користувача), від імені якого вона активізована;

$device: SS \to S$ -функція, що задає для кожної сесії суб'єкта (МАП), від імені якого вона активізована, при цьому MD - безліч МАП і $MD \subseteq S$;

$roles: SS \to 2R$ - функція, що задає для суб'єкта (користувача) безліч ролей, на які він авторизований в даній сесії, при цьому в кожен мо мент часу для кожної сесії $ss \in SS$ виконується умова $roles(ss) \subseteq SA(user\ (ss))$;

$confs: SS \to 2^R$ - функція, що задає для суб'єкта (МАП) безліч конфігурацій, на які він авторизований в даній сесії, при цьому в кожен момент часу для кожної сесії $ss \in SS$ виконується умова $confs(ss) \subseteq SA(device(ss))$;

3) елементи атрибутної політики безпеки, яка враховує особливості програмно-апаратних конфігурацій МАП і його місце розташування:

A - безліч оцінюваних атрибутів доступу, таких як, наприклад, ідентифікаційні дані про користувача, МАП, операційній системі (ОС) і додатках МАП, мережева адресна інформація, рівень конфіденційності і ідентифікатор запитуваної послуги, час запиту на доступ;

LOC - безліч можливих місць розташування;

$MA = \{ma_{|CONF|\times|A|}\}$ - безліч можливих матриць атрибутів доступу, де $ma_{|CONF|\times|A|}$ - матриця необхідних атрибутів доступу, $ma[conf, a] \subseteq A$ - безліч необхідних значень атрибутів доступу для конфігурації $conf$;

розташування та інші параметри приміщень:

$$Rooms = \left\{room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \dots, (x_{in}, y_{in}), L_{Room_i}\right)\right\}, i = \overline{1, N_{Rooms}}, \quad (1.1)$$

де L_{Room_i} - рівень вимог по захищеності приміщення; $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \dots, (x_{in}, y_{in})$ - координати n кутів приміщень;

N_{Rooms} - кількість приміщень;

розташування точок доступу БМПД $AP = A\{P = (x_j,\ y_j)\}, j = \overline{1, N_{AP}}$, де $(x_j,\ y_j)$ - координати точок доступу, N_{AP} - кількість точок доступу.

Потрібно:

1) розробити формальну модель безпеки МАП Z, що відрізняється від відомих вирахувань його місцезнаходження в корпоративних мережах з різними вимогами по захищеності;

2) провести аналіз безпеки розробленої моделі безпеки МАП;

3) здійснити імітаційне моделювання оцінювання достовірності визначення місця розташування МАП в спеціальних приміщеннях корпоративних мереж з різним рівнем захищеності і оцінити якість імітаційної моделі.

У сучасній теорії комп'ютерної безпеки найбільший розвиток в області формального моделювання безпеки КС отримав підхід, який заключався у поданні досліджуваної КС у вигляді абстрактної системи (кінцевого автомата), кожен стан якої описується доступами, реалізованими суб'єктами до сутностей, а переходи КС зі стану в стан описуються командами або правилами перетворення станів, виконання яких, як правило, ініціюється суб'єктами. В основі даного підходу використовується аксіома [9], що дозволяє виділити елементи КС, необхідні для аналізу її безпеки.

Основна аксіома комп'ютерної безпеки. В рамках суб'єкт- сутнісного підходу всі питання безпеки інформації в КС описуються доступами до сутностей.

Основні визначення суб'єкт-сутнісного підходу, такі як "сутність "," об'єкт "," суб'єкт "," доступ "дано в [10]. Розробка формальної моделі безпеки МАП в даній роботі базується на наведених визначеннях.

1.2 Розробка формальної моделі безпеки мобільного абонентського пристрою і доказ відсутності заборонених інформаційних потоків в комп'ютерній системі з мобільними абонентськими пристроями

Безпека системи захисту повинна враховувати особливості і загрози безпеки, що з'являються в ній у зв'язку з наявністю в комп'ютерній системі МАП. Облік даних особливостей дозволить підвищити адекватність формальної моделі безпеки і побудованої на її основі СЗІ.

Типовий склад сучасного МАП представлений на рис. 1.1. Очевидно, що такий пристрій здатний працювати в режимах, заборонених політикою безпеки ЗКМ. Для блокування роботи МАП в заборонених режимах необхідний механізм управління програмно-апаратною конфігурацією МАП, наприклад, на

основі АПМДЗ, що дозволяє забезпечити виконання вимог політики безпеки, встановленої в ЗКМ.

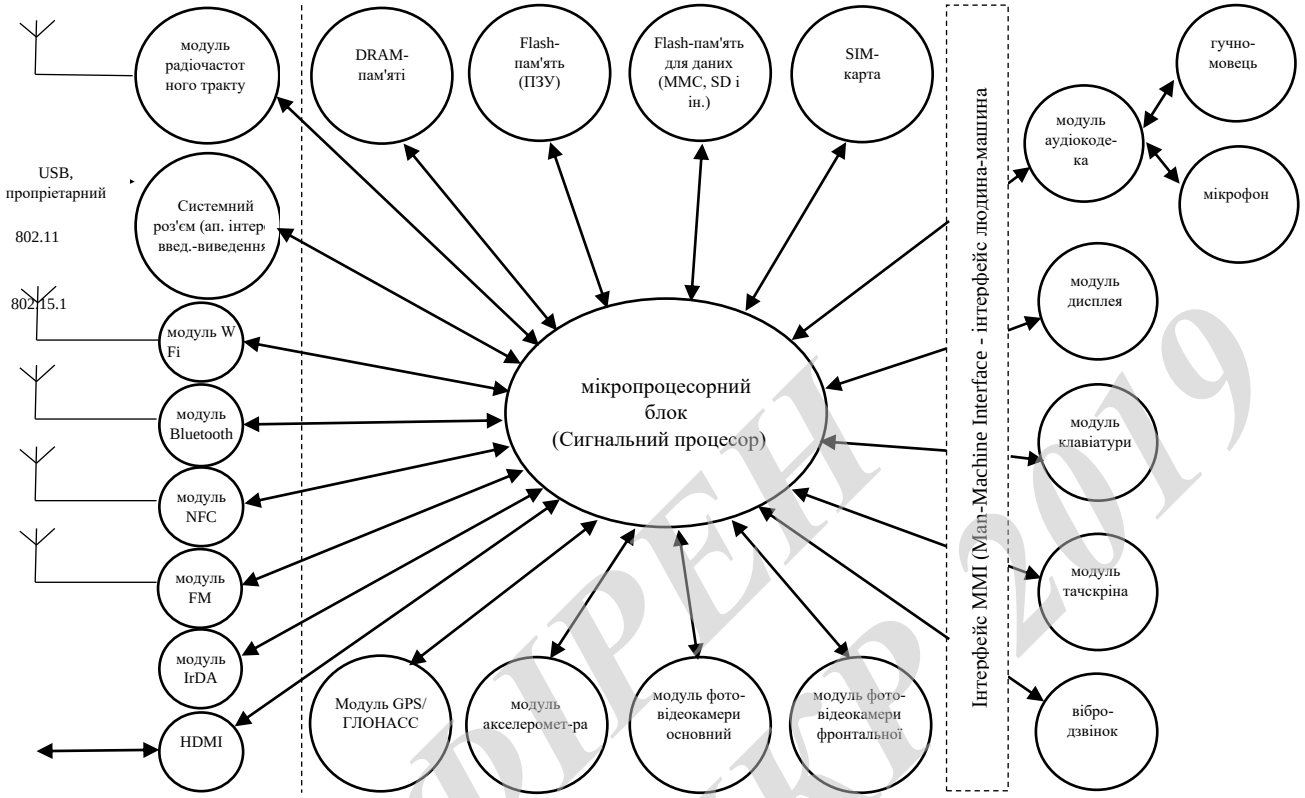
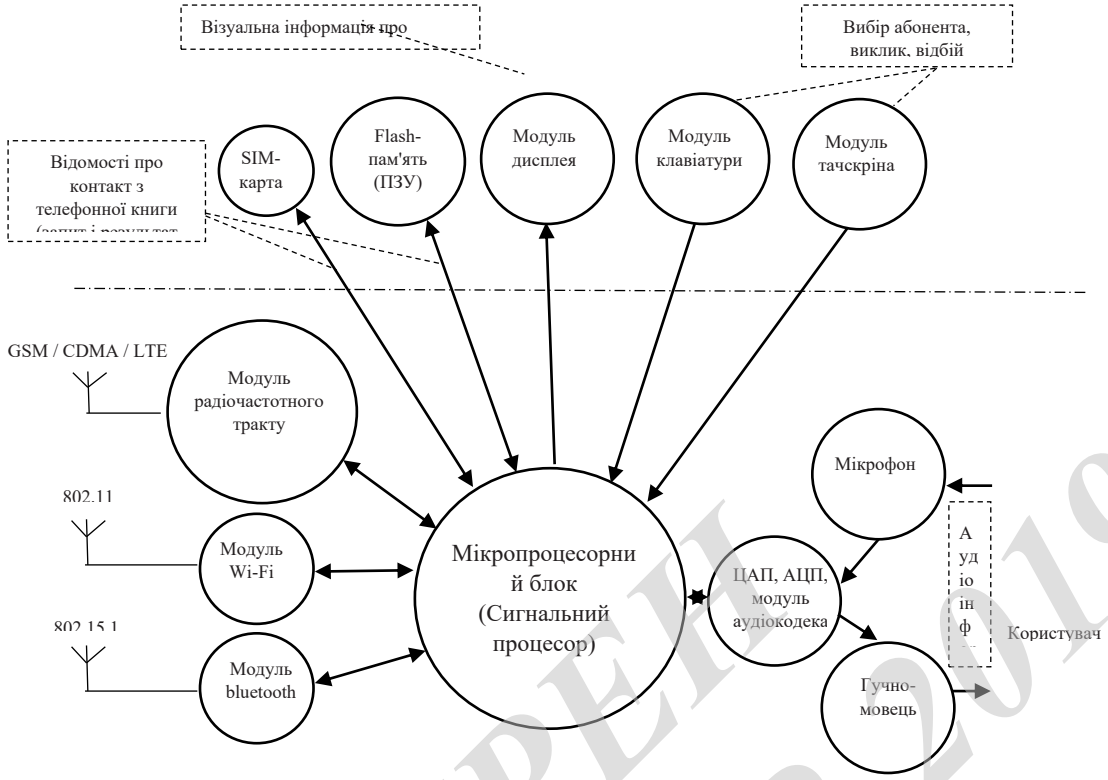


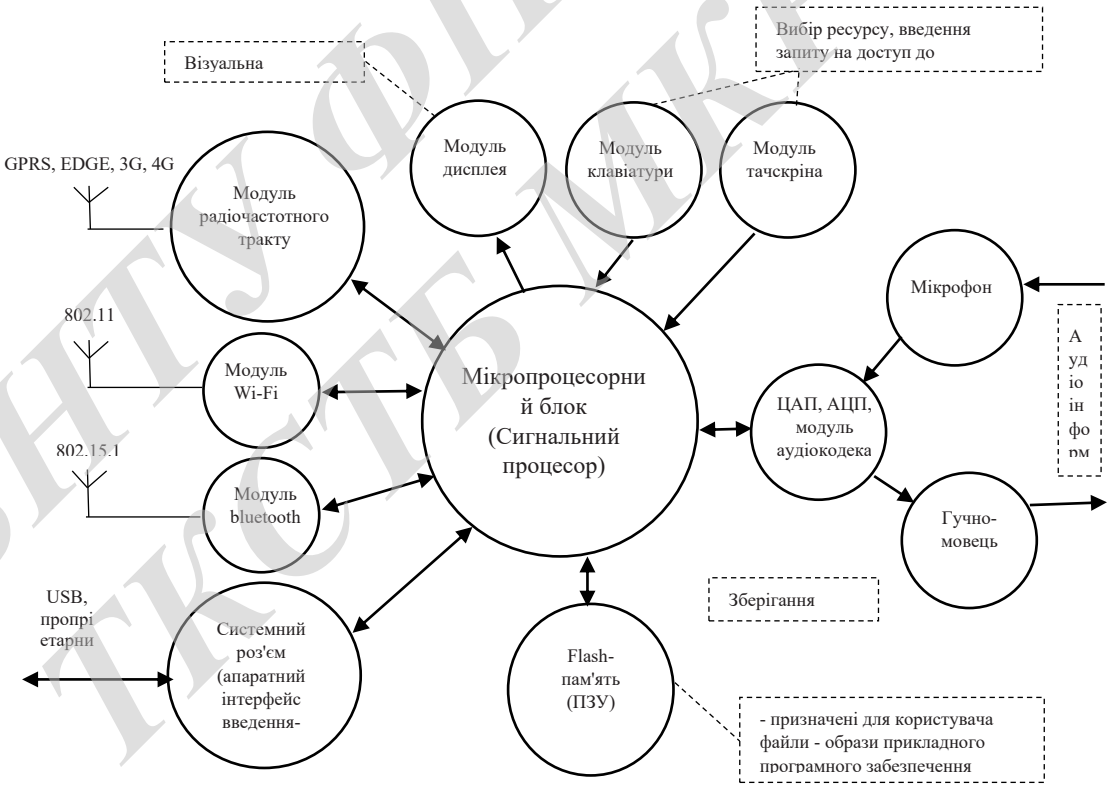
Рисунок 1.1 - Типовий склад сучасного МАП

У формальної моделі безпеки необхідно визначити стан КС, що визначаються, в тому числі, програмно-апаратною конфігурацією МАП, забезпечують безпеку інформації при заданих умовах доступу.

Для визначення складу і структури допустимих конфігурацій МАП доцільно розглянути інформаційні тракти проходження сигналів через МАП при роботі його в різних режимах [11]. На рис. 1.2 представлений склад задіяних функціональних блоків МАП: а) при інформаційному обміні голосовою інформацією (без аудіозапису розмови в локальну пам'ять), б) при інформаційному обміні даними.



а)



б)

Рисунок 1.2 - Склад задіяних функціональних блоків МАП:
а) при інформаційному обміні голосовою інформацією (без аудіозапису розмови в локальну пам'ять); б) при обміні даних

Кожна програмно-апаратна конфігурація визначає набір тих чи інших функціональних блоків МАП, які задіяні при наданні заданих послуг, а також набір прав доступу до цих функціональних блоків.

Для визначення умов, в яких повинні блокуватися заборонені режими роботи МАП, необхідно враховувати атрибути доступу, пов'язані з користувачем МАП, станом програмно-апаратного середовища МАП, адресною інформацією та іншими параметрами. До них можуть належати:

– ідентифікаційні дані про користувача, МАП, операційну систему (ОС) і додатках МАП;

– мережева адресна інформація;

– рівень конфіденційності і ідентифікатор запитуваної послуги;

– час запиту на доступ.

Принципово важливим атрибутом доступу є місце розташування. Вимоги безпеки до технічних засобів, включаючи ЗОТ і МАП в рамках нормативних документів визначаються, як правило, приміщеннями, в яких дані пристрої знаходяться, в яких може бути передбачена обробка інформації з обмеженим доступом. З огляду на те, що місце розташування МАП являється випадковою величиною, а також недостатньо високу точність визначення місця розташування при використанні технологій стандарту 802.11, дану характеристику стану МАП можна представити у вигляді вектора:

$$\vec{P}_{L_{Room}} = \{P(\tilde{L}_{Room} = "OI"), P(\tilde{L}_{Room} = "KI")\}, \quad (1.2)$$

де $P(\tilde{L}_{Room} = "OI")$ - ймовірність того, що МАП знаходиться в приміщенні з рівнем вимог по захищеності для відкритої інформації ("OI"); $P(\tilde{L}_{Room} = "KI")$ - ймовірність того, що МАП знаходиться в приміщенні з рівнем вимог по захищеності для конфіденційної інформації ("KI").

Таким чином, для управління доступом в комп'ютерній системі з МАП необхідно:

– безліч об'єктів доступу O доповнити безліччю функціональних блоків МАП: ПЗУ, ОЗУ, ЦП, АПМДЗ, модулі Bluetooth, дисплея, Wi-Fi, клавіатури, GSM, USB, тачскрін, фото- і відеокамери та інші;

– безліч суб'єктів доступу S доповнити безліччю МАП MD, такими, що $MD \subseteq S$;

– безліч ролей R доповнити безліччю можливих конфігурацій МАП, такими, що $CONF \subseteq R$, при цьому кожна конфігурація (роль) визначається набором тих чи інших прав і видів прав доступу на об'єкти доступу, які включають в себе, в тому числі, функціональні блоки МАП;

– визначити порядок оцінювання розташування з урахуванням відомих технологій визначення місця розташування і їх точності, що дозволяє забезпечити необхідну достовірність;

– визначити властивості системи захисту, що враховують рівні конфіденціальності розташування і особливості програмно-апаратних конфігурацій МАП з урахуванням мандатного розмежування доступу і особливостей функціонування системи визначення місця розташування МАП.

1.2.1 Доповнення до класичної моделі Белла-ЛаПадули в формальній моделі безпеки мобільних абонентських пристроїв

Згідно [12] дано визначення системи захисту на базі класичної моделі Белла-ЛаПадули.

Визначення 1. $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$ називається системою, коли для кожного $(x, y, z) \in \sum(Q, D, W, z_0)$ виконується умова: для $t \in N_0, (x_t, y_t, z_{t+1}, z_t) \in W$, де z_0- початковий стан системи. При цьому кожен набір $(x, y, z) \in \sum(Q, D, W, z_0)$ називається реалізацією системи, а $(x_t, y_t, z_{t+1}, z_t) \in W$ - дією системи в момент часу $t \in N_0$.

Для даної системи в [10] також наведені визначення трьох властивостей, на базі яких визначається її безпеки:

ss - властивість простої безпеки (simple security);

$*$ - властивості "зірка";

ds - властивості дискретної безпеки (discretionary security).

Порушення безпеки системи визначається витоком права доступу, яке визначається трійкою (s, o, p). Щодо даних прав дано визначення доступів в системі $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$., що володіють тими чи іншими з перерахованих властивостей. На основі даних положень визначено, яке стан системи $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$ є безпечним і приведено послідовний доказ цього твердження для класичної моделі Белла-ЛаПадула [12].

На основі зазначених тверджень і на базі відомих формальних моделей визначені наступні властивості безпеки системи $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$:

ss - властивість простої безпеки (simple security);

$*$ - властивості "зірка";

ds - властивість дискреционной безпеки (discretionary security).

Додатково введемо нову властивість системи внутрішньої безпеки для повисіть адекватність формальної моделі умовам експлуатації КС з МАП:

as - властивість атрибутної безпеки (attribute security).

Властивості простої безпеки, "зірка" і властивість дискреционной безпеки описані в класичній моделі Белл-ЛаПадули [10]. Для цілісного опису формальної моделі безпеки МАП наведено їх визначення.

Визначення 2. Доступ $(s, o, p) \in S \times O \times P$ володіє ss-властивістю відносно функцій $f = (f_s, f_o, f_c) \in F$, коли виконується одна з умов:

$p \in \{execute, append\}$;

$p \in \{read, write\}$ і $f_s(s) \geq f_o(o)$.

Визначення 3. Стан системи $(b, m, f) \in V$ володіє ss-властивістю, коли кожен елемент $(s, o, p) \in b$ володіє ss-властивістю щодо f.

Визначення 4. Доступ $(s, o, p) \in S \times O \times P$ володіє $*$ - властивості відносно функцій $f = (f_s, f_o, f_c) \in F$, коли виконується одна з умов:

$p \in execute$;

$p \in append$ і $f_o(o) \geq f_s(s)$;

$p \in read$ і $f_c(s) \geq f_o(o)$;

$p \in write$ і $f_c(s) = f_o(o)$.

Визначення 5. Стан системи $(b, m, f) \in V$ володіє $*$ -властивістю, коли кожен елемент $(s, o, p) \in b$ володіє * - властивістю щодо f.

Визначення 6. Стан системи $(b, m, f) \in V$ володіє $*$ - властивістю відносно підмножини $S' \subseteq S$, коли кожен елемент $(s, o, p) \in b$, ,де $s \in S'$ володіє $*$-властивістю щодо f. При цьому $S \setminus S'$ називається підмножиною довірених суб'єктів, тобто суб'єктів, що мають право порушувати вимоги $*$ - Властивості.

Визначення 7. Стан системи $(b, m, f) \in V$ володіє ds-властивістю, коли кожного доступу $(s, o, p) \in b$ виконується умова $p \in m[s, o]$.

Для врахування особливостей експлуатації МАП в корпоративних мережах з різними вимогами по захищеності визначимо властивість атрибутної безпеки.

Визначення 8. Стан системи $(b, m, f) \in V$ володіє as-властивістю, коли кожного доступу $(s, o, p) \in b$ виконуються одночасно умови $f_{LOC}(loc) = f_s(confs(ss))$, $f_{LOC}(loc) = f_s(user(ss))$ і $(\forall a \in A \exists a^{\text{треб}} \in A^{\text{треб}}: a = a^{\text{треб}}$ і $a^{\text{треб}} \in ma[conf, a])$.

Таким чином, на основі визначень даних властивостей можна сформулювати визначення безпечного стану комп'ютерної системи з МАП.

Визначення 9. Стан системи (b, m, f) називається безпечним, коли він володіє $*$ -властивістю щодо S ', ss-властивістю, ds-властивістю і as-властивістю.

Визначення 10. Реалізація системи $(x, y, z) \in \sum(Q, D, W, z_0)$ володіє ss-властивістю ($*$-властивістю, ds-властивістю і as- властивістю), коли в послідовності $(z_0, z_1, \ldots)$ кожний стан володіє ss-властивість ($*$-властивістю, ds-властивістю і as- властивістю).

Визначення 11. Система $\sum(Q, D, W, z_0)$, володіє ss-властивість ($*$-властивістю, ds-властивістю і as- властивістю), коли кожна її реалізація володіє $ss -$ властивістю ($*$-властивістю, ds-властивістю і as- властивістю).

Визначення 12. Система $\sum(Q, D, W, z_0)$ називається безпечною, коли вона володіє ss-властивістю, $*$-властивістю, ds-властивістю і as- властивістю одночасно.

Згідно [12] з опису даних властивостей випливає, що:

1. Володіння доступом $*$ -властивості щодо f слід володіння цим доступом ss-властивість щодо f.

2. Володіння системою ss-властивістю забезпечує заборону на читання вгору, а також не допускає модифікацію з використанням доступу *write,* коли $f_o\ (o) < f_s\ (s)$, задаючи тим самим для суб'єкта s верхній рівень конфіденціальності об'єктів, до яких він може отримати доступ *read* і *write*.

3. $*$ -властивість виключає появу в системі забороненого інформаційного потоку "зверху вниз", виконуючи вимоги мандатної політики безпеки.

4. Додатково введена властивість атрибутної безпеки as забезпечує виконання вимог політики безпеки для функціонування МАП в дозволених режимах, які визначаються конфігурацією МАП, в разі відповідності поточних умов (атрибутів) доступу, включаючи місце розташування МАП, заданим у вимогах політики безпеки.

Перевірка безпеки системи для описаних властивостей побудована згідно [12] для умов безпеки, заданих на множині дій системи $\sum(Q, D, W, z_0)$. Теореми та їх доведення відомі. Покажемо, що система $\sum(Q, D, W, z_0)$ буде володіти новою властивістю as атрибутної безпеки для безлічі всіх можливих дій.

Теорема 1. Система $\sum(Q, D, W, z_0)$ володіє as-властивістю атрибутної безпеки для будь-якого початкового стану z_0, що володіє as-властивістю, тоді і тільки тоді, коли для кожної дії $\left(q, d, (b^*, m^*, f^*), (b, m, f)\right) \in W$ виконуються умови 1, 2.

Умова 1. Кожен доступ $(s, o, p) \in b^* \setminus b$ володіє as-властивістю відносно f^*.

Умова 2. Якщо $(s, o, p) \in b$ і не володіє as-властивістю щодо f^*., то $(s, o, p) \notin b^*$.

Доведення. Спочатку доведемо достатність умов.

Достатність. Нехай виконані умови 1 і 2 і нехай $(x, y, z) \in \sum(Q, D, W, z_0)$-довільна реалізація системи. тоді $\left(x_t\ y_t, (b_{t+1}, m_{t+1}, f_{t+1}), (b_t, m_t, f_t)\right) \in W$, де $z_{t+1} = (b_{t+1}, m_{t+1}, f_{t+1})$, $z_t = (b_t, m_t, f_t)$для $t \in N_0$.

Для $(s, o, p) \in b_{t+1}$ виконується одна з умов: або $(s, o, p) \in b_{t+1} \setminus b_t$, або $(s, o, p) \in b_t$. З умови 1 випливає, що стан системи z_{t+1} поповнилося доступами, які володіють as-властивістю щодо f^*. З умови 2 слідує, що доступи з b_t, які не володіють as-властивістю щодо f^*, які не входять в b_{t+1}. Отже, кожен доступ $(s, o, p) \in b_{t+1}$ володіє as-властивістю відносно f^* і за визначенням стан z_{t+1} володіє as-властивістю для $t \in N_0$. Так як за умовою стан z_0 володіє as-властивістю, то обрана довільна реалізація (x, y, z) також володіє as-властивістю. Достатність умов теореми доведена.

Необхідність. Нехай система $\sum(Q, D, W, z_0)$, z володіє as-властивістю. Будем вважати, що в безліч W входять тільки ті дії системи, які зустрічаються в її реалізаціях. Тоді для кожного $\left(q, d, (b^*, m^*, f^*), (b, m, f)\right) \in W$ існує реалізація $(x, y, z) \in \sum(Q, D, W, z_0)$ та існує $t \in N_0$.: $\left(q, d, (b^*, m^*, f^*), (b, m, f)\right) = (x_t\ y_t, z_{t+1}, z_t)$. Так як реалізація системи (x, y, z) володіє as-властивістю, то і стан z_{t+1}= (b^*, m^*, f^*) володіє as-властивістю по визначенню. Отже, умови 1 і 2 виконуються. Необхідність умов теореми доведена.

Також в [25, 26] доведено, що для описаної моделі відсутня логічна ув'язка умов виконання системою властивостей безпеки, даних в їх визначеннях, з закладеними в модель умовами їх перевірки. У зв'язку з цим велике значення має коректне визначення властивостей безпеки, не суперечать здоровому глузду і логіці забезпечення безпеки інформації.

Оскільки знову введена as-властивість атрибутної безпеки яка визначає сукупність додаткових обмежень на доступи в системі, то такий опис властивості безпеки, як мінімум, не погіршує рівня безпеки, встановленого в класичній моделі Белла-ЛаПадули, а виконання даної умови дозволяє обмежити потенційно небезпечні доступи в системі, тим самим забезпечивши виконання закладених в політику безпеки вимог, і підвищити адекватність формальної моделі безпеки МАП умов її експлуатації в КС.

1.2.2 Доповнення до мандатної рольової моделі управління доступом в формальній моделі безпеки мобільних абонентських пристроїв

У формальній моделі безпеки МАП враховані особливості мандатноролевого управління доступом. Аналіз безпеки рольового і мандатноролевого управління доступом відомий і наведений в [14].

У запропонованій формальній моделі безпеки додатково введені такі умови:

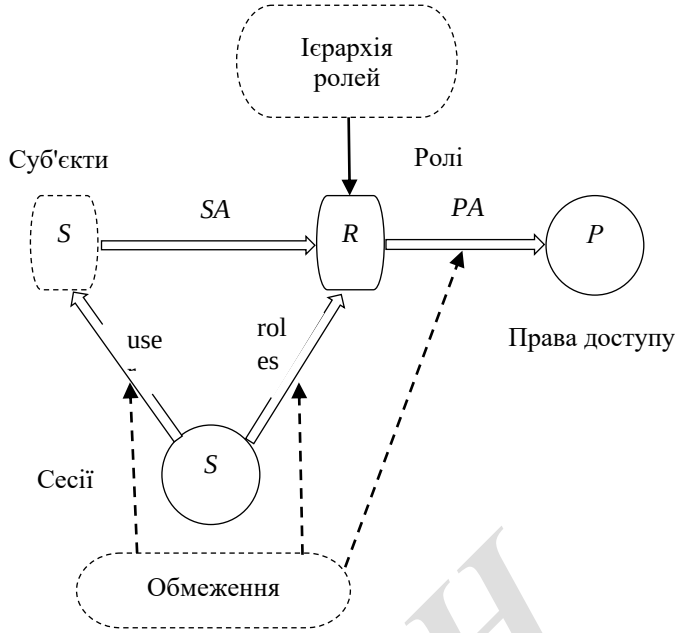
– безліч МАП *MD* є підмножина суб'єктів системи;

– безліч функціональних блоків МАП, таких як модуль GSM, Bluetooth, Wi-Fi, передача даних, фото- і відеокамера та інші визначені як підмножина об'єктів системи;

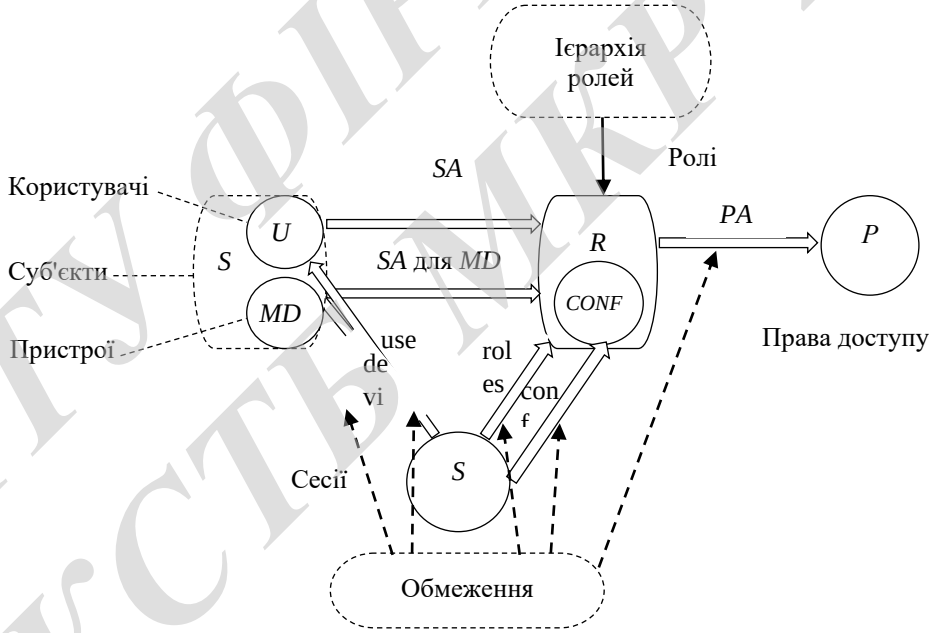
– конфігурація МАП *conf* є аналогом ролі користувача, при цьому підмножина конфігурацій є елементом множини ролей;

– на безлічі ролей визначені співвідношення $PA: R \to 2^P$ *і* $SA: S \to 2^R$, де кожній ролі (конфігурації) задано безліч прав доступу, що відносяться до прав на доступ до функціональних блоків МАП, і кожному мобільному абонентському пристрою $MD \subseteq S$ задано безліч дозволених конфігурацій $SA: MD \to 2^{CONF}$.

В рамках теоретико-множинного підходу зазначені умови сформулювати таким чином, що вони розширюють безліч суб'єктів, об'єктів і ролей, встановлені в системі, не порушуючи їх цілісності, але вводячи додаткові обмеження. У зв'язку з цим обмеження, встановлені для класичних ролей, поширюються і на універсальні ролі, що включають в свій склад конфігурації МАП. Структура елементів класичної рольової моделі управління доступом і рольової моделі управління доступом з конфігураціями МАП представлені на рис. 1.3. З аналізу рис. 1.3б наочно видно, що обмежений накладаються на умови визначення ролей, включаючи конфігурації МАП, а також права доступу.



а)



б)

Рисунок 1.3 - Структура елементів: а) класичного рольового управління доступом; б) рольового управління доступом з МАП і їх конфігураціями

Як показано в [15] мандатне управління доступом порівняно легко реалізується на базі рольового управління доступом з доказом неможливості реалізації заборонених інформаційних потоків від об'єктів з високим рівнем конфіденційності до об'єктів з низьким рівнем конфіденційності.

Покажемо, що при введенні поняття конфігурація МАП, безліч яких представляють собою аналог ролі користувача $CONF \subseteq R$, неможлива реалізація заборонених інформаційних потоків від об'єктів з високим рівнем конфіденційності до об'єктів з низьким рівнем конфіденційності.

Визначення 13. Доступ $\big(s,(o,p)\big) \in S \times P$ є безпечним для ліберального мандатного управління доступом, коли виконується одна з умов:

$p = read$ і $f_s\big(user(ss)\big) \geq f_o(o)$ і $f_s\big(device(ss)\big) \geq f_o(o)$ (ss-властивість);

$p = write$ і, якщо існує доступ $\big(s,(o',read)\big) \in S \times P$, то $f_o(o) \geq f_o(o')$ (Ліберальна* -властивість).

Визначення 14. Доступ $(s,o,p) \in S \times P$ є безпечним для суворого мандатного управління доступом, коли виконується одна з умов:

$p = read$ і $f_s\big(user(ss)\big) \geq f_o(o)$ і $f_s\big(device(ss)\big) \geq f_o(o)$ (ss-властивість);

$p = write$ і, якщо існує доступ $\big(s,(o',read)\big) \in S \times P$, то $f_o(o) = f_o(o')$ (Сувора* -властивість).

Побудуємо систему рольового управління доступом на основі поняття конфігурація МАП $CONF \subseteq R$. Нехай

$CONF = \{x\_read \mid x \in L\} \cup \{x\_write \mid x \in L\}$ - безліч конфігурацій МАП;

$P = \{(o,read) \mid o \in O\} \cup \{(o,write) \mid o \in O\}$ - безліч прав доступу, де o - функціональний модуль МАП (наприклад, модуль GSM, Wi-Fi, фото-, відео-камера і т.д.).

Задамо на безлічі конфігурацій МАП CONF ієрархію, при цьому ієрархії конфігурацій на множинах $\{x\_read \mid x \in L\}$ і $\{x\_write \mid x \in L\}$ будуть незалежні.

Визначення 15. Ієрархія на безлічі конфігурацій МАП $CONF$ у відповідності до вимог ліберального мандатного управління доступом називається ставлення часткового порядку " $\leq$ ", де для конфігурацій МАП $conf, conf' \in CONF$ справедлива нерівність $conf \leq conf'$, коли виконується одна з умов:

$p = x\_read, p' = x'\_read$ і $x \leq x'$;

$p = x\_write, p' = x'\_write$ і $x' \leq x$.

Визначення 16. Ієрархією на безлічі конфігурацій МАП *CONF* у відповідності до вимог суворого мандатного управління доступом називається

ставлення часткового порядку " ≤ ", де для конфігурацій $conf, conf' \in CONF$ справедлива нерівність $conf \leq conf'$, коли виконується одна з умов:

$p = x\_read, p' = x'\_read$ і $x \leq x'$;

$p = x\_write,\ p' = x'\_write$ і $x = x'$ (кожна конфігурація МАП виду x_write порівнянна тільки сама з собою.

Визначення 17. Модель рольового управління доступом відповідає вимогам мандатного управління доступом, коли ієрархія на безлічі конфігурацій МАП, що є підмножиною ролей, $CONF \subseteq R$ відповідає вимогам визначення 15, і виконуються обмеження:

обмеження функції SA - для кожного суб'єкта (МАП або користувач) $s \in S$ конфігурація МАП (роль) $x\_read = \bigoplus SA(s) \cap \{y\_read \mid y \in L\} \in SA(s)$ (тут $x \in f_s(s)$ і $\{y\_write | y \in L\} \subset SA(s)$;

обмеження функції $conf$ - для кожної сесії $ss \in SS$ справедлива рівність $conf(ss) = \{y\_read | y \in L, y \leq x\} \cup \{x\_write\}$;

обмеження функції PA - повинно виконуватися в такий спосіб:

для кожного $x \in L$ доступ $(o, read) \in PA(x\_read)$ тоді і тільки тоді, коли доступ $(o, write) \in PA(x\_write)$;

для кожного доступу $(o, read) \in P$ існує єдина конфігурація МАП x_read: $(o, read) \in PA(x\_read)$(тут $x = f_o(o)$).

Визначення 18. Модель рольового управління доступом відповідає вимогам суворого мандатного управління доступом, коли ієрархія на множині конфігурацій МАП, що є підмножиною ролей, $CONF \subseteq R$ відповідає вимогам визначення 16, і виконуються обмеження:

обмеження функції SA - для кожного суб'єкта (МАП або користувач) $s \in S$ конфігурація МАП (роль) $x\_read = \bigoplus (SA(s) \cap \{y\_read \mid y \in L\}) \in SA(s)$ (тут $x = f_s(s)$ і $\{y\_write | y \in L\} \subset SA(s)$;

обмеження функції $confs$ - для кожної сесії $ss \in SS$ справедлива рівність $conf(ss) = \{x\_read \mid x\_write\}$;

обмеження функції PA - повинна виконуватися в такий спосіб:

для кожного $x \in L$ доступ $(o, read) \in PA(x\_read)$ тоді і тільки тоді, коли доступ $(o, write) \in PA(x\_write)$;

для кожного доступу $(o, read) \in P$ існує єдина конфігурація МАП (роль) x_read: $(o, read) \in PA(x\_read)$ (тут $x = f_o(o)$).

Таким чином, вимоги відповідно ліберальному і суворому мандатному управлінню доступом для моделей рольового управління доступом співпадають

у всьому, крім вимог до відповідної ієрархії ролей і обмеженням на функцію $confs$.

В рамках моделі мандатного рольового управління доступом з конфігураціями МАП такими, що $CONF \subseteq R$, дамо визначення інформаційного потоку.

Визначення 19. Будемо вважати, що існує інформаційний потік від об'єкта $o \in O$ до об'єкта $o' \in O$ (функціонального модуля МАП) тоді і тільки тоді, коли існують конфігурації $conf, conf\ ' \in CONF$, сесія $ss \in SS$ такі, що $(o, read) \in PA(conf)$, $(o\ ', write) \in PA(r')$ і $r, r\ ' \in confs(ss)$.

Обґрунтуємо, що в моделі рольової управління доступом, відповідної вимогам ліберального і суворого мандатного управління доступом, неможлива реалізація заборонених інформаційних потоків від об'єктів з високим рівнем конфіденційності до об'єктів з низьким рівнем конфіденційності.

Теорема 2. Якщо модель рольового управління доступом з конфігураціями МАП відповідає вимогам ліберального або суворого мандатного управління доступом, то в ній для будь-яких об'єктів $o' \in O$ таких, що $f_o(o) > f_o(o')$, неможливе виникнення інформаційного потоку від o до o'.

Доведення. Доведемо від противного. Нехай існують об'єкти (функціональні модулі МАП) $o, o' \in O$ такі, що $f_o(o) > f_o(o')$, і можливо виникнення інформаційного потоку від o до o'. За визначенням 19 існують конфігурації МАП $conf, conf' \in CONF$ і сесія $ss \in SS$ такі, що $(o, read) \in PA(conf), (o', write) \in PA(conf')$ і $conf, conf' \in confs(ss)$.

Отже, виконується одна з умов:

виконуються вимоги ліберального мандатного управління доступом і за визначенням 15 виконуються умови $conf = f_o(o)\_read,\ conf' = f_o(o)\_write$ і $f_o(o) \leq f_o(o')$;

виконуються вимоги суворого мандатного управління доступом і по визначенню 16 виконуються умови $conf = f_o(o)\_read, conf' = f_o(o)\_write$ і $f_o(o) = f_o(o')$.

Протиріччя. Теорема доведена.

Доказ теорем 1 і 2, в яких враховано наявність в комп'ютерній системі МАП, за допомогою яких користувачі можуть отримувати доступ до послуг корпоративних мереж з різними вимогами по захищеності, їх місця розположення і умови доступу, показує, що запропонована формальна модель безпеки МАП може бути застосована в якості основи для реалізації вимог політики безпеки в корпоративних мережах з різними вимогами по захищеності, які експлуатують МАП.

1.3 Імітаційне моделювання визначення місця розташування мобільного абонентського пристрою, що дозволяє оцінити достовірність місцезнаходження мобільного абонентського пристрою в спеціальному приміщенні

Необхідно відзначити, що за рамками формальної моделі безпеки МАП і представлених доказів залишилася проблема точності визначення місця розташування МАП і, зокрема, точність визначення місця розташування МАП в приміщеннях всередині будівлі. На відміну від визначення місця розташування на відкритій місцевості всередині будівель немає можливості використовувати супутникову навігацію через слабкого сигналу, при цьому СЗІ вимагають точності, яка відповідає точністю, що досягається в супутникових системах навігації.

До базових принципів [16], на яких ґрунтуються всі способи визначення місця розташування, відносяться:

– тріангуляція і трилатерація - оцінювання розташування на основі геометричних властивостей кутів до об'єкта (тріангуляція) або відстаней від трьох і більше об'єктів з відомим місцем розташування (трилатерація) [17];

– аналіз карти вимірів - оцінка місця розташування на основі карти точок вимірювань параметрів сигналу (карти сигнального простору) [18];

– аналіз близькості - позиціонування на основі близькості до приймача сигналу щодо інших [19];

– аналіз динаміки руху [20].

Показники для оцінювання якості системи визначення місця розташування детально представлені в [21]. Порівняльна характеристика і оцінка дечких відомих систем визначення місця розташування по представленим показникам якості представлена в табл. 1.1.

Таблиця 1.1 - Порівняльна характеристика систем і технічних рішень визначення місця розташування

Система/ Тех.ріш.	Бездротова технологія/Алгоритм	Точність	Похибка	Складність	Масшт./Дозв.	Варт.
Microsoft RADAR [103, 104]	Wi-Fi / метод *k* - найближчих сусідів, алгоритм Вітербо	3-5 м	50% при 2,5 м. 90% при 5,9 м	Серед.	добре/2D, 3D	Низьк.
Horus [149]	Wi-Fi / ймовірнісний метод	2 м.	90% при 2,1 м	Серед.	добре /2D	Низьк.
DIT [105, 107]	Wi-Fi / 1) нейронні мережі 2) метод опорних векторів (МОВ)	3 м	1) 90% при 5,12 м 2) 90% при 5,4 м	Серед.	добре /2D, 3D	Низьк.
Ekahau [130]	Wi-Fi / ймовірнісний метод (відстеження)	1 м	50% при 2 м	Серед.	добре /2D, 3D	Низьк.
SnapTrack	GPS, TDOA	5 м	50% при 25 м	Висок.	добре /2D, 3D	Серед.
WhereNet	УВЧ-діапазон, TDOA / 1) метод найменших квадратів; 2) метод мінімальних залишків	2-3 м	50% при 3 м	Серед.	Дуж. добре /2D, 3D	Низьк.
Robot-based [126, 145]	Wi-Fi / баєвський підхід	1,5 м	Більше 50% при 1,5 м	Серед.	добре /2D,	Серед.
Sappire Dart	Різноспрямована СШП, TDOA	<30 см	50% при 30 см	0,1 Гц - 1 Гц	добре /2D, 3D	
MultiLoc [128]	Wi-Fi / SMP (Symmetric Mul- tiprocessing)	2,7 м	50% при 2,7 м.	Низьк.	добре /2D	Серед.
LAND- MARC	Активний RFID, RSS/метод *k* - найближчих сусідів	<2 м	50% при 1 м	Серед.	Вузли розм. щільно	Низьк.
TIX [109]	Wi-Fi / TIX (Triangular Interpolation and eXtrapolation)	5,4 м	50% при 5,4 м	Низьк.	добре /2D	Серед.
PinPoint 3D-1D	УКВ (40МГц), RTOF / Баєвський підхід	1 м	50% при 1 м	5 с	добре /2D	Хор
GSM- "Почерк"	GSM, RSS / Зважений метод *k* NN	5 м	80% при 10 м	Серед.	відм/2D, 3D	Серед.
FLIPS [101]	Wi-Fi / Триангуляція і нечітка логіка	2 м	Більше 50% при 2 м	Серед.	добре /2D	Серед.

Порівняльний аналіз технологій визначення місця розташування по точності і призначенню наведено на рис. 1.4.

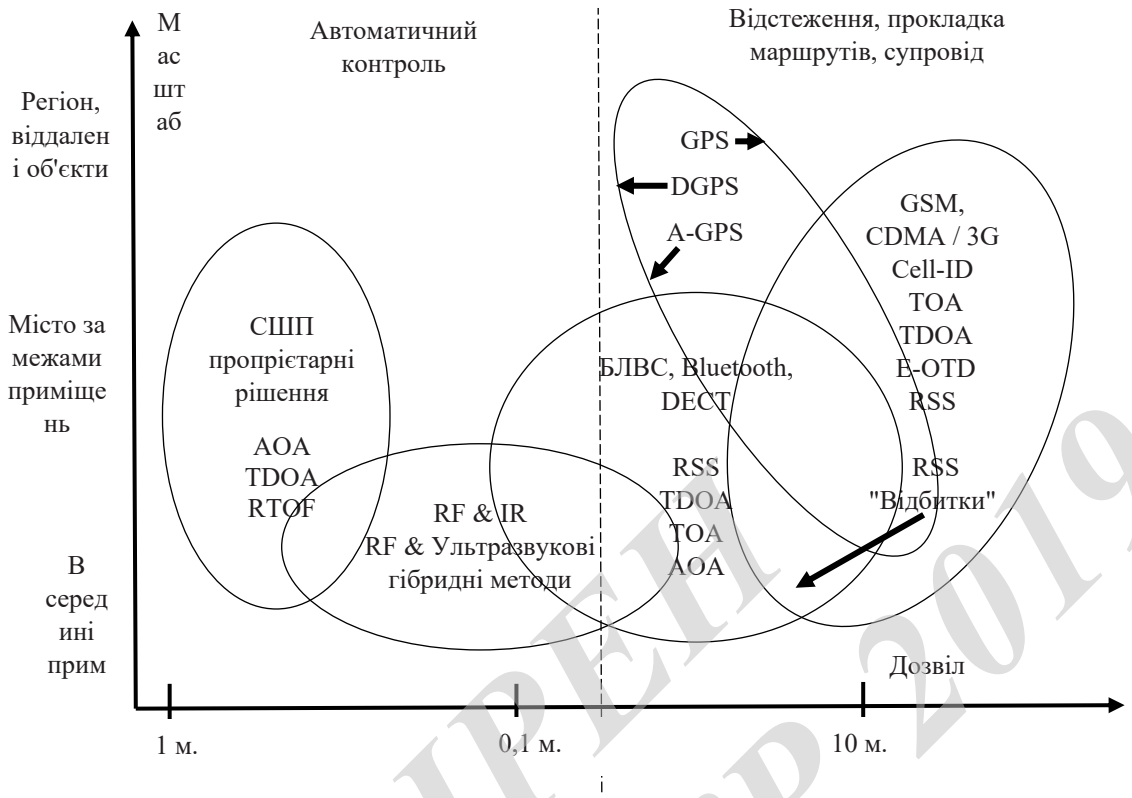


Рисунок 1.4 - Порівняльний технологій визначення місця розташування

З аналізу рисунка видно, що технологій, що використовуються для визначення місця розташування, відносно небагато. До них відносяться GSM / CDMA / 3G / LTE; RFID / Bluetooth / Wi-Fi; УКВ / СШП, а також технології, що використовують лазерні далекоміри і датчики, що вимірюють орієнтацію в просторі - альтиметр, гіроскопи і 3Д-акселерометри, ВОЛЗ. В роботі [73] показано, що сучасний технологічний рівень не дозволяє використовувати інерційні датчики в якості основи для системи визначення місця розташування в приміщеннях внаслідок ефекту накопичення помилки за короткостроковий період. Дані недоліки були частково усунені в технології Google Tango [10], що використовує в якості додаткової розмірності, що характеризує місце розташування МАП всередині будівлі, графічний потік, одержаний з вбудованої в МАП камери, і відповідну йому базу даних координат у вигляді 3Д-моделі будівлі. Очевидною, що дана технологія не може бути застосована в ЗКМ через вимоги ІБ.

Технології супутникової навігації не можна застосовувати всередині приміщень через значне згасання сигналу від супутників [22]. Технології на базі сигналів GSM / CDMA / 3G / LTE володіють низькою точністю для вирішення завдання визначення місця розташування МАП. Ультразвукові методи, методи

радіочастотної ідентифікації (RFID), технології на базі ВОЛЗ не дозволяють організувати захищений канал управління МАП, а деякі з них не забезпечують, в тому числі, ідентифікацію МАП.

До системи визначення місця розташування МАП пред'являється ряд вимог, виконання яких впливає на забезпечення конфіденційності інформації:

– точність визначення місця розташування повинна дозволяти ідентифікувати приміщення, в якому знаходиться користувач МАП, з мінімальною помилкою 2-го роду;

– повинна забезпечуватися ідентифікація користувача МАП в системі визначення місця розташування.

Виходячи з аналізу табл. 1.1 і рис. 1.4, а також відомих особливостей технічних реалізацій зазначених технологій, прийнятну точність визначення місця розташування всередині будівлі, а також ідентифікацію користувача МАП, дозволяють забезпечувати методи, засновані на застосуванні радіочастотної ідентифікації (RFID), а також методи, засновані на застосуванні БМПД. На основі робіт [23] був проведений порівняльний аналіз даних технологій. Результати аналізу представлені в табл. 1.2.

Таблиця 1.2 - Порівняльний аналіз ефективності датчиків радіочастотної ідентифікації та БМПД для вирішення завдання визначення місця розположення МАП

Показник	Технологія	
	Радіочастотна ідентифікація (RFID)	Бездротові мережі передачі даних (802.11)
Середня вартість	Низька / Середня (для активних RFID)	Середня
Показник	точність менше 1 м	1-7 м
Складність реалізації	Середня	Низька / Середня (для систем з навчанням)
Масштабованість	Низька	хороша
Просторове покриття	2D	3D
Стійкість до перешкод	Низька	хороша
Стійкість до атак типу "Людина посередині"	Низька	висока
Можливість створення каналу управління МАП	Відсутня	є
Необхідність наявності зчитувача / rfid-мітки в МАП	Є (відсутній в МАП в теперішній час)	Є (є в більшості сучасних МАП)

На відміну від технології RFID способи визначення місця розташування на основі БМПД позбавлені даних недоліків, але при цьому володіють більш високою вартістю і меншою точністю визначення місця розташування МАП. У ряді наукових публікацій [24] пропонується використовувати комбіновані технічні рішення, що дозволяють компенсувати недоліки обох.

Завдання визначення місця розташування і завдання захищеного інформаційної взаємодії може вирішуватися з використанням єдиного модуля безпровідникового зв'язку стандарту 802.11, або може бути розділена на технологічно незалежні бездротові модулі. Для сигналів стандарту 802.11 рішення задачі визначення місця розташування може бути здійснено з використанням методів тріангуляції (трилатерації) і аналізу карти сигнального простору. Слід зазначити, що метод трилатерації не вимагає проведення попередніх вимірювань рівня сигналів мережі на відміну від методів аналізу карти вимірів, що істотно спрощує її розробку, експлуатацію та супровід. Однак в той же час підсистеми визначення місця розташування, засновані на методі трилатерації, володіють більш низькою точністю в порівнянні з системами на основі аналізу карти сигнального простору.

З точки зору рішення завдання магістерського дослідження при визначенні розташування істотне значення має не стільки координати знаходження МАП, скільки приміщення, в якому воно знаходиться. Причина цього полягає в тому, що вимоги безпеки визначаються саме приміщенням, в якому знаходиться МАП. Очевидно, що приміщення - це істотно більш грубий об'єкт для розпізнавання в порівнянні з координатами МАП. Кожна з розглянутих технологій визначення місця розташування на базі БМПД і стандарту 802.11 призначена саме для обчислення координат точки розташування МАП на карті, а вже по точці визначається приміщення, до якого вона відноситься.

Необхідно відзначити, що похибка даних технологій дозволяє говорити не про координати точки розташування МАП, а про окружності, в межах якої може перебувати пристрій, при цьому радіус даної окружності дорівнює максимальній помилці визначення місця розположення для заданої технології. Враховуючи, що в межах даної окружності можуть перебувати різні приміщення з різними вимогами по захищеності, була запропонована слідуюча гіпотеза. Для підвищення достовірності визначення місцезнаходження МАП в спеціальних приміщеннях, до яких пред'являються підвищені вимоги ПЗ захищеності, необхідно обчислити площу приміщень кожного рівня

захищеності, що знаходяться всередині окружності, що визначає ймовірність місцезнаходження МАП. Ставлення отриманої площі приміщень до загальної площі даної окружності дозволить визначити ймовірність знаходження МАП в спеціальному приміщенні.

В якості базових технологій, які використовують БМПД для визначення місце розташування, а також для *обґрунтування алгоритмічної можливості розв'язання* запропонованого підходу по обчисленню ймовірності знаходження МАП в спеціальному приміщенні незалежно від обраного методу, пропонується використовувати технології, засновані на застосуванні:

– методу трилатерації (тріангуляції) сигналу МАП, приймати декількома точками доступу БМПД [25];

– методу *k* - найближчих сусідів [26];

– методу, заснованого на використанні баєвського підходу [15].

Математичний апарат, на основі якого будуються дані технології, і дослідження їх ефективності представлені в додатку А і роботах [17]. Вибір даних методів обумовлений:

– різної обчислювальної складністю;

– різними вимогами по обслуговуванню і обчислювальної потужності;

– різною похибкою визначення місця розташування.

Рішення задачі обчислення площі приміщень кожного рівня захисту захищеності, що знаходяться всередині окружності та щоб визначити ймовірне знаходження МАП, необхідно розвязувати, виходячи з таких умов:

– конфігурація і розташування приміщень заздалегідь відома;

– координати точки розташування МАП і розташування кола, в межах якої може перебувати МАП, кожен раз обчислюється відомими методами;

– конфігурація і розташування приміщень всередині даної окружності є геометричні об'єкти довільної форми;

– максимальний радіус окружності, в межах якої може перебувати МАП, залежить від використовуваної технології визначення місця розташування і дорівнює максимальному значенню помилки визначення місця розташування для заданої технології, що отримується емпіричним шляхом.

При зазначених умовах використання класичного геометричного підходу для обчислення площі фігури неприйнятно, в першу чергу, в звязку з необхідністю обчислення площі фігур довільної конфігурації в кожен момент часу і необхідністю врахування великої кількість можливих варіантів. Найбільш підходящим способом визначення площ довільних фігур є метод

статистичних випробувань - метод Монте-Карло [25]. Даний метод дозволяє визначити площу довільної фігури в колі, що визначає ймовірне місцезнаходження МАП, проте може знадобитися попереднє навчання.

Попереднє навчання полягає в зборі статистики помилок визначення місця розташування для заданої технології. Дана статистика (ряд розподілення значень помилки визначення місця розташування) є основою для проведення статистичних випробувань. При цьому випадковою величиною є помилка визначення місця розташування.

Застосування методу Монте-Карло для обчислення ймовірності знаходження МАП в спеціальному приміщенні [21] при використанні спільно з технологіями визначення місця розташування на базі БМПД дозволить знизити вплив нестійкості радіосигналів БМПД на помилку визначення місця розташування МАП і підвищити достовірність обчислення ймовірності знаходження МАП в спеціальному приміщенні ЗКМ.

1.3.1 Модель системи визначення місця розташування мобільного абонентського пристрою, що дозволяє оцінити ймовірність його місцезнаходження в спеціальному приміщенні з підвищеними вимогами по захищеності

Як було показано раніше, ключове значення для визначення вимог безпеки, що пред'являються до МАП, мають не стільки координати його місця знаходження, скільки інформацію про приміщення, в якому він знаходиться. Тому для вирішення завдання визначення ймовірності місцезнаходження МАП в спеціальному приміщенні необхідні відомості про склад і параметри приміщень ЗКМ. Дані відомості характеризують описову модель будівлі і можуть бути представлені у вигляді

$$Rooms = \left\{\left((x_{i1}, y_{i1}), \dots, (x_{in}, y_{in}), L_{Room_i}\right)\right\}, i = \overline{1, N_{Room}}, \quad (1.3)$$

де $(x_{i1}, y_{i1}), \dots, (x_{in}, y_{in})$ - координати n кутів i -го приміщення, з рівнем вимог по захищеності $L_{Room\,i}$; N_{Room} - кількість приміщень.

В результаті обчислення місця розташування у відповідно з представленими моделями визначення місця розташування МАП можуть бути отримані координати МАП - $(\tilde{x}, \tilde{y})$. Помилка визначення місця знаходження в цьому випадку з урахуванням того, що реальний стан МАП - (x, y), обчислюється за допомогою формули:

$$e_L = \sqrt{(x - \tilde{x})^2 + (y - \tilde{y})^2}. \quad (1.4)$$

В табл. 1.1 представлені статистичні характеристики помилок вимірювань місця розташування для різних технологій визначення місця розташування в приміщеннях в середині будівлі. Як видно з даної таблиці, реальне місце розташування користувача МАП знаходиться в межах кола з центром з координатами $(\tilde{x}, \tilde{y})$ і радіусом, рівним максимальному значенню помилки визначення місця розташування: $R_e = max[e_L]$. З огляду на те, що величина R_e порівнянна з габаритами приміщень, то реальне місце розташування користувача МАП може значно відрізнятися від обчисленого, тому рішення задачі визначення ймовірність місцезнаходження МАП в спеціальному приміщенні є нетривіальною і вимагає врахування додаткових факторів. Графічна ілюстрація даного завдання представлена на рис. 1.5. З аналізу рис. 1.5 видно, що реальне місце розташування МАП (x, y) може знаходитися в приміщеннях будь-якого рівня вимог по захищеності, оскільки в радіусі максимальної помилки визначення місця розташування R_e від від обчисленої точки $(\tilde{x}, \tilde{y})$ знаходяться приміщення всіх рівнів. Очевидно, що значення координат обчисленої точки $(\tilde{x}, \tilde{y})$ залежать від ряду факторів, які впливають випадковим чином, а також обраної технології визначення місця розташування. З огляду на те, що карта розташування приміщень відома, а також можуть бути отримані емпіричним шляхом (на етапі навчання системи) статистичні параметри помилки визначення місця розташування, можна оцінити ймовірність того, що користувач знаходиться в приміщенні з заданим рівнем вимог по захищеності.

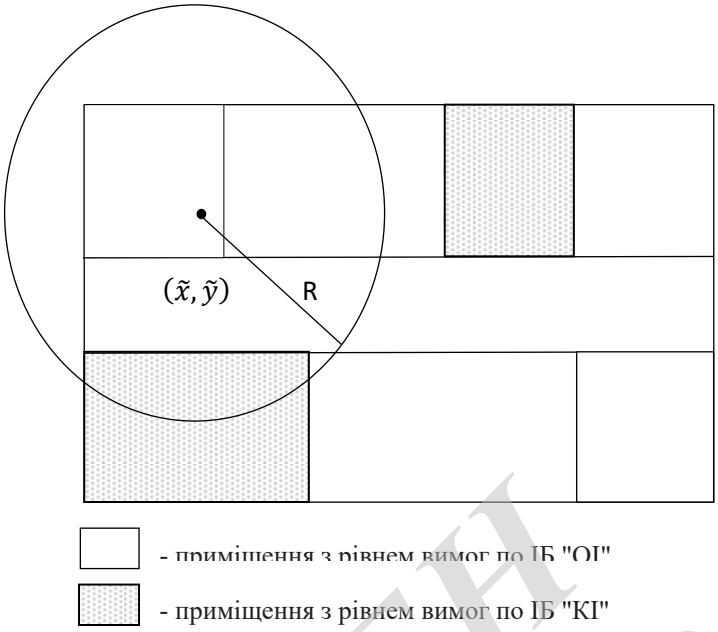


Рисунок 1.5 - Завдання визначення ймовірності місцезнаходження МАП в спеціальному приміщенні

Знаючи координати центру кола $(\tilde{x}\,, \tilde{y})$, її радіус R_{e} і карту розташування приміщень, оцінка ймовірності того, що користувач знаходиться в приміщенні з заданим рівнем по захищеності, може бути представлена як відношення площі приміщень заданого рівня до площі кола з центром в точці $(\tilde{x}\,, \tilde{y})$ і радіусом R_{e}. Таким чином, для ЗКС з рівнями вимог по захищеності приміщень $L_{Room} =$ {"ОІ","КІ"} оцінка ймовірності того, що користувач знаходиться в приміщенні з заданим рівнем вимог по захисту захищеності може бути представлена у вигляді виразу:

$$P\left(\tilde{L}_{Room} = L_{Room}\right) = \frac{F_{Sg}(L_{Room},(\tilde{x}\,,\tilde{y}),R_{\text{e}}),}{\pi \cdot R_e^2}, \qquad (1.5)$$

де L_{Room} - заданий рівень вимог ПЗ захищеності, для якого виробляється оцінювання; R_{e}- радіус кола, що характеризує максимальну помилку визначення місця знаходження; $(\tilde{x}\,, \tilde{y})$- координати обчисленого місця знаходження; $F_{Sg}(L_{Room}, (\tilde{x}\,, \tilde{y}), R_{\text{e}})$- функція, що обчислює площу приміщень з рівнем L_{Room}, що знаходяться всередині кола з центром в точці $(\tilde{x}\,, \tilde{y})$, радіусом R_{e}і площею $\pi \cdot R_e^2$

Тоді оцінка ймовірності того, що користувач знаходиться в приміщенні з тим чи іншим рівнем вимог по захищеності може бути представлена у вигляді вектора:

$$P_{L_{Room}} = \left\{P\left(\tilde{L}_{Room} = \text{"ОІ"}\right), P\left(\tilde{L}_{Room} = \text{"КІ"}\right)\right\}. \qquad (1.6)$$

Обчислення функції $F_{Sg}(L_{Room}, (\tilde{x}, \tilde{y}), R_{\text{e}})$ для довільної конфігурації розташування приміщень, а також довільних значень $(\tilde{x}, \tilde{y})$ і R_{e} є важкою задачею для геометричних методів, однак вона легко може бути вирішена чисельним методом на основі методу статистичних випробувань (методу Монте-Карло) [51, 125]. Даний метод заснований на отриманні великого числа реалізації стохастичного (випадкового) процесу, який формується таким чином, щоб його ймовірнісні характеристики співпадали з аналогічними величинами розв'язуваної задачі.

Реалізація методу Монте-Карло з метою вирішення завдання обчислення функції $F_{Sg}(L_{Room}, (\tilde{x}, \tilde{y}), R_{\text{e}})$ полягає в наступному:

1) за допомогою генератора випадкових чисел із заданим законом розподілення ймовірностей формуються координати випадкової точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ таким чином, щоб вони лежали всередині кола з центром в точці (x_i', y_i') і радіусом R_{e}, де N_{MC}- кількість експериментів;

2) визначається приміщення, в якому знаходиться поточна точкаx (x_i', y_i'), і відповідний йому рівень вимог по ІБ $\tilde{L}_{Room} = F_{L_{Room}}\big((x_i', y_i'), Rooms\big)$, де $Rooms = \{room_i = \big((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \ldots, (x_{in}, y_{in}), L_{Room_i}\big)\}$- розташування і рівні вимог по захищеності приміщень, $i = \overline{1, N_{Rooms}}$, $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \ldots, (x_{in}, y_{in})$- координати n кутів приміщень, N_{Rooms} - кількість приміщень;

3) лічильник влучень в приміщення з $L_{Room_i} = \tilde{L}_{Room}$ збільшується на одиницю - $N\left(L_{Room_i}\right) := N\left(L_{Room_i}\right) + 1$.

Закон розподілу ймовірностей для випадкових величин - координат точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ залежить від використовуваної технології визначення місця розташування. Величина (x_i', y_i') характеризує обчислене місце розташування МАП і формується на основі статистики вимірювань помилок визначення місця розташування. Збір даної статистики здійснюється на етапі розгортання БМПД.

Оскільки конфігурація приміщень в різних будівлях відмінна одна від одної, матеріали стін, міжкімнатних перекриттів і дверей вносять спотворення в поширення радіосигналу і сам сигнал БМПД досить нестабільний, то доцільно статистику вимірювань помилок визначення місця розташування представити у вигляді гістограми частот (ряду розподілу):

$$\lambda_{e_L} = \left\{ P_e, P\{a \le e_L < b\} = \sum_{a \le e_L < b} p(e_L) \,\middle|\, \sum_{0 \le e_L \le R_{\text{e}}} p(e_L) = 1 \right\}, \qquad (1.7)$$

де R_{e} - максимальне значення помилки визначення місця розташування; $P\{a \le e_L < b\}$ - ймовірність того, що помилка визначення місця розташування лежить на відрізку (a, b) , де a - нижня межа, b - верхня межа відрізка;$\sum_{a \le e_L < b} p(e_L)$- сума ймовірностей виникнення помилки визначення місця розташування, що дорівнює величині e_L . Графічне представлення даного ряду розприділення для розглянутих технологій зображено на рис. А.3.

Оцінка часу навчання системи визначення місця розташування для отримання ряду розподілу (1.6) залежить від кількості вимірювань в приміщеннях і їх щільності. Час вимірювання рівня сигналу в сучасних точках доступу і МАП складає долі секунди. Для досліджуваної карти приміщень, представленої на рис. А.1, число точок вимірювань для методів k - найближчих сусідів і баєвського підходу, з урахуванням того, що вимірювання здійснювалися через кожен метр по горизонталі і вертикалі, формуючи таким образом сітку вимірювань, склало значення близько 400 точок. Значення отримано з використанням програми для ЕОМ [29]. Таким чином, оцінююче значення часу навчання системи визначення місця розташування для розглянутого прикладу становить орієнтовно 7 хвилин без урахування часу, що витрачається на переміщення вимірювача.

Оскільки на результат вимірювання рівня сигналу впливає чимала кількість факторів [29], включаючи конфігурацію приміщень, розміщення меблів, кількість випромінювачів і точок прийому, то періодичність перенавчання системи визначення місця розташування необхідно встановлювати виходячи з фактичних змін в даних параметрах:

– перепланування будівлі;

– зміна інтер'єру будівлі;

– реєстрація нових користувачів МАП;

– зміни обладнання БМПД;

– планування заходів з залученням нових користувачів МАП та інші події.

Перший етап реалізації методу Монте-Карло - формування випадкової точки (x_i', y_i') по заданому закону розподілу. Основою методу Монте-Карло є отримання більшого числа реалізації стохастичного (випадкового) процесу, який формується таким чином, щоб його ймовірнісні характеристи збігалися з аналогічними величинами розв'язуваної задачі. Для поточного завдання таким стохастичним процесом є процес визначення місця розташування, а випадковою величиною - помилка визначення місцезнаходження. Тому

генератор випадкових чисел, який формує координати випадкової точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ повинен виробляти випадкові числа у відповідність з законом розподілу помилки визначення місця розташування. Ряди розподілу у вигляді гістограм частота помилок визначення місця розташування для різних технологій представлені на рис. А.3. Якщо уявити щільність розподілу помилки визначення місця розташування у вигляді градієнта всередині кола з діаметром R_e , то графічно це буде виглядати приблизно так, якпоказано на рис. 1.6. З даного малюнка видно, що координати випадкових точок $(x_i', y_i'), i = \overline{1, N_{MC}}$ при формуванні їх за законами, представленим у вигляді рядів розподілуі зображених на рис. А.3, частіше виявляються в районі центру кола, ніж у її країв. Такий підхід дозволяє врахувати особливості використовуваної технології визначення місця розташування і підвищити достовірність процесу класифікації місця розташування МАП.

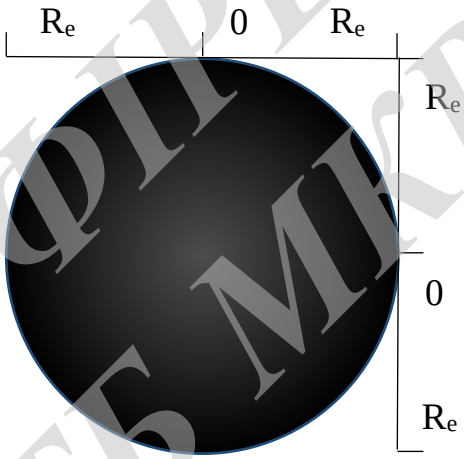


Рисунок 1.6 - Графічне представлення щільності розподілупомилки визначення місця розташування всередині зонипохибки з радіусом R_e

Внаслідок застосування методу Монте-Карло значення функції $F_{Sg}(L_{Room}, (\tilde{x}, \tilde{y}), R_e)$ обчислюється як

$$F_{Sg}(L_{Room}, (\tilde{x}, \tilde{y}), R_e) = \frac{N(L_{Room})}{N_{MC}}, \quad (1.8)$$

оцінка ймовірностей того, що користувач знаходиться в приміщенні з того чи іншого рівня захищеності:

$$P_{L_{Room}} = \left\{ \frac{N(\tilde{L}_{Room}="OI")}{N_{MC}}, \frac{N(\tilde{L}_{Room}="KI")}{N_{MC}} \right\}. \quad (1.9)$$

Точність даного методу істотно залежить від числа випробувань - N_{MC} і параметрів генератора випадкових чисел, який використовується для формування координат випадкової точки $(x_i', y_i'), i = \overline{1, N_{MC}}$. В роботі [4, с. 235]

похибка методу Монте-Карло оцінюється як $\varepsilon \approx \frac{1}{\sqrt{N_{MC}}}$. Таким чином, при заданій точності $\varepsilon_{\text{необ}}$ необхідну кількість випробувань складає $N_{MC} \approx \frac{1}{\varepsilon^2_{\text{необ}}}$.

Виходячи з даних виразів і заданого порогу точності методу, можна вибрати необхідну кількість випробувань. У табл. 1.3 представлені дані про відповідність кількості випробувань заданої точності методу Монте-Карло.

Таблиця 1.3 - Відповідність кількості випробувань від заданої точності методу Монте-Карло

Точність, $\varepsilon_{\text{необ}}$	0,001	0,002	0,005	0,01	0,015	0,02	0,05
Кількість випробувань, N_{MC}	1000000	250000	40000	10000	4444,(4)	2500	400

Оскільки запропонована оцінка (1.5) є відносною частотою, то вона володіє такими статистичними властивостями як незміщеність, спроможність (на основі закону великих чисел) і ефективність [30], при цьому вона є асимптотично нормальною відповідно до теореми Муару-Лапласа.

Отримані в (1.8) оцінки ймовірності знаходження МАП в приміщеннях того чи іншого рівня захищеності можуть бути використані для прийняття рішення системою управління безпекою МАП про те, в приміщенні якого рівня захищеності знаходиться МАП. Критерій прийняття рішення про рівень захищеності приміщення, запропонований в магістерській роботі представлений таким співвідношенням:

$$\tilde{L}_{Room} = \begin{cases} \text{"KI"}, \text{при } \frac{N(\tilde{L}_{Room}=\text{"KI"})}{N_{MC}} \geq L_K^{\text{необ}} \\ \text{"OI"}, \text{при } \frac{N(\tilde{L}_{Room}=\text{"KI"})}{N_{MC}} < L_K^{\text{необ}} \end{cases} \quad (1.10)$$

де граничне значення для критерію $L_K^{\text{необ}}$ визначаються таким чином, щоб виконувалася вимога замовника за кількістю помилок 2-го роду:

$$P_\beta\left(\tilde{L}_{Room} > L_{Room}\right) \leq P_\beta^{\text{доп}} \quad (1.11)$$

Важливим завданням системи управління безпекою МАП є забезпечення конфіденційності інформації. Грунтуючись на цьому, граничне значення $L_K^{\text{необ}}$ має обиратись у такий спосіб, щоб конфіденційність інформації була забезпечена. Критичним показником достовірності визначення місця розташування МАП в спеціальних приміщеннях ЗКМ є величина помилки 2-го роду. Нижче, в табл. 1.4 подано пояснення, що характеризують вплив помилки

класифікації місця розташування МАП на забезпечення конфіденційності інформації.

Таблиця 1.4 – Вплив помилки класифікації місця розташування МАП на конфіденційність інформації

Тип помилки	Помилка 1-го роду	Помилка 2-го роду
Прийняте рішення	Конфігурація МАП блокує функціональні можливості МАП, які в даному місцерозположенні МАП дозволені	Конфігурація МАП залишає не заблоковані функціональні можливості МАП, які повинні бути відключені у даному місцерозположенні
Наслідки	1. Конфіденційність інформації не порушена 2. Порушена доступність послуг	1. Конфіденційність інформації порушена

Таким чином, значення критерію (1.10) і вимог (1.11) дозволяють регулювати рівні помилок 1-го і 2-го роду при ухваленні рішення про місце знаходження МАП в спеціальних приміщеннях ЗКМ, при цьому помилки 2-го роду являються критичними, оскільки порушують конфіденційність інформації, в той час як помилки 1-го роду призводять тільки до порушення доступності деяких послуг, що надаються користувачеві МАП. Графічно зона помилок 1-го, 2-го роду представлена на рис. 1.7.

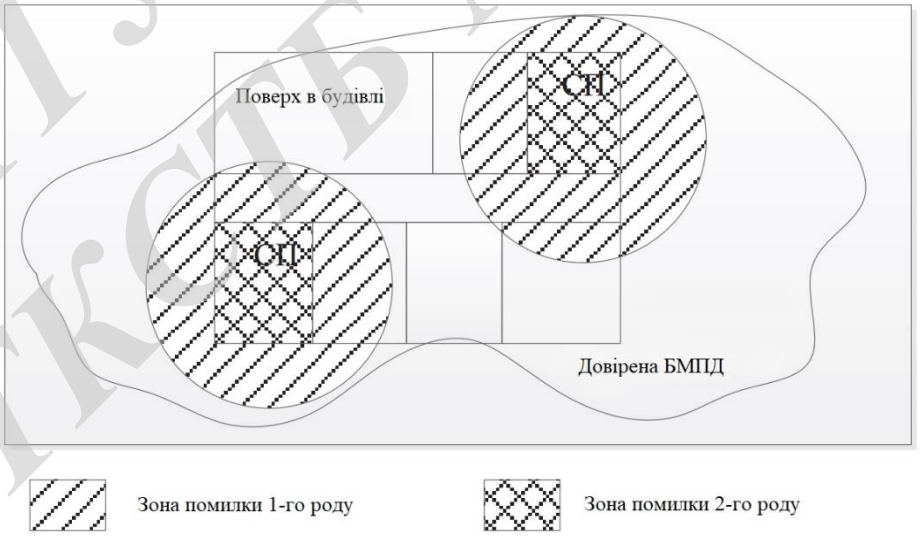


Рисунок 1.7 - Графічне представлення помилок 1-го, 2-го роду при визначенні місценаходження МАП в спеціальних приміщеннях (СП)

Залежно від обраної технології визначення місця розташування МАП і значення порога прийняття рішення будуть відрізнятися і зони помилок 1-го2-го роду.

1.3.2 Розробка імітаційної моделі системи визначення місця розташування, що дозволяє оцінити ймовірність місцезнаходження мобільного абонентського пристрою в спеціальному приміщенні

Результати розробки імітаційної моделі викладені в роботах [31]. В якості *об'єкта моделювання* обраний процес визначення місця розташування МАП, що включає в себе:

– моделювання руху користувачів МАПпо території будівлі, в якому розгорнуто корпоративні мережі з різним рівнем захищеності;

– моделювання вимірювань рівнів сигналу БМПД МАП точками доступу;

аналітичне обчислення ймовірності знаходження МАП в спеціальних приміщеннях.

Основними завданнями (кордонами) імітаційного моделювання є:

– обгрунтування алгоритмічної можливості розв'язання задачі підвищення достовірності визначення місцезнаходження МАП в спеціальних приміщеннях за рахунок застосування методу статистичних випробувань (методу Монте-Карло);

– обгрунтування оптимальних параметрів алгоритмів визначення місця розташування і обчислення ймовірності знаходження МАП в спеціальному приміщенні.

Імітаційне моделювання здійснювалося з урахуванням наступних обмежень:

– БМПД, що складається з довірених точок доступу, охоплює всі приміщення, в яких необхідно надавати послуги мобільним користувачам;

– технічні характеристики МАП і точок доступу БМПД відомі і стабільні;

– в якості основи для технології визначення місця розташування використовується БМПД на базі стандарту 802.11 і один з наступних методів: метод трилатерації (тріангуляції), метод k -найближчих сусідів, метод, заснований на використанні баєвського підходу;

– вплив параметрів, що характеризують особливості будови, в тому числі, середні розміри приміщень, наявність холів і коридорів, товщина стін,поверховість на поширення радіосигналу враховується при навчанні системи формування ряду розподілу помилок визначення місця розташування МАП;

– параметри радіосигналу (вид модуляції, смуга частот, маніпуляційна швидкість і ін.) не роблять істотного впливу на вимірювання рівня сигналу МАП, що використовується в якості вихідних даних;

– вплив швидких завмирань внаслідок багатопроменевості поширення радіохвиль в приміщеннях в разі вибору технології трилатерації враховується за рахунок застосуванням відповідної моделі поширення радіохвиль за аналогією з умовами міської інфраструктури для щільної забудови;

– регулювання потужності МАП з боку базових станцій в зоні доступу БМПД не проводиться.

Основним критерієм ефективності для порівняння технічних рішень з визначення місця розташування МАП є: *достовірність і своєчасність визначення місцезнаходження МАП* в спеціальному приміщенні.

В якості середовища імітаційного моделювання було використано пропрограмне забезпечення AnyLogic [31] версії 6.4.1. Реалізація запропонованої моделі виконана за допомогою бібліотек Enterprise Library, Pedestrian Library і Rail Yard Library. Функціонально розроблений додаток для імітаційного моделювання в середовищі AnyLogic складається з наступних компонентів:

1. Модуль формування траєкторії руху користувача МАП.
2. Модуль формування запитів на доступ до послуг ЗКМ.
3. Модуль вимірювання рівня сигналу МАП.
4. Модулі визначення місця розташування на базі методів трилатерації, *k* - найближчих сусідів і баєвського підходу.
5. Модуль обчислення ймовірності місця знаходження МАП в спеціальному приміщені з урахуванням методу Монте-Карло і оцінювання помилок класифікації.
6. Підсистема аналізу статистичних характеристик досліджуваних випадкових процесів і випадкових величин і візуалізації результатів моделювання.

Таким чином, задум імітаційного моделювання полягає в моделюванні руху користувачів МАП, в процесі якого здійснюються вимірювання рівня

сигналу МАП точками доступу і їх подальша аналітична обробка з метою обчислення ймовірності знаходження МАП в спеціальних приміщеннях і оцінювання помилок класифікації.

В основі функціонування модулів формування траєкторії руху користувача МАП і формування запитів на доступ до послуг лежить зібрана статистика використання МАП за допомогою розробленого додатка [76]. Фрагмент статистики представлений на рис. 1.8. До її складу входить інформація про послуги, час і місце використання послуг, ідентифікаційні дані МАП.

```
%%event=inc_sms:900;time=03.04.2014      18:27:17      GMT+12:00
;latitude=0.0;longitude=0.0;network_type=GSM;base_station_id=321
466;iface_name=lo,iface_mac=null,ip_addr=::1%1,ip_addr=127.0.0.1
,ip_addr=10.223.88.183,iface_name=rmnet1,iface_mac=null;
%%event=finish_call;time=04.04.2014      07:23:58      GMT+12:00
;latitude=0.0;longitude=0.0;network_type=GSM;base_station_id=321
187;iface_name=lo,iface_mac=null,ip_addr=::1%1,ip_addr=127.0.0.1
,ip_addr=10.223.106.125,iface_name=rmnet1,iface_mac=null;
```

Рисунок 1.8 - Фрагмент статистики використання мобільного пристрою

Послідовність точок траєкторії руху, як і послідовність запитів, реалізовані у вигляді ланцюга Маркова, що формується за рахунок вбудованого в середовище AnyLogic генератора випадкових чисел з рівномірним законом розподілу і сформованих на основі емпіричних даних матриць перехідних ймовірностей. Модулі формування траєкторії руху користувача МАП і формування запитів на доступ до послуг ЗКМ реалізовані в додатку [32].

В якості карти розташування приміщень використовувалася схема, представлена на рис. 1.9.

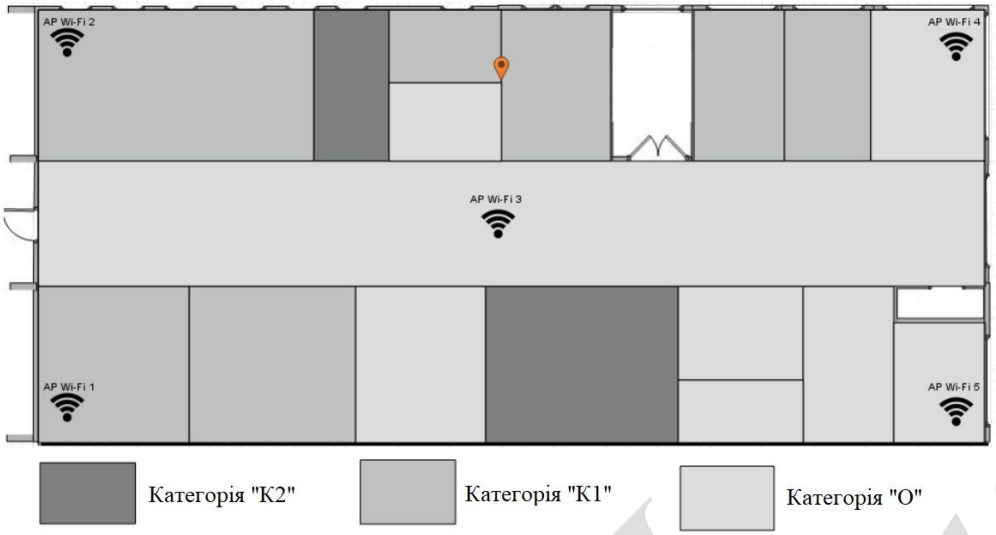


Рисунок 1.9 - Схема приміщень для проведення експериментів

Приміщення розділені за рівнями захищеності. Карта приміщень в імітаційній моделі реалізована у вигляді структури, що описується виразом (1.1).

Для реалізації імітаційного моделювання поширення радіосигналу був проведений експеримент з метою дослідження коливань рівня сигналу в точці прийому від декількох джерел. Метою даного експерименту було визначення найбільш оптимального закону формування рівня сигналу в імітаційній моделі.

В експерименті було використано наступне обладнання:

1. Ноутбук з технічними характеристиками: процесор: Core i5 2 300 МГц; Встановлена пам'ять (ОЗУ): 4,00 ГБ; Тип системи: 64-розрядна ОС; ОС: Windows 7 Professional SP 1.

2. USB-адаптери 3Com OfficeConnect Wireless 54 Mbps 11g Compact.

3. Три точки доступу на базі трьох ПЕОМ з технічними характеристиками: процесор: Dual 3.20 GHz, IntelCore i5-3470; встановлена пам'ять (ОЗУ): 8,00 ГБ; тип системи: 64-розрядна ОС; ОС: Windows 7 Professional SP

Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу представлена на рис. 1.10.

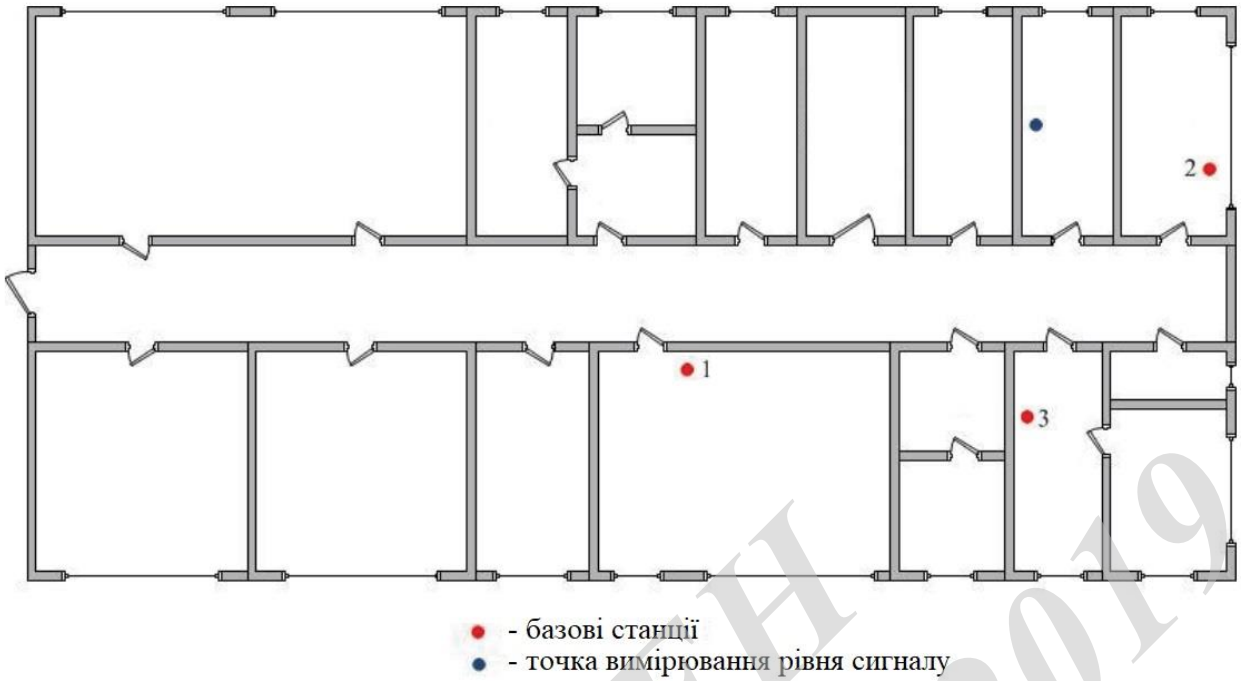
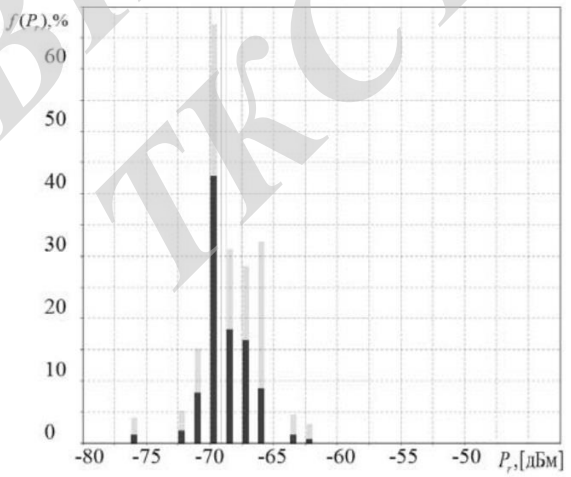


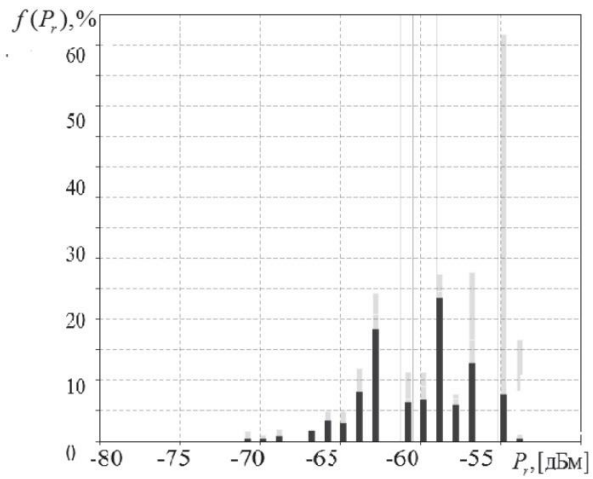
Рисунок 1.10 - Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу

В експерименті використовувалися широкомовні пакети, а також періодично проводився запис рівня сигналу базових станцій в точці прийому. Вимірювання рівня потужності сигналу здійснювалася при чотирьох різних орієнтаціях бездротового адаптера, що виконує роль точки прийому. Докладні чисельні результати вимірювань представлені в табл. Б.1 додатка Б.

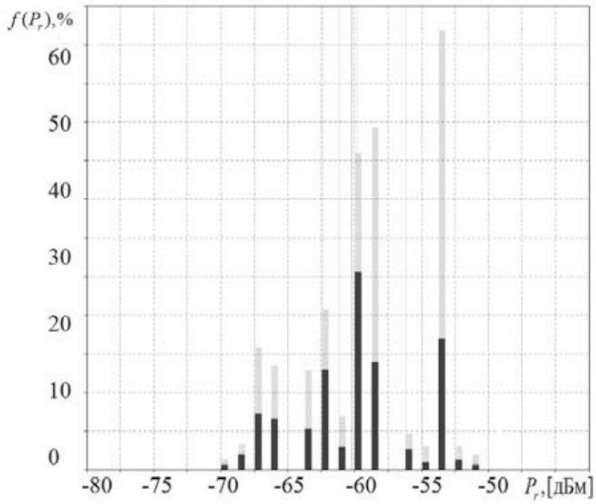
На рис. 1.11 а-в представлені щільності розподілу рівнів потужності сигналу бездротових точок доступу в точці прийому.



а)



б)



в)

Рисунок 1.11 Густині розподіли рівнів потужності сигналу бездротових точок доступу в точці прийому: а) точка доступу № 1, б) точка доступу № 2, в) точка доступу № 3

Результати вимірювань у вигляді щільності розподілу рівнів потужності сигналу бездротових точок доступу для різних положень точки прийому представлені на рис. Б. 1 додатка Б.

Статистичні параметри функції розподілу ймовірностей рівнів сигналу бездротових точок доступу для різних положень точки прийому, а також результати перевірки гіпотези про приналежність вибірок нормальному закону розподілу відповідно до критерію χ^2 [33] представлені в табл. 1.5.

Таблиця 1.5 - Статистичні параметри розподілу ймовірностей рівнів потужності сигналу бездротових точок доступу для різних положень точки прийому

№ точки доступу	Положення	Виб. середнє	Виб. СКО	Довірить. інтервал	Мін. знач.	Макс. знач.	Рівень значущості α для критерію x^2 при перевірці гіпотези про приналежність вибірки до нормального закону розподілу
1	1	-71,914	0,801	0,21	-74	-70	0,1 α 0,2
	2	-70,015	1,566	0,388	-73	-66	0,0005 α 0,001
	3	-72,03	1,46	0,291	-77	-67	α 0,0005
	4	-70,986	0,972	0,225	-73	-69	0,01 α 0,025

	1-4	-71,304	1,496	0,17	-77	-66	α 0,0005
2	1	-61,194	2,745	0,696	-71	-57	0,01 α 0,025
	2	-58,969	3,216	0,796	-67	-55	0,2 α 0,3
	3	-67,218	3,227	0,629	-70	-55	α! 0,5
	4	-55,167	0,983	0,982	-57	-54	α! 0,5
	1-4	-60,432	3,322	0,426	-71	-54	α 0,0005
3	1	-63,836	1,625	0,415	-71	-61	α 0,0005
	2	-60,923	2,938	0,727	-70	-58	0,001 α 0,005
	3	-65,921	3,236	0,631	-72	-57	0,001 α 0,005
	4	-64,946	3,487	0,807	-72	-59	α 0,0005
	1-4	-64,179	3,508	0,396	-72	-57	0,05 α 0,1

Як видно з табл. 1.5 рівень значущості α при перевірці за допомогою критерію типу X^2 гіпотези про приналежність вибірки нормальному закону не перевищує значення 0,1.

Проведений експеримент також показав, що похибка вимірювання рівня сигналу в середньому становить 2,188 дБм зі середньоквадратичним відхиленням (СКВ), рівним 1,039 дБм при довірчому інтервалі для вибіркового середнього - 0,654 дБм . Таким чином, результати експерименту дозволяють використувати в розробленій імітаційній моделі нормальний закон розподілення помилки вимірювання потужності сигналу з наступними параметрами: М $e(t) = 0, \sigma\, e(t) = 3$ дБм і модель вимірювань у вигляді:

$$\tilde{P}(t) = P_r(t) + e(t) = P_t \cdot \frac{\lambda^2}{(4\pi R^2(t))} + \frac{1}{3[\text{дБм}]\sqrt{2\pi}} e^{-\frac{x^2}{18[\text{дБм}]}} \qquad (1.12)$$

де $P_r(t)$ - рівень сигналу, обчислений у відповідності з виразом (А.4);

x - випадкова величина, розподілена по рівномірному закону в діапазоні [0,1] P_t - відома відстань від користувача МАП до точки вимірювання (точки доступу), яка визначається траєкторією руху користувача.

Дана модель вимірювань рівня прийнятого точками доступу сигналу реалізована в модулі вимірювання рівня сигналу бездротової мережі розробленої імітаційної моделі.

В імітаційній моделі змінними параметрами є:

P_t – рівень потужності передавача [Вт];

f- частота передавача [Гц];

$Rooms$ - структура, яка містить відомості про координати приміщення і вимоги за рівнем з захищеності;

M $e(t)$- математичне відхилення помилки вимірювання рівня приймаючого сигналу;

$e(t)$ - середньоквадратичне відхилення помилки виміру рівня приймаючого сигналу;

номера використовуваних для вимірювань точок доступу;

координати (розташування) використовуваних для вимірювань точок доступу; *dx_kNN, dy_kNN* - параметри сітки карти вимірювань сигналів для метода *k* -найдлижчих сусідів, де *dx _ kNN* - крок сітки по горизонталі і *dy_kNN*- крок сітки по вертикалі;

k_kNN - число "сусідів" сигнального простору, що використовується в методі *k* - найдлижчих сусідів;

- кількість вимірювань в кожній точці сигнального простору для методу, заснованого на баєвському підході;

(dx_HMM , dy_HMM) - параметри сітки карти вимірювань сигналів для методу, заснованого на баєвському підході, де *dx_HMM* - крок сітки по горизонталі і *dy_HMM* - крок сітки по вертикалі;

k_HMM - число "сусідів" сигнального простору, що використовується в методі, заснованому на баєвському підході;

N_MC - кількість випробувань для методу Монте-Карло;

закон розподілу випадкової величини, що використовується для здійснення випробувань в методі Монте-Карло (рівномірні або емпіричний);

R_e - параметр , що визначає величину, заданого радіуса зони помилки визначення місця розташування з центром в точці з обчисленим місцем розташування користувача МАП.

μ поріг спрацьовування для класифікації розташування МАП.

Моделюючий алгоритм імітаційної моделі представлений в додатку В.

В якості *критеріїв ефективності* розроблюваної моделі використовуються оцінки помилок класифікації розташування, що виражаються через чисельні значення ймовірностей помилок 1-го і 2-го роду. Ухвалені рішення про достовірності класифікації розташування здійснюються за рахунок порівняння поточного моделіруючого розташування і обчисленого за рахунок застосування оцінюючої аналітичної моделі.

1.3.3 Оцінка якості імітаційної моделі системи визначення місця розташування мобільного абонентського пристрою

Оцінка якості і витрат виділених ресурсів на розробку моделі проводилася на основі [34]. При імітаційному моделюванні на достовірність результатів впливає цілий ряд додаткових факторів, основними з яких є:

– моделювання випадкових факторів, засноване на використанні датчиків випадкових чисел, які можуть вносити "спотворення" вповедінку моделі;

– наявність нестаціонарного режиму роботи моделі;

– використання декількох різнотипних математичних методів в рамках однієї моделі;

– залежність результатів моделювання від плану експерименту;

– необхідність синхронізації роботи окремих компонентів моделі.

Придатність імітаційної моделі для вирішення задач дослідження характеризують тим, в якій мірі вона володіє цільовими властивостями. Основними з них є: *адекватність* , *стійкість* , *чутливість* .

Під *адекватністю* розуміють ступінь відповідності моделі тому реальному явищу або об'єкту, для опису якого вона будується. Адекватність моделі визначається ступенем її відповідності не стільки реальному об'єкту, скільки цілям дослідження. Процедура оцінки адекватності моделі проводилася на основі методів математичної статистики за рахунок порівняння вимірювань на реальній системі і результатів експериментів на моделі.

Стійкість моделі як здатність зберігати адекватність при дослідженні ефективності системи на всьому можливому діапазоні робочого навантаження, а також при внесенні змін у конфігурацію системи. Стійкість результатів моделювання оцінена методами математичної статистики.

Чутливість моделі полягає в оцінюванні реакції моделі до зміни параметрів навантаження і внутрішніх параметрів самої системи.

Перевірка адекватності моделі здійснювалася по параметру вибіркове середнє значення помилки визначення місця розташування $\bar{e}_L$, а також вибіркове середньоквадратичне відхилення помилки визначення місця розташування $\bar{\sigma}_{\text{L}}$.

Перевірка адекватності моделі по параметру $\bar{e}_L$ (середнє значення помилки визначення місця розташування) представлена в табл. 1.6, за параметром $\bar{\sigma}_{\text{L}}$ (також вибіркове середньоквадратичне відхилення помилки визначення місця розположення) - в табл. 1.7.

Таблиця 1.6 Перевірка адекватності моделі по параметру $\bar{e}_L$

Позначення відгуку	$\bar{e}_L$	$\bar{e}_L^*$
Кількість складових вибірок	180	177
Середнє значення, $\bar{Y}$	2,481	2,269
Оцінка дисперсії відгуку, D_n	2,758	2,459
Дисперсія різниці, D_{pn}	2,634	
Значення t -статистики, t_n	0,62	
Кількість ступенів свободи	201	
Критичне значення t - статистики $t_{кр}$	1,653	

Таблиця 1.7 - Перевірка адекватності моделі по параметру $\bar{V}_L$

Позначення відгуку	$\bar{e}_L$	$\bar{e}_L^*$
Кількість складових вибірок	140	140
Середнє значення, $\bar{Y}$	1,661	1,763
Оцінка дисперсії відгуку, D_n	0,168	0,130
Дисперсія різниці, D_{pn}	0,151	
Значення t -статистики, t_n	0,62	
Кількість ступенів свободи	288	
Критичне значення t - статистики $t_{кр}$	1,65	

Число ступенів свободи (t –статистики) для вибраних параметрів находиться в межах від 200 до 300. Для рівня значущості $\alpha = 0{,}05$ при якому число ступенів свободи критичне значення t –статистики $t_{кр} \approx 1{,}653$. Порівнюючи значення t -статистики в табл. 1.6-1.7 с $t_{кр}$, бачимо, що можна прийняти гіпотезу про близькість середнього значення відгуків моделі і реальної системи ($t_{моделі} \leq t_{кр}$). Отже, імітаційна модель адекватна досліджуваної системи.

На початку часу роботи моделі процеси, які протікають в ній не будуть стаціонарними. Через деякий інтервал часу перехідний процес закінчиться, і модель перейде в стаціонарний режим роботи, ймовірнісні характеристики якого не залежатимуть від часу моделювання [6]. Так як на практиці обмежуються відсіканням початкового періоду, що дорівнює 3-4 кратному часу проходження моделі самими " повільними заявками", в якості *тривалості перехідного періоду* приймемо $T_0 = 2496$ модельних одиниць або $N = 9$ прогонів моделі.

Визначення необхідного *числа реалізацій n* забезпечує задану точність і надійність результату. Для визначення числа реалізацій скористаємося формулою [6]:

$$n = \frac{t_a^2(1-p)}{\varepsilon^2}. \quad (1.13)$$

Для знаходження ймовірності необхідна попередня оцінка на малому числі випробувань. Так як проведення попередньої оцінки не не передбачається, то скористаємося найгіршим випадком: $p = 0{,}5$.

Для величини довірчого інтервалу $\varepsilon = 10^{-2}$ і апріорної ймовірності настання події $\alpha = 0{,}99$ значення t-критерію Стьюдента дорівнює $t_\alpha = 2{,}53$, а число реализаций:

$$n = \frac{2{,}53^2 - 0{,}5(1-0{,}5)}{10^4} = 16003. \quad (1.14)$$

Для визначення найбільш впливових вхідних параметрів моделі необ-обхідно дослідити *чутливість* імітаційної моделі. Перевірку чутливих-ності вості моделі до зміни вихідних даних здійснимо на прикладі. Діапазони зміни вхідних параметрів представлені в табл. 1.8, де k - число найбільш ймовірних станів прихованої марковської моделі, що враховуються при обчисленні розташування МАП, а M - число вимірювань в точці, що виробляють для збору статистики вимірювання рівня сигналу МАП.

Розрахунок кількості дослідів для дослідження чутливості імітаційної моделі показав, що необхідно провести не менше 10 дослідів. Значення вхідних параметрів наведені в табл. 1.9.

Таблиця 1.8 - Діапазони зміни вхідних параметрів

Вхідні параметри	Мінімальне значення параметра	Максимальне значення параметра	Приріст параметра,%
k	1	10	100
M	10	180	100

Таблиця 1.9 - Значення вхідних параметрів для оцінки чутливості

№ експ.	1	2	3	4	5	6	7	8	9	10
k	1	2	3	4	5	6	7	8	9	10
M	10	20	30	40	50	60	70	80	90	100

Результати дослідження чутливості імітаційної моделі наведені в табл. 1.10.

Таблиця 1.10 - Результати дослідження чутливості імітаційної моделі

Вхідний параметр	Вихідний параметр $\hat{e}_L$			Співвідношення з приростом вхідного параметра
	min	max	$\delta\hat{e}_L, \%$	
k	2,445	3,86	44,8	0,448
M	2,481	3,131	23,1	0,231

Збільшення вхідних параметрів і зміни вихідного параметра вираховуються за формулою

$$\delta X = \frac{2\cdot(max\ X - \min X)}{max\ X - \min X} \cdot 100\% \qquad (1.15)$$

Перевірка чутливості підтвердила факт того, що "відгуки" (вихідні результати) моделі відповідають критеріям чутливості моделі.

Внаслідок оцінки якості моделі можна зробити висновок, що модель досить чутлива до вхідних результатів.

Стійкість результатів моделювання може бути також оцінена методами математичної статистики. Для перевірки гіпотези про стійкість результатів може бути використаний критерій Уілкоксона, який служить для перевірки того, чи належать дві вибірки до однієї і тієї ж генеральної сукупності (тобто чи володіють вони одною і тою же статистичнию ознакою). В якості вибірок для оцінки стійкості результатів взяті показники помилок визначення місця розташування МАП, представлені в табл. 1.11.

Таблиця 1.11 - Вибірки результатів моделювання оцінки помилки визначення місця розташування МАП

№експ.	1	2	3	4	5	6	7	8	9	10
Вибірка №1	1,783	4,801	3,195	1,419	1,418	0,763	2,473	2,699	0,463	1,067
Вибірка №2	1,008	0,769	0,728	0,437	1,549	1,099	1,454	2,080	3,195	5,623

Для рівня значимості $\alpha = 0{,}05$ значення статистики для прийняття гіпотези про однорідність вибірок повинна задовольняти нерівності $|T| \leq 1{,}96$. Для представлених вибірок статистика за критерієм Уілкоксона дорівнює $T = 0{,}82$. Відповідно, вибірки з рівнем значущості $\alpha = 0{,}05$ можна вважати однорідними, що свідчить про те, що результати моделювання стійкі.

1.3.4 Результати моделювання визначення місця розташування мобільного абонентського пристрою

Результати моделювання отримані для схеми приміщень, які показані на рис. 1.9. В якості вихідних даних взяті такі дані, як:

1) технічні характеристики МАП:

– потужність передавача +0,07943282347242815 Вт;

– частота передавача 2,4 ГГц;

– помилка вимірювання рівня потужності МАП, яка моделюється нормальним законом розподілу ймовірностей з наступними статистичними параметрами: $M[P_r] = 0$ Дбм, $\sigma\ [P_r] = 3$ Дбм.

2) розташування, рівні захищеності і параметри приміщень визначаються схемою приміщень, представленою на рис. 1.9, при розмірах будівлі 16,8м × 38,0м.

3) точки доступу бездротової мережі в системі координат досліджуваної будівлі розташовані в таким способом: $AP_1 = (3{,}6\text{м}; 19{,}2\text{м})$, $AP_2 = (3{,}6\text{м}; 5{,}2\text{м})$, $AP_3 = (20{,}0\text{м}; 12{,}0\text{м})$, $AP_4 = (37{,}6\text{м}; 5{,}2\text{м})$, $AP_5 = (37{,}6\text{м}; 19{,}2\text{м})$.

Розрахунок місця розташування МАП здійснювався в відповіднно з виразами для методу трилатерації - (А.3) - (А.19), для методу k –найближчих сусідів - (А.20) - (А.25), для методу на основі баєвського підходу - (А.26) - (А.31).

Розрахунок ймовірності місцезнаходження МАП в спеціальному приміщенні здійснювався в відповідності з виразами (1.4) - (1.10).

Результати моделювання отримані за допомогою розроблених програм для ЕОМ [35].

На рис. 1.12 представлена залежність помилок 1-го і 2-го роду при обчислені ймовірності місцезнаходження МАП в спеціальному приміщенні отриманому місця розташування користувача МАП, розрахованому на основі баєвського підходу, в процесі імітаційного моделювання в залежності від часу.

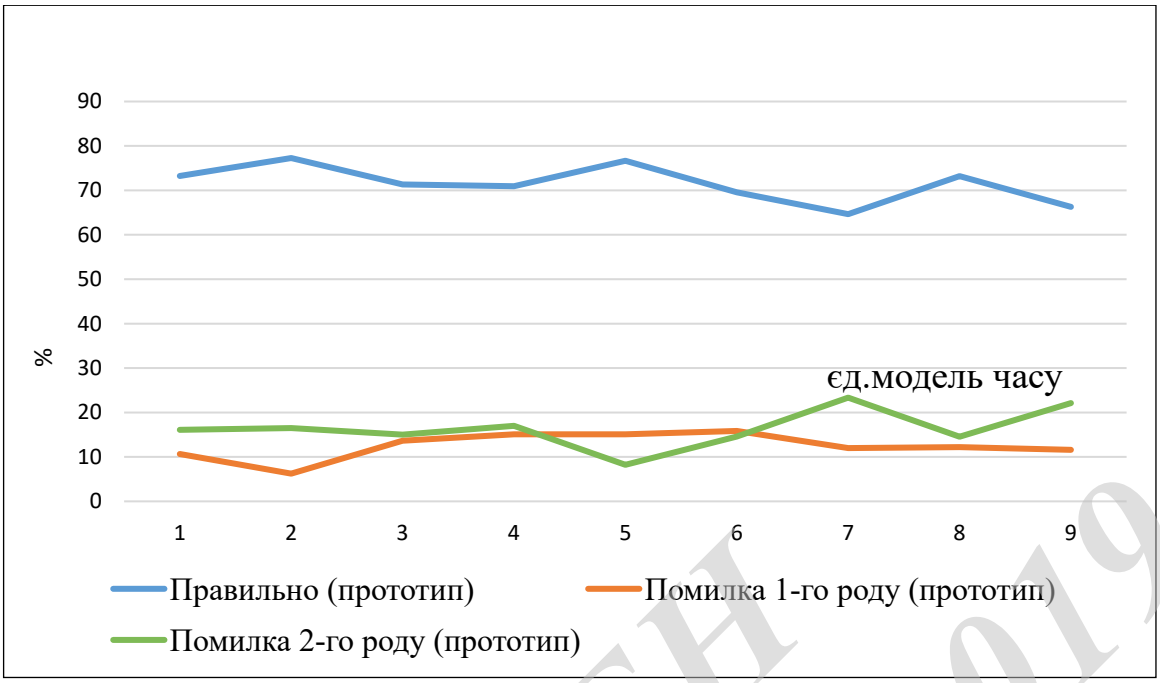


Рисунок 1.12 - Графік залежності помилок 1-го і 2-го роду при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні

У табл. 1.12 представлені чисельні результати експерименту.

Таблиця 1.12 – Залежність помилок 1-го і 2-го роду при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні за отриманим місцем розташування користувача МАП

Од.модел.часу	1	2	3	4	5	6	7	8	9	10	1
Правильно	73,25	77,277	71,335	70,922	76,661	69,572	64,644	73,209	66,29	74,209	73,25
Помилка 1-го роду	10,664	6,24	13,657	15,09	15,107	15,849	12,006	12,225	11,599	13,579	10,664
Помилка 2-го роду	16,085	16,481	15,006	16,987	8,23	14,577	23,348	14,565	22,11	12,21	16,085

Із результатів експериментів видно, що в досліджуваному прототипі без використання методу Монте-Карло помилки 1-го і 2-го роду є випадковими величинами - реалізаціями одного і того ж стаціонарного випадкового процесу з середніми значеннями: $\alpha = 12{,}6016$ і $\beta = 15{,}9599$ з числом правильних прийнятих рішень в середньому в 71,7369 відсотках випадків.

На рис. 1.13 представлена залежність помилок 1-го і 2-го роду при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні за отриманим розташуванням МАП від числа випробувань M в методі Монте-Карло.

При цьому поріг прийняття рішення про рівень захищеності приміщення у відповіднрсті з виразами (1.8), (1.9) і (1.10) було поставлено на рівні $L_{K1}^{\text{необ}} = 0{,}05$; $L_{K2}^{\text{необ}} = 0{,}05$.

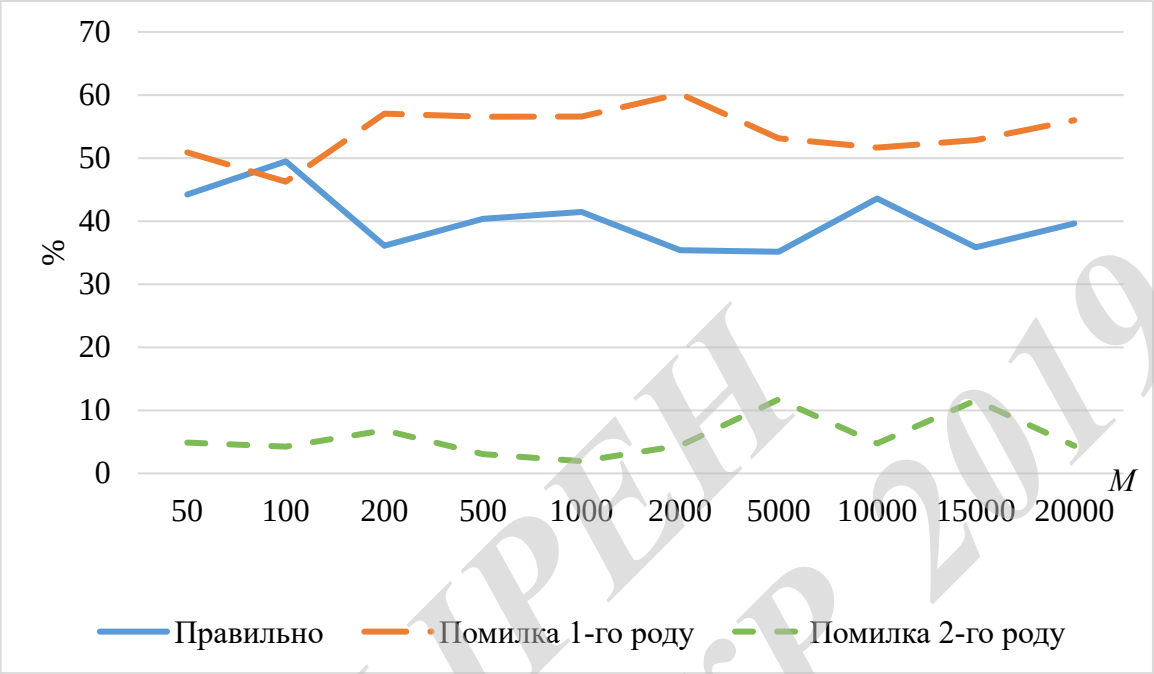


Рисунок 1.13 - Графік залежності помилок 1-го і 2-го роду при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні від числа випробувань *M* в методі Монте-Карло

У табл. 1.13 представлені чисельні результати даних експерименту.

Таблиця 1.13 – Залежність помилок 1-го і 2-го роду при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні від числа випробувань *M* в методі Монте-Карло

M	50	100	200	500	1000	2000	5000	10000	15000	20000
Правильно	44,226	49,482	36,115	40,38	41,461	35,402	35,15	43,586	35,861	39,631
Помилка 1-го роду	50,891	46,263	57,045	56,554	56,598	60,188	53,126	51,652	52,861	55,999
Помилка 2-го роду	4,882	4,254	6,838	3,064	1,94	4,409	11,723	4,761	11,599	4,368

З результатів експерименту з використанням методу Монте-Карло можна зробити кілька висновків:

1) величина помилки 2-го роду в порівнянні прототипом нижче в середньому в 5раз;

2) оптимальну кількість випробувань для методу Монте-Карло становитьM 1000.

При використанні методу Монте-Карло для обчислення ймовірності місцезнаходження МАП в спеціальному приміщенні в якості закону розподілу випадкової величини, що характеризує похибку визначення місця розташування, використовувався рівномірний закон розподілу і емпіричний. Емпіричний закон розподілу визначався гістограмою частот щільності розподілу ймовірностей помилки визначення місця розташування для обраного методу.

В табл. 1.14 представлені результати дослідження ефективності ме-тода Монте-Карло при класифікації місця розташування МАП методом трилатерації для різних законів розподілу ймовірностей випадкової величини.

Таблиця 1.14 Дослідження ефективності методу Монте-Карло при обчисленні ймовірності місцезнаходження МАП в спеціальному приміщенні на основі методу трилатерації в залежності від порога прийняття рішення $L^{\text{необх}}$.

$L_{\text{необх}}$	Рівномірний закон			Емпіричний закон		
	Правильно	α	β	Правильно	α	β
0,0000001	36,152	60,525	3,321	14,314	85,044	0,64
0,000001	39,858	48,425	11,715	14,162	85,264	0,573
0,00001	36,208	57,335	6,456	23,178	76,821	0
0,0001	38,209	56,253	5,537	14,025	85,252	0,722
0,001	38,295	50,727	10,976	17,204	80,943	1,852
0,01	34,635	61,407	3,956	17,403	80,753	1,842
0,02	33,385	64,57	2,044	19,336	78,24	2,422
0,03	39,484	48,107	12,408	20,525	74,756	4,717
0,04	35,593	60,27	4,136	23,053	71,198	5,747
0,05	37,561	56,926	5,512	25,601	71,033	3,365
0,06	36,934	60,137	2,928	26,151	72,217	1,631
0,07	40,6	50,437	8,962	30,201	66,243	3,555
0,08	39,269	51,39	9,339	34,922	62,859	2,217
0,09	37,956	53,359	8,683	36,006	60,802	3,19
0,1	38,117	57,303	4,579	35,296	55,821	8,882
0,11	36,995	53,951	9,052	37,685	52,331	9,983
0,12	40,798	55,212	3,989	40,904	53,515	5,579
0,13	42,216	49,092	8,691	42,503	52,234	5,261
0,14	43,923	49,74	6,336	44,955	48,282	6,761
0,15	45,545	49,141	5,312	47,443	44,008	8,547
0,16	41,708	45,768	12,523	48,852	43,381	7,766

0,17	46,805	41,002	12,192	51,563	41,204	7,232
0,18	47,332	42,312	10,354	47,325	36,603	16,07
0,19	49,665	43,323	7,01	53,104	36,891	10,003
0,2	57,913	35,743	6,343	53,06	32,945	13,994

На рис. 1.14 представлений графік залежності помилок 1-го і 2-го роду від порога прийняття рішення при використанні методу Монте-Карло для визначення ймовірності місцезнаходження МАП в спеціальному приміщенні на основі методу трилатерації.

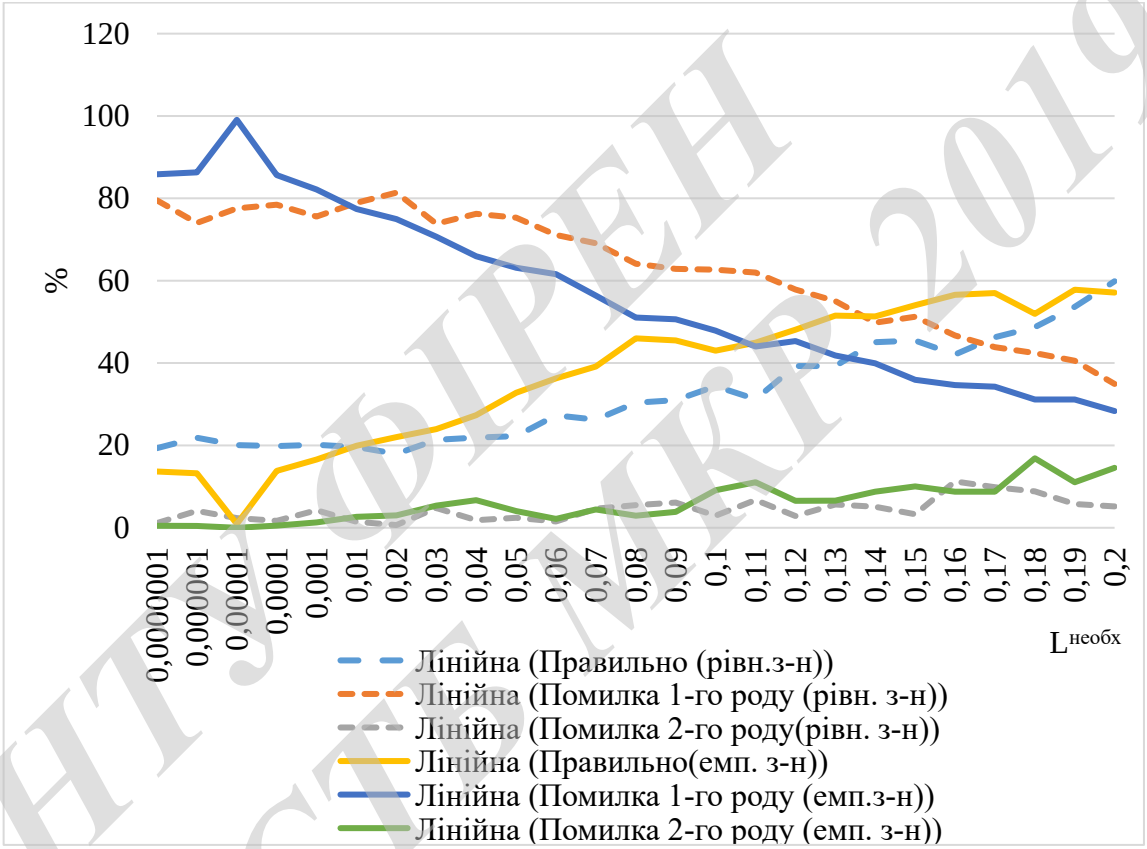


Рисунок 1.14 Графік залежності помилок 1-го і 2-го роду від порога прийняття рішення при використанні методу Монте-Карло

Із результатів експерименту видно, що при використанні емпіричного закону розподілу помилка 2-го роду менше для $L^{\text{неох}} < 0{,}13$ в порівнянні з рівномірним. Однак при цьому кількість правильних рішень для рівномірного закону вище, ніж для емпіричного за умови $L^{\text{неох}} < 0{,}15$.

Результати аналогічного експерименту для методу k -найближчих сусідів представлені в табл. 1.15 і на рис. 1.15.

Таблиця 1.15 - Дослідження ефективності методу Монте-Карло при класифікації місця розташування МАП методом k -найближчих сусідів в залежності від порога прийняття рішення $L^{\text{неох}}$.

$L_{\text{необх}}$	Рівномірний закон			Емпіричний закон		
	Правильно	α	β	Правильно	α	β
0,0000001	19,339	79,506	1,153	13,667	85,836	0,496
0,000001	21,859	74,041	4,099	13,232	86,308	0,458
0,00001	20,074	77,563	2,362	0,93	99,069	0
0,0001	19,838	78,456	1,704	13,831	85,653	0,514
0,001	20,165	75,584	4,249	16,559	82,143	1,296
0,01	19,596	78,927	1,476	19,92	77,403	2,675
0,02	17,953	81,382	0,664	22,036	74,949	3,013
0,03	21,364	73,834	4,801	23,955	70,673	5,371
0,04	21,904	76,248	1,846	27,355	65,943	6,701
0,05	22,26	75,302	2,437	32,786	63,153	4,06
0,06	27,321	71,127	1,55	36,279	61,576	2,144
0,07	26,244	69,09	4,664	39,179	56,364	4,455
0,08	30,389	64,118	5,492	46,022	51,044	2,932
0,09	30,994	62,866	6,139	45,492	50,627	3,88
0,1	34,375	62,692	2,931	43,006	47,872	9,12
0,11	31,251	61,987	6,761	44,941	44,004	11,054
0,12	39,263	57,877	2,859	48,101	45,353	6,544
0,13	39,288	55,053	5,658	51,535	41,857	6,607
0,14	45,067	49,818	5,114	51,313	39,92	8,765
0,15	45,459	51,236	3,304	54,031	35,921	10,047
0,16	42,064	46,685	11,25	56,583	34,664	8,751
0,17	46,281	43,852	9,866	56,987	34,252	8,759
0,18	48,712	42,436	8,85	51,965	31,159	16,874
0,19	53,653	40,579	5,766	57,816	31,137	11,045
0,2	59,867	34,924	5,208	57,108	28,341	14,55

Із результатів експерименту видно, що при використанні емпіричного закону розподілу помилка 2-го роду менше для $L^{\text{неох}} < 0{,}03$ в порівнянні з рівномірним, а кількість правильних рішень вище за умови $L^{\text{неох}} < 0{,}03$.

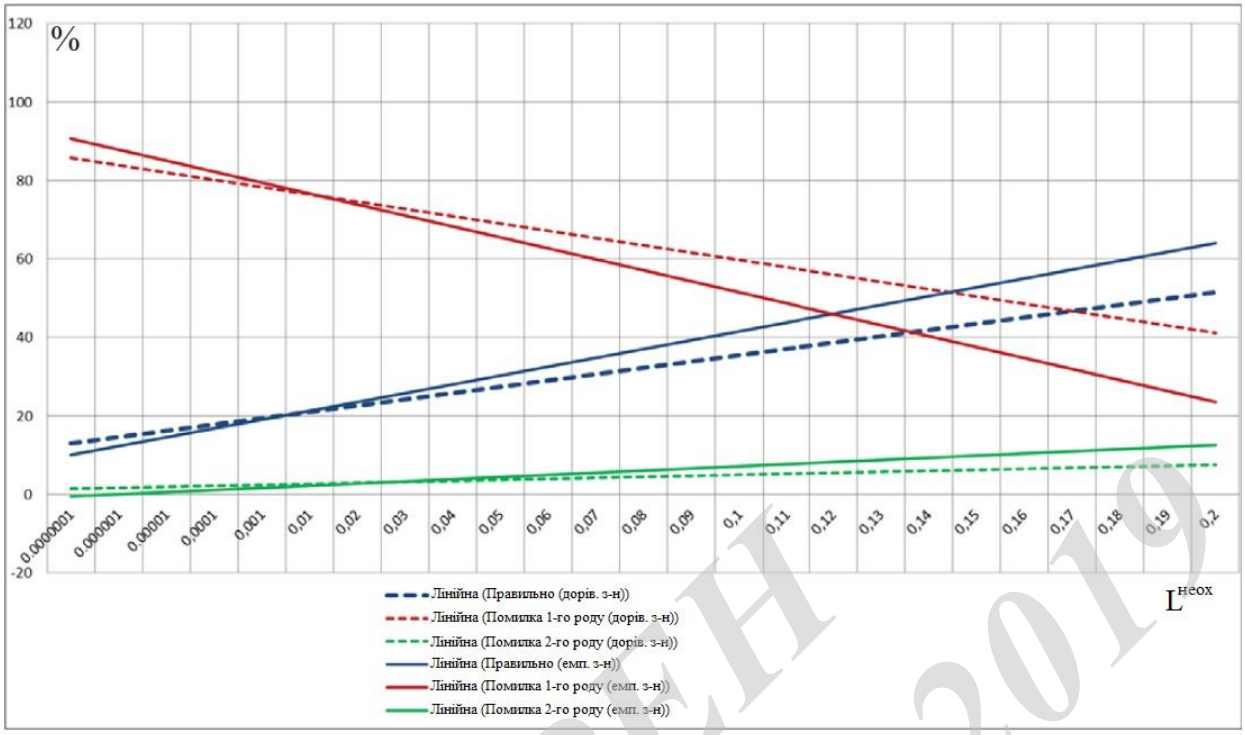


Рисунок 1.15 - Графік залежності помилок 1-го і 2-го роду від порога прийняття рішення при використанні методу Монте-Карло для прийняття рішення про рівень захищеності приміщення на основі обчисленого методом k -найближчих сусідів місцерозташування МАП

Результати аналогічного експерименту для методу на основі баєвського підходу представлені в табл. 1.16 і на рис. 1.16. Параметри помилок 1-го і 2-го роду, а також число правильних рішень для баєвського підходу вище в разі застосування емпіричного закону розподілу в порівнянні з рівномірним для будь-яких значень порога $L^{\text{неох}}$.

Таблиця 1.16 - Дослідження ефективності методу Монте-Карло при класифікації місцерозташування МАП на основі баєвського підходу в залежності від порога прийняття рішення.

$L_{\text{необх}}$	Рівномірний закон			Емпіричний закон		
	Правильно	α	β	Правильно	α	β
0,0000001	16,48	82,816	0,702	18,176	80,204	1,619
0,000001	20,651	77,191	2,157	15,986	82,816	1,193
0,00001	18,417	80,175	1,406	22,115	75,658	2,226
0,0001	17,734	81,273	0,991	2,114	97,84	0,044
0,001	18,977	78,69	2,331	14,096	85,185	0,717
0,01	18,442	80,502	1,055	22,554	75,625	1,82

0,02	17,287	82,143	0,568	26,496	70,312	3,191
0,03	21,488	74,751	3,76	31,977	66,301	1,72
0,04	19,575	78,751	1,672	37,745	58,432	3,822
0,05	20,456	77,467	2,076	42,744	55,38	1,875
0,06	25,507	73,186	1,306	39,596	49,931	10,471
0,07	24,708	71,321	3,97	43,642	51,51	4,847
0,08	29,497	65,462	5,04	45,64	46,598	7,761
0,09	30,932	63,643	5,424	30,277	69,7	0,021
0,1	33,246	64,057	2,695	50,416	39,296	10,287
0,11	30,969	62,654	6,675	57,181	37,895	4,922
0,12	38,832	58,575	2,592	60,205	34,882	4,912
0,13	39,443	55,39	5,166	58,332	36,459	5,207
0,14	45,148	49,996	4,854	58,406	32,301	9,292
0,15	45,97	50,963	3,065	61,099	32,334	6,565
0,16	42,331	46,754	10,913	64,88	27,814	7,304
0,17	47,385	43,209	9,404	62,225	28,026	9,748
0,18	49,548	42,119	8,331	61,861	26,107	12,031
0,19	54,951	39,32	5,728	68,815	25,945	5,238
0,2	60,579	34,567	4,852	67,104	25,201	7,693

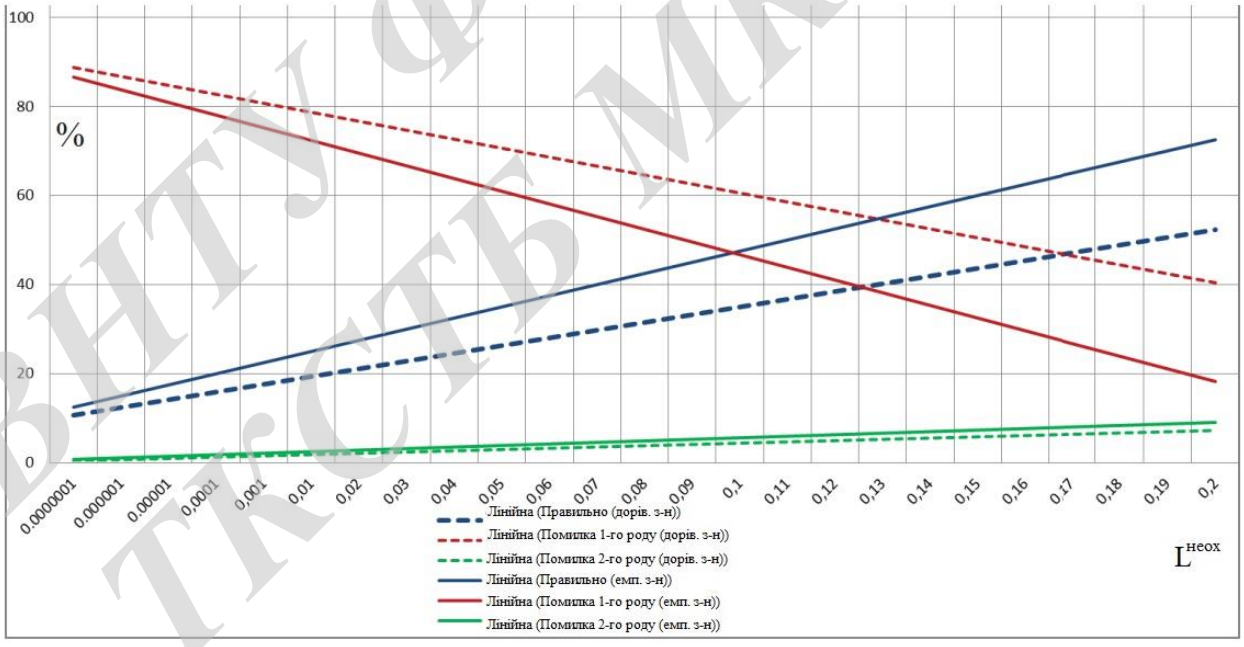
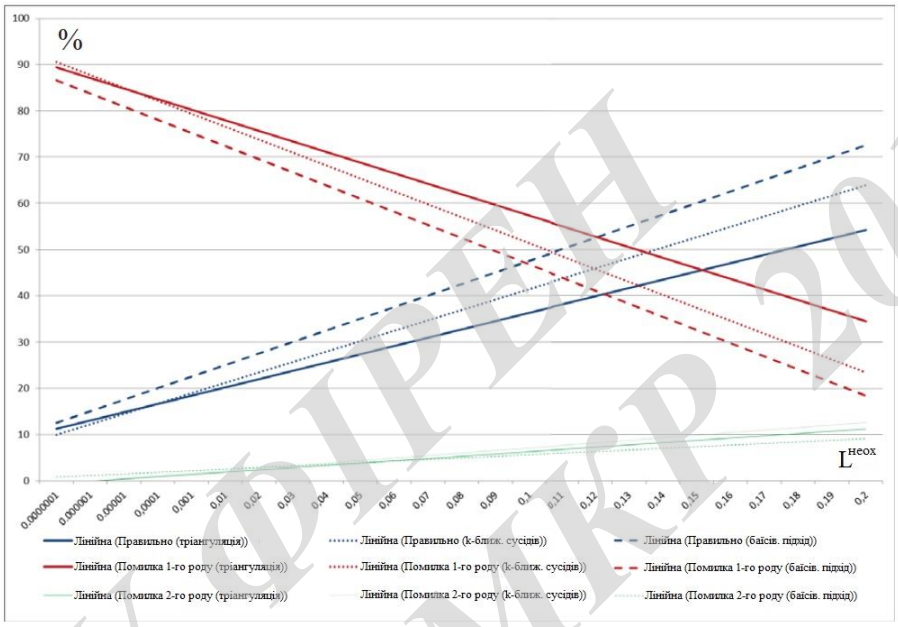


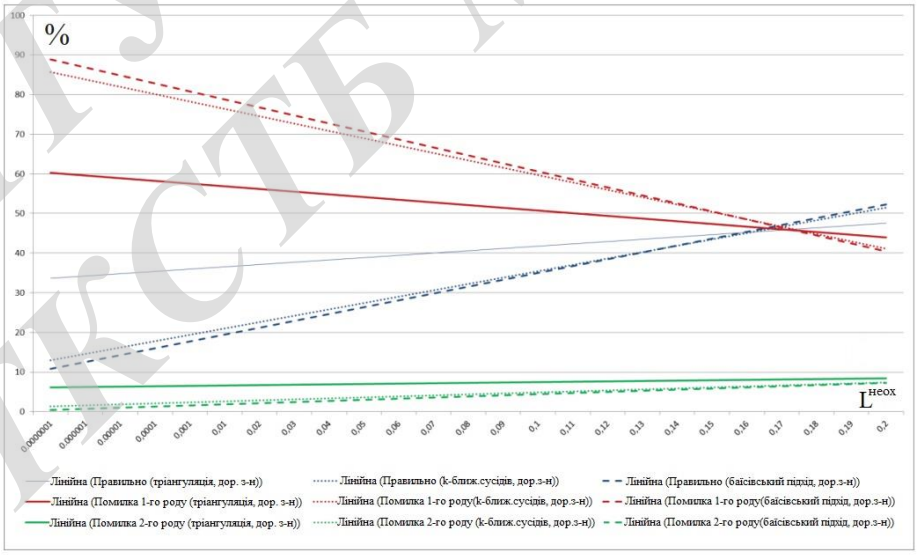
Рисунок 1.16 - Графік залежності помилок 1-го і 2-го роду від порога прийняття рішення при використанні методу Монте-Карло для визначення рівня захищеності приміщення на основі баєвського підходу

Порівняльний аналіз різних технологій визначення місця розташування в поєднанні із застосуванням методу Монте-Карло для визначення ймовірності знаходження МАП в спеціальному приміщенні наведено на рис. 1.17.

На рисунках чітко видно, що кількість правильних рішень про рівень захищеності приміщення в разі застосування емпіричного закону вище, ніж для рівномірного, незалежно від використовуваної технології визначенні місця розташування. Те ж саме стосується і помилок 2-го роду,поазники по яким нижчі для емпіричного закону.



а)



б)

Рисунок 1.17 -Порівняльний аналіз використання різних технологій визначення місця розташування в поєднанні із застосуванням методу Монте-Карло:
а) для закону емпіричного розподілу;
б) для рівномірного закону розподілу.

1.4 Висновки по першому розділу

1. Розроблена формальна модель безпеки МАП дозволяє врахувати ряд атрибутів доступу, включаючи місце розташування МАП, для формування керуючі команди на зміну конфігурації МАП з метою переведення його в захищений стан, що задовольняє вимоги безпеки інформації та якості послуг, що надаються.

2. Обґрунтовано коректність даної моделі на основі доказів відсутності заборонених інформаційних потоків від об'єктів з високим рівнем конфіденційності до об'єктів з низьким рівнем конфіденційності.

3. Показано, що застосування розробленої формальної моделі безпеки МАП дозволяє обмежити потенційно небезпечні доступи в системі, тим самим забезпечивши виконання закладених в політику безпеки вимог,підвищити адекватність ЗЗІ, побудованої на основі даної формальної моделі безпеки МАП, умов її експлуатації в КС.

4. Розроблено модель системи визначення місця розташування МАП, що дозволяє оцінити ймовірність його місцезнаходження в спеціальному приміщенні з підвищеними вимогами по захищеності.

5. Обґрунтовано використання БМПД, що дозволяє одночасно здійснювати як вимір рівня сигналу МАП точками доступу, так і захищену інформаційну взаємодію між МАП і ЗКМ, знижуючи тим самим через витрати при проектуванні і супроводі в порівнянні з системами визначення місця розташування на основі датчиків і інших технологій.

6. Обґрунтовані алгоритмічні можливості розв'язання запропонованого підходу по обчисленню ймовірності знаходження МАП в спеціальному приміщенні. Показано, що для підвищення достовірності визначення місця розташування МАП доцільно використовувати емпіричні дані про статистику помилки визначення місця розташування, а граничне значення критерію прийняття рішення про рівень захищеності приміщення, в якому знаходиться МАП, необхідно вибирати виходячи з вимог замовника і допустимих значень помилки 2-го роду.

7. Апробація моделі системи визначення місця розташування здійснена за допомогою імітаційного моделювання. Проведена всебічна оцінка її якості, що включає в себе перевірку адекватності, чутливості і стійкості, отримані оцінки параметрів приватних моделей, що впливають на достовірність визначення місця розташування МАП.

2 АЛГОРИТМ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНОГО АБОНЕНТСЬКОГО ПРИСТРОЮ, ЩО ДОЗВОЛЯЄ ВИЗНАЧИТИ ОПТИМАЛЬНУ ПРОГРАМНО-АПАРАТНУ КОНФІГУРАЦІЮ ПРИСТРОЮ З УРАХУВАННЯМ АТРИБУТІВ ДОСТУПУ І ВИМОГ БЕЗПЕКИ І ЯКОСТІ ПОСЛУГ

Даний розділ присвячений розробці алгоритму управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності [37]. Алгоритм побудований на основі розробленої формальної моделі безпеки МАП і входить до її складу моделі системи визначення місця розташування, що дозволяє оцінити ймовірність місцезнаходження МАП в спеціальному приміщені з підвищеними вимогами по захищеності. Крім того, в алгоритмі реалізовані процедури, що дозволяють враховувати особливості сигнально-перешкодої обстановки в бездротових мережах передачі даних і вимоги щодо якості надання послуг.

До складу даного алгоритму входять:

1) комплекс алгоритмів визначення місця розташування МАП, а також алго-ритми навчання підсистем визначення місця розташування на базі методів трилатерації, *k* -найближчих сусідів і баєвського підходу;

2) алгоритм визначення ймовірності місцезнаходження МАП в спеціальному приміщенні ЗКМ;

3) алгоритм розрахунку оцінки інформаційної швидкості в каналі БМПД;

4) алгоритм управління програмно-апаратною конфігурацією МАП.

В розділі представлено опис циклу управління станом МАП, визначені рівняння стану і спостереження, мета управління, представлені основні критерії, на підставі яких здійснюється вибір оптимальної конфігурації МАП. Представлено доказ основних властивостей алгоритму.

2.1 Постановка завдання на розробку алгоритму управління безпеку мобільного абонентського пристрою

Основне завдання алгоритму управління безпекою МАП - управління програмно-апаратною конфігурацією МАП, що дозволяє узгодити стан МАП до вимог політики безпеки ЗКМ, обумовленими, в тому числі, умовами, в яких перебуває МАП, а також нормативними вимогами щодо якості послуг, що надаються. Для зміни стану МАП з керуючої підсистеми в МАП передається керуюча команда, яка дозволя застосувати сформовану конфігурацію.

Схема циклу управління безпекою (програмно-апаратної конфігурації) МАП [41] представлена на рис. 2.1.

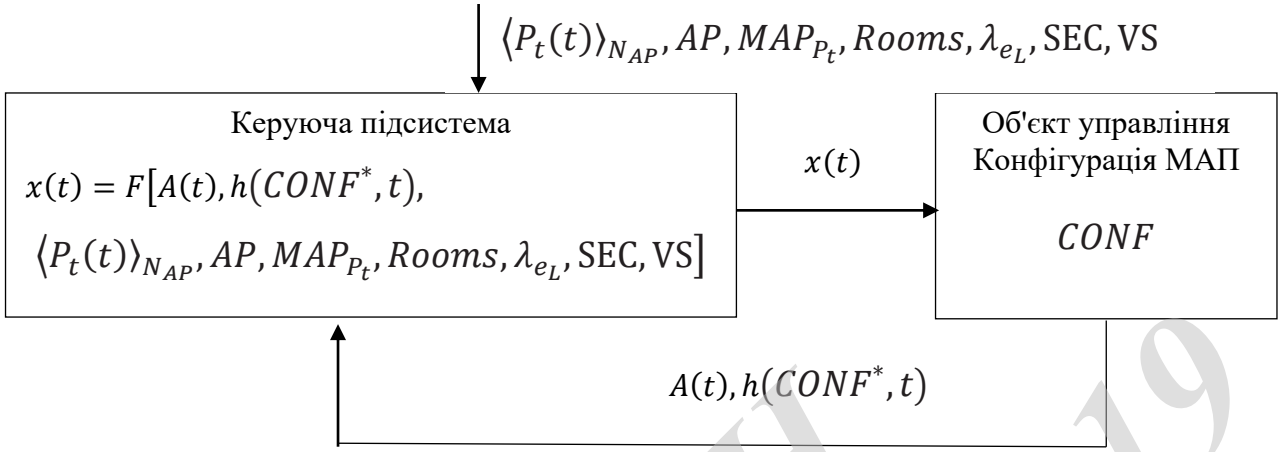


Рисунок 2.1 - Схема управління конфігурацією МАП

Стан об'єкта управління - програмно-апаратна конфігурація МАП характеризується сукупністю прав доступу до функціональних блоків (об'єктів доступу) *CONF* . Дані права реалізує, що входить до складу МАП аппаратно-програмний модуль довіреного завантаження.

В керуючу підсистему - центр управління інформаційної безпеки ЗКМ, а саме, в контролер доступу МАП надходять дані про поточні атрибути доступу $A(t)$ і поточної конфігурації МАП $h(CONF^*, t)$. Довірена БМПД передає в керуючу систему інформацію про рівень сигналу МАП в вигляді безлічі $\langle P_t(t)\rangle_{N_{AP}}$, де N_{AP} - кількість точок доступу БМПД, в зоні дії яких знаходиться

МАП. Формування керуючої команди $x(t)$ на зміну конфігурації МАП керуюча система здійснює також за рахунок обліку даних про розташування точок доступу БМПД *AP* , карти сигнального простору MAP_{P_t} (при необхідності), карти приміщень $Rooms$, статистики помилок визначення місця розташування МАП для використовуваної технології λ_{e_L} , матриці правил політики безпеки ЗКМ SEC і матриці нормативів інформаційних швидкостей для послуг МАП VS.

На основі викладеного сформовано рівняння спостереження:

$$CONF(t) = g\left[t, x(t), A(t) \times P_{L_{Room}}(t) \times h(CONF^*, t)\right], \quad (2.1)$$

де $P_{L_{Room}}(t)$- ймовірність знаходження МАП в спеціальному приміщенні ЗКМ.

Рівняння стану для процесу управління конфігурацією МАП при цьому може бути представлено у вигляді

$$CONF(t) = f\left[CONF(t_0), x(\tau) \in [t_0, t]\right], \quad (2.2)$$

де $CONF(t_0)$ -початковий (базовий) стан МАП при його включенні; $x(\tau)$ - керуюча команда в момент часу τ для перекладу МАП в черговий стан

Метою управління конфігурацією МАП є досягнення максимальної результативності захисту інформації при його експлуатації в корпоративних мережах з різними вимогами по захищеності, при цьому результативність може бути оцінена ймовірністю забезпечення безпеки інформації. Тоді мета управління формально може бути визначена як

$$max[P_{\text{БІ}}(T)] = P_{\text{КІ}}(T) \cdot P_{\text{ДІ}}(T) \cdot P_{\text{ЦІ}} | P_{\text{ЦІ}} = 1 \quad (2.3)$$

Завдання на розробку алгоритму відноситься до класу оптимізаційних і формально може бути представлене у вигляді:

$$\begin{cases} f(S^*) \to max, \\ \sum_{i=1}^{f(S^*)} V_{lm}^{i} \le \hat{V}_{lm}, \\ S^* = F_S(CONF^*) | CONF^* \in CONF^{\text{доп}}, S^* \subseteq S, \end{cases} \quad 2.4)$$

де S - безліч, що подаються за допомогою МАП послуг; $f(S^*)$- цільова функція, що максимізує кількість наданих користувачеві МАП послуг при заданих умовах; $V_{lm}^{S_i^*}$ - норматив інформаційної швидкості для i -ї послуги S_i^* в бездротовому радіоканалі між l -м МАП і m -й точної доступу; $\hat{V}_{lm}$ - оцінна максимально можлива інформаційна швидкість в бездротовому радіоканалі між l -м МАП і m -й точної доступу; $CONF^*$ - нова конфігурація МАП; $CONF^{\text{доп}}$ - безліч допустимих конфігурацій МАП при поточних атрибутах доступу і місцезнаходження МАП; F_S - функція відображення конфігурації МАП на безліч послуг, які можуть бути надані користувачеві МАП при даній конфігурації.

Аналіз формальної постановки задачі (2.4) відповідно [38] дозволяє класифікувати оптимізаційну задачу як *багато критеріальну оптимізацію цілого чисельного динамічного програмування* .

Для вибору оптимальної конфігурації МАП в якості критеріїв оцінювання оптимальності використовуються: матриця правил політики безпеки і нормативи інформаційної швидкості для наданих користувачеві МАП послуг.

Матриця правил політики безпеки може бути представлена як

$$SEC = \begin{vmatrix} CONF_0 & a_{00} & \cdots & a_{0N_A} & L_0 \\ CONF_1 & a_{10} & \cdots & a_{1N_A} & L_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ CONF_{N_{CONF}} & a_{N_{CONF}0} & \cdots & a_{N_{CONF}N_A} & L_{N_{CONF}} \end{vmatrix}, \quad (2.5)$$

де $CONF_i, i = \overline{1, N_{CONF}}$ - конфігурації МАП; $a_{i0}, .., a_{ij}, .., a_{iN_A}$ - значення N_A атрибутів доступу для i -й конфігурації МАП; L_i - місце розташування МАП для яких допустимо призначення i -й конфігурації МАП.

Матриця нормативів інформаційної швидкості для наданих користувачеві МАП послуг може бути представлена як $VS = |vs_i|, i = \overline{1, |S|}$, де S - безліч послуг; vs_i - норма інформаційної швидкості для i -ї послуги.

Вирішальне правило F_{RECONF} для вибору безлічі допустимих конфігурацій МАП на основі матриці правил політики безпеки, безлічі значень поточних атрибутів доступу A_i і отриманої оцінки місця розташування МАП $\tilde{L}_{Room}$ може бути представлено у вигляді:

$$CONF^{\text{доп}} = F_{RECONF}\ (\tilde{L}_{Room}, A_i) | \tilde{L}_{Room} = L_{Room}^{\text{необх}} : \\ : \left(\forall CONF_i \in CONF^{\text{доп}} \exists L_{Room}^{\text{необх}} = F_{L_{Room}}(CONF_i)\right) \wedge \quad (2.6)$$
$$\wedge \left(\forall a_i \in A_i\ \exists a_i^{\text{необх}} \in A_i^{\text{необх}} = F_A(CONF_i) : a_i = a_i^{\text{необх}}\right).$$

Результатом роботи системи управління МАП є сукупність $CONF(t) = \{M, f_t, P_t\}$` , що представляє собою призначену МАП конфігурацію, інформація про яку передається керуючій команді. Приклад дозволених конфігурацій представлений в табл. 2.1.

Таблиця 2.1 - Приклад таблиці правил політики безпеки, що визначає конфігурації МАП і вимоги до них

Конфігурація МАП	Рівень захищеності приміщення, треб *Room L*	Атрибути доступу (треб *i a*)			
		Час	*ID* МАП	*User ID*	…
$CONF_0$	$L_O\ L_{К1} L_{К2}$	∞	∞	∞	…
$CONF_1$	L_O	∞	5, 29, 53, …	3, 7, 12,…	…
$CONF_2$	L_O	8:00-17:30	7, 11, 52, …	3, 17, 23,…	…
$CONF_3$	$L_{К1}$	∞	13, 17, …	5, 11, …	…
$CONF_4$	$L_{К1}$	16:00-17:00	17	5	…
$CONF_5$	$L_{К2}$	∞	13	1	…
$CONF_6$	$L_{К2}$	11:00-13:00	17, 21	1, 27	…

Склад даної таблиці розробляється на етапі проектування системи управління доступом, а зміст визначається політикою безпеки ЗКМ і задається адміністратором безпеки.Узагальнена блок-схема розробленого алгоритму управління безпеки [41] представлена на рис. 2.2.

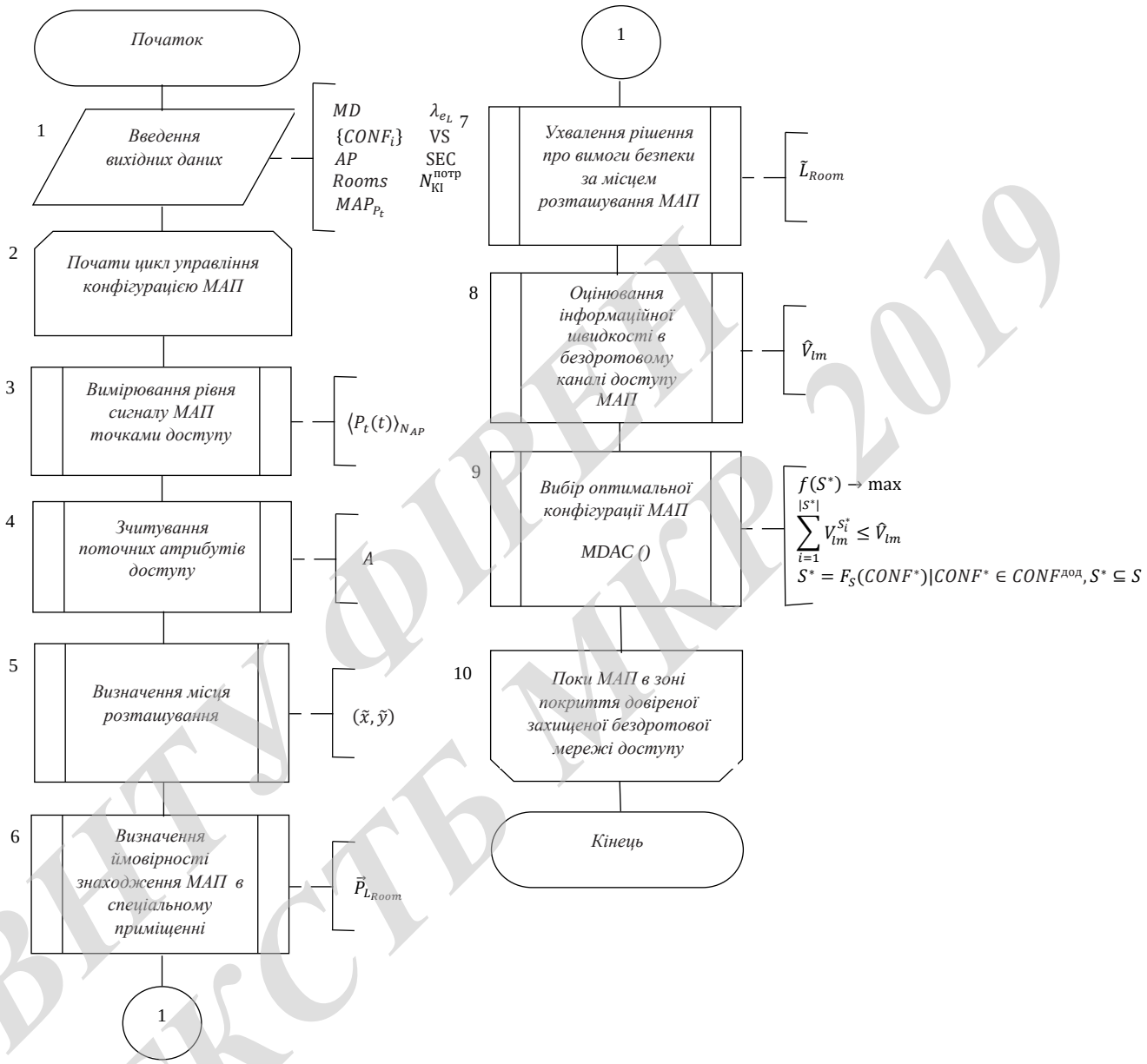


Рисунок 2.2 - Узагальнена блок-схема алгоритму управління безпекою МАП

На першому кроці алгоритму в блоці 1 здійснюється ініціалізація вихідних даних:

– введення технічних характеристик приймально-передавальних пристроїв;

– введення параметрів приміщень;

– введення координат точок доступу бездротової мережі і карти сигнального простору;

– введення параметрів алгоритмів визначення місця розташування МАП;

– введення параметрів політики безпеки МАП в ЗКМ, нормативів інформационного швидкості.

У блоці 1 здійснюється ініціалізація вихідних даних.

Блоки 2-10 реалізують цикл управління МАП.

У блоці 3 реалізується вимірювання рівня сигналу МАП точками доступу БМПД і передача значень в керуючу підсистему.

У блоці 4 здійснюється зчитування поточних атрибутів доступу.

У блоці 5 здійснюється розрахунок місця розташування МАП.

У блоці 6 обчислюється ймовірність знаходження МАП в спеціальному приміщенні за допомогою чисельного методу обчислення площі на основі методу Монте-Карло.

У блоці 7 здійснюється прийняття рішення про вимоги безпеки за місцем розташування МАП.

У блоці 8 проводиться оцінювання інформаційної швидкості в бездротводному каналі доступу МАП на основі поточної сигнально-перешкодної обстановки.

У блоці 9 здійснюється вибір оптимальної конфігурації МАП на основі заданих в ЗКМ правил політики безпеки МАП і з урахуванням поточних атрібутів доступу.

Блок № 5 реалізує алгоритм визначення місця розташування МАП на території будівлі, в якому передбачена експлуатація корпоративних мереж з різними вимогами щодо захищеності. У даній роботі використані відомі алгоритми. На їх програмну реалізацію отримано свідоцтво [39].

В роботі досліджувалася ефективність управління безпекою МАП стосовно трьом відомим алгоритмам визначення місця розташування, в склад яких входять:

1. Алгоритм визначення розташування на основі методу трилатерації, представлений на рис. В.4. Математичні вирази для розрахунку координат місця розташування МАП даним методом представлені виразами (А.3) - (А.18). Відмінною особливістю даного алгоритму є відсутність необхідності попередніх вимірювань рівнів потужності сигналу і складанні карти сигнального простору. Однак алгоритм на основі методу Трилатерації менш точний в порівнянні з алгоритмами на основі методу k -найближчих сусідів і

баєвського підходу, що вимагають навчання і складання карти сигнального простору.

2. Алгоритм визначення розташування на основі методу *k* -найближчих сусідів, представлений на рис. В.5. Алгоритм навчання класифікатора на основі методу *k* -найближчих сусідів зображений на рис. В.11. Математичні вирази для обчислення координат місця розташування МАП методом *k* - найближчих сусідів представлені виразами (А.20) - (А.25).

3. Алгоритм визначення розташування на основі баєвського класифікатора (прихованих марковських моделей), представлений на рис. В.6, Б.7. Алгоритм навчання баєвського класифікатора зображений на рис. В.10. Математичні вирази для розрахунку координат місця розташування МАП на основі баєвського підходу представлені виразами (А.26) - (А.31).

Методи *k* -найближчих сусідів і баєвського підходу для визначення місця розташування МАП в приміщеннях є більш точними в порівнянні з методом трилатерації однак для їх реалізації необхідно навчання підсистеми визначення місця розташування - складання карти вимірів. У ряді випадків таке навчання неможливо, тому в якості альтернативи даним методам можна використовувати менш точний метод трилатерації.

2.2 Алгоритм визначення ймовірності місцезнаходження мобільного абонентського пристрою в спеціальному приміщенні

На основі обчисленого розташування МАП можна визначити приміщення, в якому ймовірно перебуває даний пристрій. Рівень захищеності приміщення, атрибути доступу і встановлена в ЗКМ політика безпеки в сукупності визначають вимоги безпеки до МАП, які можуть бути представлені у вигляді пакету, профілю захисту або завдання з безпеки [20]. Приклад варіанту формалізованих вимог безпеки до МАП в ЗКМ представлений в табл. 2.1.

На рис. В.8, В.9 представлений алгоритм визначення ймовірності місця розташування МАП в спеціальному приміщенні на основі методу Монте-Карло.

У блоці 1 алгоритму здійснюється введення вихідних даних:

– отримані емпіричним шляхом дані про вибіркові середні помилки визначення місця розташування для використовуваного алгоритму визначення місця розташування і вибірково середньоквадратичне відхилення помилки визначення місця розташування;

– параметр, що визначає число "сигма", що враховується при обчисленні радіуса зони помилки визначення місця розташування;

– кількість випробувань для реалізації методу Монте-Карло;

– обчислене місце розташування користувача МАП;

– гістограма частот щільності ймовірності розподілу помилки визначення розташування;

– параметри приміщень, що включають в себе їх координати і рівні захищеності.

У блоці 2 здійснюється ініціалізація початкових значень для:

– радіусу зони, яка визначає ймовірне місце розташування користувача МАП;

– початкові значення вектора ймовірностей, що визначає ймовірності віднесення до того чи іншого рівня захищеності обчисленого місця розташування МАП.

У блоці 3 реалізований ітератор циклу обчислень випробувань у відповідності з методом Монте-Карло.

У блоці 4 здійснюється вибір закону розподілу ймовірностей випадкової величини процесу, використовуваного в методі Монте-Карло.

У блоці 5 задається значення радіуса зони, яка визначає ймовірне місцерозташування МАП, для рівномірного закону розподілу ймовірностей випадкової величини процесу, використовуваного в методі Монте-Карло.

У блоках 6-10 реалізовано моделювання випадкового процесу в відповідність до закону розподілу ймовірностей помилки обчислення місця розташування, що визначаються гистограммой частот і емпіричними даними. В процесі моделювання обчислюється значення радіуса зони, яка визначає ймовірне місце розташування МАП, для емпіричного закону розподілу ймовірностей випадкової величини процесу, використовуваного в методі Монте-Карло.

У блоці 11 за рахунок використання генератора випадкових чисел з рівномірним розподілом ймовірностей генерується точка з координатами всередині кола з обчисленим в блоках 4-10 радіусом.

В блоках 12-14 здійснюється пошук приміщення, в якому знаходиться згенерована точка з випадковими координатами, а також підрахунок кількості точок , які потрапили в приміщення різних рівнів захищеності. Попадання точки в приміщення з рівнем "ОІ" збільшує рівень лічильника "ОІ" на одиницю. Аналогічно відбувається і для інших рівнів захищеності.

У блоках 15-19 здійснюється розрахунок ймовірності знаходження МАП в приміщеннях з різними рівнями захищеності, виконуваного на основі метода Монте-Карло і заданого порогу прийняття рішення

У.блоці 20 на основі обчисленої оцінки місця розташування МАП і поточних атрибутів доступу здійснюється вибірка з бази даних сукупності вимог безпеки, що пред'являються до МАП.

Математичні вирази для розрахунку ймовірності знаходження МАП в спеціальному приміщенні і прийняття рішення про рівень захищеності приміщення, в якому ймовірно перебуває МАП представлені виразами (1.2) - (1.9).

2.3 Алгоритм оцінювання інформаційної швидкості в бездротовому каналі доступу з OFDM модуляцією, що враховує сигнальну обстановку з перешкодами

Використання технології бездротового з'єднання доступу для МАП характеризується досить складною сигнально-перешкодною обстановкою. В першу чергу через те, що пристрої використовуються в приміщеннях всередині будівлі, внаслідок чого серйозно впливає багатопроменеве поширення сигналу і поява швидких завмирань, а також значна кількість перевідображень, поглинання сигналу, що проходить через конструкції будівлі.

Виходячи з цього, для формування оптимальної конфігурації МАП, яка дозволяє надати користувачеві послуги необхідної якості, виникає потреба враховувати реальну інформаційну швидкість в бездротовому каналі доступу з урахуванням сигнально-перешкодної обстановки.

Класичний метод оцінки інформаційної швидкості передбачає, що прийом сигналу здійснюється на тлі білого шуму. В реальності ж, як показано в [13], в умовах приміщень, а також інших МАП і базових станцій в мережі виникають додаткові внутрісистемні перешкоди, які необхідно враховувати. Існують підходи, що дозволяють отримати оцінку інформаційної швидкості з використанням індексу модуляції і схеми кодування [12], а також на основі формули Шеннона для каналу з адитивним білим гауссовським шумом [39]. В роботі [33] проведено аналіз даних і зроблено висновок, що вони дають досить завищені значення. В [40] запропонована методика, заснована на формулі Шеннона, але дозволяє враховувати сигнально-перешкодну обстановку в каналі

з OFDM модуляцією з багатопроменевим поширенням і між символьною інтерференцією.

В основі методики, в запропонованій роботі [40], лежить оцінка інформаційної швидкості V_{lm} від l -го МАП до m -й базової станції на основі формули Шеннона:

$$V_{lm} \approx k_\lambda \cdot \frac{v_c}{2} \cdot \sum_{r=1}^{I^u} log_2(\gamma_{lm}^{sr} + 1), \tag{2.7}$$

де k_λ- коефіцієнт, що враховує частку інформаційної складової швидкості передачі в пропускній здатності каналу зв'язку; v_c - кількість OFDM символів в секунду; I^u - кількість тих підносійних в радіоканалі; γ_{lm}^{sr} - відношення сигнал/завада для r –і підносійний.

Факторами, що впливають на помилки при прийомі окремого OFDM символу, крім шуму вимірювання, є багатопроменеве поширення сигналу, а також присутність сигналів сусідніх кодових символів, пов'язане з асинхронністю роботи різних передавальних пристроїв при демодуляції. Виходячи з цього, сигнал на вході демодулятора може бути представлений у вигляді:

$$Z_{lm}^k(t) = \sum_{i=1}^{I^u} \sum_{m'=1}^{M} \sum_{q=1}^{Q} Re\left\{A_{glm} \cdot \left[\dot{x}_{ik}^{m'} \cdot exp\left(j\omega_{im'}\left(t - t_{gk}^{lm'}\right)\right) \cdot \right.\right.$$

$$\cdot v\left(t - t_{gk}^{lm'}, -T_p, T_D\right) + \dot{x}_{i(k+1)}^{m'} \cdot exp\left(j\omega_{im'}\left(t - t_{g(k+1)}^{lm'}\right)\right) \cdot \tag{2.8}$$

$$\left.\left. \cdot v\left(t - t_{g(k+1)}^{lm'}, -T_p, T_D\right)\right]\right\} \cdot v\left(t - \hat{t}_k^{lm}, 0, T_D\right) + n(t)\ ,$$

де M - кількість передавальних пристроїв; Q - кількість врахованих променів; A_{glm}- амплітуда q -го променя від m' -го передавального пристрою до l -му приймаючому; $\dot{x}_{ik}^{m'}$- модулювання k -й OFDM символ на i -й піднесе від m' -го передатчика; $\hat{t}_k^{lm}$- час приходу q -го променя, k -го кодового символу m' -го передатчика до l -му приймача; T_p- тривалість циклічного префікса; T_D - тривалість OFDM символу; $\hat{t}_k^{lm}$ - обраний час прийому k -го кодового символу m- передадчика.

$v(t, T_-, T_+) = \begin{cases} 1, -T_- \le T_+ \\ 0, (t < -T_-) \cup (t > -T_+) \end{cases}$-прямокутний імпульс: $n(t)$-перешкода.

В роботі [40] зроблено припущення, що для оцінювання статистичних параметрів перешкод, що входять у вираз (2.8), досить визначити математичне

сподівання і дисперсію, оскільки стандартні алгоритми прийому розрахованані на гауссовський розподіл перешкод. При цьому показано, що, прийнявши розподіл символів $\dot{x}_{ik}^{m'}$ рівномірним, математичне очікування перешкоди дорівнюватиме нулю. Дисперсія перешкоди, з урахуванням того, що розподіл ймовірностей моменту надходження сигналу $P(\Delta t_k^l)$ прийнято рівномірним, всіма передавачами використовуються однакові підносійні, їх кількість однакова, вид модуляції і середня що передається потужність постійна, може бути визначена як $\dot{y}_{rl}^{kE}$

$$\sigma_{\dot{y}_{rl}^{kE}}^2 = \frac{1}{\pi^2 \cdot (I-1)} \cdot \sum_{\substack{m'=1 \\ m \neq m}}^{M} A_{lm'}^2 \cdot \sum_{i=N_{m'rm}+1}^{I^u+N_{m'rm}} \frac{1}{i^2} \cdot \cdot \sum_{\Delta t_k^l=1}^{I-1} \left\{ \sin^2\left(\frac{\pi \cdot i \cdot (I-\Delta t_k^l)}{I}\right) + \sin^2\left(\frac{\pi \cdot i \cdot \Delta t_k^l}{I}\right) \right\}, \quad (2.9)$$

де $A_{lm'}^2$ - середня потужність, яка надходить від передавача з номером m' на вхід приймача *l* по всім променям.

Аналіз цього виразу показує, що дисперсія перешкод визначається потужностями сигналів перешкод $A_{lm'}^2$ і деяким коефіцієнтом, що враховує *lm*ступінь впливу перешкоди, що залежить від частотного розносу піднесе, на якій йде передача і каналів перешкод. Позначивши даний коефіцієнт через $K(f)$, дисперсія перешкод може бути представлена як:

$$\sigma_{\dot{y}_{rl}^{kE}}^2 = \sum_{\substack{m'=1 \\ m' \neq m}}^{M} A_{lm'}^2 \cdot K(f_{m'} - f_{rm}), \quad (2.10)$$

де $A_{lm'}^2$ - середня потужність сигналу від m'-го передавального пристрою до *l* -му $f_{m'}$приймає; f_{rm}- частота передавача перешкоди; f_{rm} - частота піднесе, на якій здійснюється передача; $K(f)$ - функція, що враховує вплив перешкод і розраховується за формулою:

$$K(f) = \sum_{i=f \cdot T_D+1}^{f \cdot T_D+1^u} \begin{cases} \frac{(2 \cdot I - 1)}{3 \cdot I}, \text{при } i = 0, \\ \frac{1}{\pi^{2 \cdot}(I-1) \cdot i^2} \cdot \sum_{\Delta t_k^l=1}^{I-1} \left(1 - \cos\left(\frac{2 \cdot \pi \cdot i \cdot \Delta t_k^l}{I}\right)\right), \end{cases} \quad (2.11)$$

при $i \neq 0$,

де I - загальна кількість тих підносійних, використовуваних в OFDM сигналі; Δt_k^l - можлива затримка передачі OFDM символу із моменту його прийняття.

На основі представлених виразів відношення сигнал / перешкода на вході канального демодулятора буде виглядати як

$$\gamma_{lm}^{s\gamma} = \frac{\bar{A}_{lm'}^{r\,2}}{\sum_{\substack{m'=1 \\ m' \neq m}}^{M} \bar{A}_{lm'}^2 \cdot K(f_{m'} - f_{rm}) + \sigma_n^2}. \qquad (2.12)$$

Додатково необхідно врахувати відміну потужності корисного сигналу від середньої потужності, викликане багатопроменевим поширення. Для цього вводиться деякий коефіцієнт запасу Г по відношенню до рівня сигнал / перешкода [11]:

$$\gamma_{lm}^{s\gamma} \approx \frac{\gamma_{lm}^{r}}{\Gamma} \qquad (2.13)$$

З огляду на, що, як правило, $\gamma_{lm}^{s\gamma} \gg 1$, шукану оцінку інформаційної СКВ-рости можна записати у вигляді:

$$\hat{V}_{lm} \approx k_\lambda \cdot \frac{v_c}{2} \sum_{r=1}^{I^u} log_2\left(\gamma_{lm}^{s\gamma} + 1\right) - k_\lambda \cdot \frac{v_c}{2} \cdot I^u \cdot log_2(\Gamma), \qquad (2.14)$$

Значення k_λ і *для мережі з відомими параметрами і розгорнутими в конкретних умовах можна вважатиПОстійними і оцінити їх за допомогою критерия мінімуму СКВ на основі результатів проведених емпіричних тестів:

$$k_\lambda = \frac{L \cdot \sum_{l=1}^{L} V_{lm} V_{lm_{real}} - \sum_{l=1}^{L} V_{lm} \cdot \sum_{l=1}^{L} V_{lm_{real}}}{L \cdot \sum_{l=1}^{L} V_{lm}^2 - \left(\sum_{l=1}^{L} V_{lm}\right)}, \qquad (2.15)$$

$$\Gamma = 2^{-2\frac{\sum_{l=1}^{L} V_{lm_{real}} - k_\lambda \cdot \sum_{l=1}^{L} V_{lm}}{|k_\lambda \cdot v_c}}. \qquad (2.16)$$

Таким чином, підсумкова, що розраховується в алгоритмі оцінка інформційної швидкості передачі, може бути отримана на основі відомих технічних характеристик БМПД, результатів проведених емпіричних тестів і вимірювання параметрів k_λ і * в бездротовому радіоканалі, що розраховуються за допомогою виразів (2.15) і (2.16), і аналітичних виразів (2.11) - (2.14).

2.4 Алгоритм управління програмно-апаратною конфігурацією МАП

Реалізація алгоритму управління програмно-апаратною конфігурацією МАП грунтується на застосуванні правил політики безпеки, що визначаються місцем розташування пристрою і атрибутами доступу, і критеріями якості послуг користувачеві МАП в ЗКМ послуг. Варіант реалізації даного алгоритму описаний в роботах [41]. Для формування конфігурації МАП необхідно вирішити багатокритерну оптимізаційну задачу.

Вимоги безпеки визначають функціональні вимоги до МАП і його користувачеві, а також гарантії, які технічно реалізуються у вигляді сукупності прав доступу користувача, що визначає дозволені користувачеві доступи (операції) і конфігурацію МАП, визначальну дозволені функціональні можливості МАП при поточних умовах доступу. Крім вимог безпеки ще одним критерієм вибору конфігурації МАП являються нормативи інформаційної швидкості в радіоканалі, що дозволяють забезпечити мобільному користувачеві необхідний рівень якості послуг зв'язку на основі отриманої оцінки інформаційної швидкості, яка враховує сигнально-перешкодну обстановку.

Реалізація алгоритму управління програмно-апаратною оптимальною конфігурацією МАП представлена на рис. 2.3.

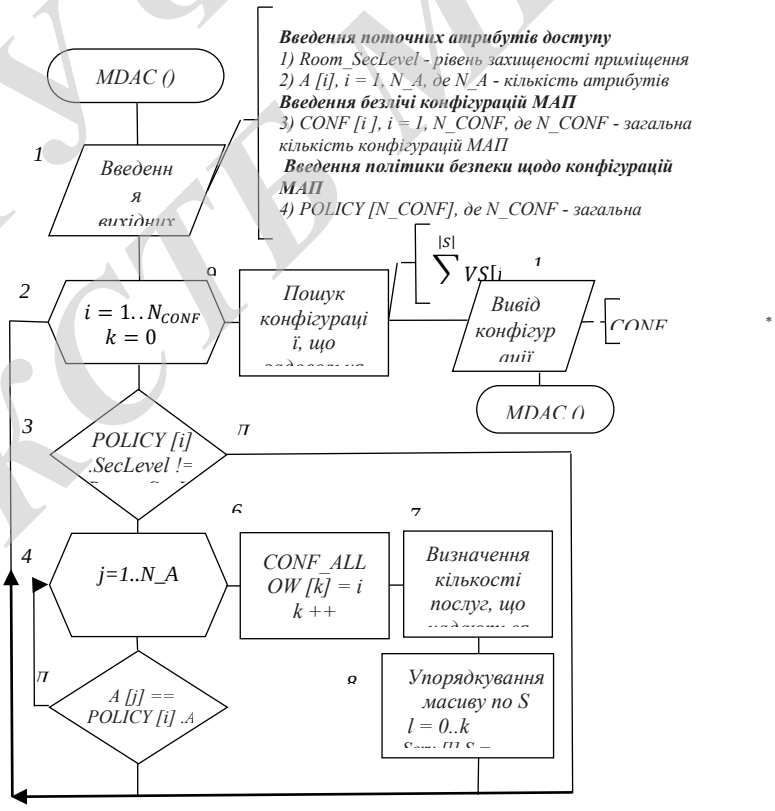


Рисунок 2.3 – Блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП

У блоці 1 даного алгоритму здійснюється введення вихідних даних:

– рівень захищеності приміщення, в якому знаходиться користувачМАП;

– вектор атрибутів доступу користувача МАП;

– безліч можливих конфігурацій МАП і політика безпеки щодо конфігурацій МАП;

– безліч можливих прав доступу користувача МАП;

– матриця нормативів інформаційних швидкостей що подаються МАП послуг;

– оцінка інформаційної швидкості в радіоканалі МАП.

У блоках 2-6 здійснюється вибірка допустимих конфігурацій МАП, відповідних до поточних умов доступу.

У блоці 7 здійснюється визначення кількості послуг, яке буде надавати МАП при заданій допустимій конфігурації.

У блоці 8 відбувається упорядкування масиву допустимих конфігурацій за кількістю наданих послуг.

У блоці 9 здійснюється пошук конфігурації з масиву допустимих, що задовольняє критерію відповідності суми необхідної інформаційної швидкості для послуг, що надаються значенням оцінки інформаційної швидкості радіоканалі МАП.

У блоці 10 здійснюється висновок оптимальної конфігурації МАП.

Рішення оптимізаційної задачі методом цілого чисельно-динамічного програмування даним алгоритмом здійснюється наступним чином:

1) Задається область значень у вигляді безлічі можливих конфігурацій МАП *CONF* і вихідні дані у вигляді безлічі атрибутів доступу A і рівня захищеності приміщення $L_{\text{МАП}}$, в якому знаходиться в даний момент МАП.

2) Задаються безлічі критеріїв у вигляді:

– політики безпеки МАП, яка визначає значення атрибутів доступу для вибору допустимих конфігурацій МАП в вигляді матриці SEC вираження (2.5);

– безліч VS нормативів інформаційних швидкостей для послуг, наданих МАП.

3) Визначається безліч допустимих конфігурацій $CONF^{\text{доп}} \subset CONF$ у відповідність з вирішальним правилом, представленим виразом (2.6).

4) Безліч $CONF^{\text{доп}}$ впорядковується у відповідність з критерієм $|S^*| \rightarrow max$, де $S^* = F_S(CONF^*) | \, CONF^* \in CONF^{\text{доп}}, \; S^* \subseteq S, S$ - безліч, що подаються за допомогою МАП послуг; $|S^*|$ - потужність безлічі S^*; F_S – функція

відображення конфігурації МАП на безліч послуг, які можуть бути надані користувачеві МАП при даній конфігурації. На даному етапі здійснюється пошук допустимої конфігурації МАП, що дозволяє надавати мобільному користувачеві максимальну кількість послуг. Даний пошук здійснюється циклічно для упорядкування масиву $CONF^{\text{доп}}$ за спаданням, у відповідність з критерієм $|S^*| \to \max$. Таким чином, що $|S_1^*| \le |S_2^*| \le \cdots \le |S_n^*|$, де

$S_1^* = F_S\,(CONF_i) \in CONF^{\text{доп}} = (CONF_1, CONF_2, \ldots, CONF_n)$ S^* o max , де в лівій частині нерівності розташована сума інформаційних швидкостей для послуг, що надаються j -й конфігурацією $CONF_j$

Таким чином, на 5-му кроці визначається оптимальна конфігурація МАП, яка задовольняє вимоги безпеки у відповідність з політикою безпеки МАП, яка визначається матрицею SEC, і вимогам якості наданих МАП послуг, які визначаються безліччю VS .

В якості чисельного прикладу розглянемо ЗКМ з політикою безпеки МАП, заданої матрицею:

$$SEC = \begin{vmatrix} CONF_0 & U & U & U & \overline{L_0 \cup L_1 \cup L_2} \\ CONF_1 & 2 & 101 & 15 & L_2 \\ CONF_2 & 3 & 102 & 18 & L_0 \\ CONF_3 & 2 & 102 & 17 & L_1 \\ CONF_2 & 2 & 102 & 17 & L_1 \\ CONF_4 & 3 & 103 & 18 & L_2 \\ CONF_2 & 3 & 101 & 16 & L_1 \\ CONF_1 & 4 & 101 & 17 & L_1 \\ CONF_3 & 3 & 103 & 16 & L_1 \\ CONF_4 & 2 & 102 & 17 & L_1 \end{vmatrix}$$

а безліч нормативів інформаційних швидкостей згідно [42] задано якVS $VS = \{vs_i\} = \{384,64,128,128,64,512,256,64,1024\}$ для $|S| = 9$, де $vs_i -$ норматив інформаційної швидкості для i -ї послуги s_i.

Нехай необхідно визначити оптимальну конфігурацію для МАП з наступними атрибутами доступу: $A = \{2,102,17\}$, $L_{\text{МАП}} = L_1$ при розрахованій оцінці інформаційної швидкості в радіоканалі V +1024.

Правило F_S для розглянутих конфігурацій задано наступними від-відносинами

$$CONF_0 \overset{F_S}{\to} \{s_1, s_2, s_3, s_4, s_5\},$$

$$CONF_1 \overset{F_S}{\to} \{s_2, s_4, s_5, s_6, s_7\},$$

$$CONF_2 \overset{F_S}{\to} \{s_6, s_7, s_8\},$$

$$CONF_3 \overset{F_S}{\rightarrow} \{s_2, s_6, s_7, s_8\},$$

$$CONF_4 \overset{F_S}{\rightarrow} \{s_4, s_5, s_6, s_7, s_9\}$$

Знайдемо оптимальну конфігурацію МАП для заданих умов і критеріїв пошуку.

Крок 1. Область значень задана безліччю $CONF = \{CONF_0, CONF_1, CONF_2, CONF_3, CONF_4\}$, $A = \{2{,}102{,}17\}, L_{\text{МАП}} = L_1$.

Крок 2. Критерії задані матрицею SEC і безліччю *VS* .

Крок 3. У відповідність з вирішальним правилом, представленим виразом (3.6), заданими атрибутами доступу $A = \{2{,}102{,}17\}$, і $L_{\text{МАП}} = L_1$ безліч допустимих критеріїв визначено як $CONF^{\text{доп}} = \{CONF_2, CONF_3, CONF_4\}$.

Крок 4. Упорядковуємо безліч $CONF^{\text{доп}}$ у відповідність з критерієм, $|S_n^*| \rightarrow max$, де $S^* = F_S(CONF^*)|CONF^* \in CONF^{\text{доп}}$, $S^* \subseteq S$. В результаті отримуємо $CONF^{\text{доп}} = \{CONF_4, CONF_3, CONF_2\}$.

Крок 5. Здійснюється покроковий аналіз отриманої впорядкованої безлічі $CONF^{\text{доп}}$на предмет задоволення його елементів критеріям $\left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j \rangle} \leq \hat{V}_{lm} | CONF_j \in CONF^{\text{доп}}$ і $|S^*| \rightarrow \max$. В результаті отримуєм:

- для $CONF_4$ $|S^*| = 5, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_4 \rangle} = 1984, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j \rangle} > \hat{V}_{lm}$
- для $CONF_3$ $|S^*| = 4, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_3 \rangle} = 896, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j \rangle} \leq \hat{V}_{lm}$
- для $CONF_4$ $|S^*| = 2, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_2 \rangle} = 832, \left(\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*}\right)_{\langle CONF_j \rangle} \leq \hat{V}_{lm}$

Таким чином, з допустимих конфігурацій МАП заданим критеріям задовольняє конфігурація $CONF_3$.

2.5 Оцінка властивостей розробленого алгоритму управління безпекою мобільного абонентського пристрою

Для розробленого алгоритму управління безпекою МАП була проведена оцінка таких основних властивостей [43]:

– результативність;

– елементарність;

– коректність;

– обчислювальна складність;

– складність алгоритму по пам'яті;

– точність;

– збіжність.

Результативність (відсутність аварійної зупинки) алгоритму досягається перевіркою коректності вхідних даних. Всі дані вводяться в алгоритм на етапі пуско-налагоджувальних робіт, тому за умови, що вони введені коректно, *алгоритм результативний* .

Даний алгоритм є елементарним , тому що містить блоки, які виконують прості операції: привласнення, обчислення математичних виразів і порівняння. Для блоків, які не є елементарними, призначених для перетворення вихідних даних, елементарність досягається докладним опиисом операцій, що здійснюються над даними в цих блоках. Не елементарними блоками в розробленому алгоритмі являються тільки блоки вимірювання рівня сигналу, що приймається точками доступу. В даному блоці реалізується операція виведення даних з драйвера модуля бездротового зв'язку, що містять інформацію про рівень потужності прийнятого від МАП сигналу.

Доказ коректності алгоритму зводиться до вказівки блоків, які є виходами з усіх можливих циклів. Загального алгоритму циклів немає. Приватні підпрограми мають цикли, побудовані за принципом циклу "for" без операцій додаткової модифікації ітератора всередині тіла циклу, що дає підставу говорити про те, що всі цикли кінцеві. Таким чином, *алгоритм є коректним* .

Загальна тимчасова складність алгоритму визначається часом ініціалізації ($T_{\text{ініц}}$) і часом, витрачаємо на процедури визначення місцерозположення (T_{LOC}), формування вимог безпеки (T_{POLICY}) і формування конфігурації МАП (T_{CONF}). Таким чином, складність алгоритму складе

$$S_t = T_{\text{ініц}} + T_{LOC} + T_{POLICY} + T_{CONF}, \qquad (2.17)$$

де $T_{LOC} = \{t_{\text{трілат}}, \lfloor t_{kNN}, t_{\text{НММ}} \}$, $t_{\text{трілат}}$- складність алгоритму трілатерації, t_{kNN}- складність алгоритму визначення місця розташування на основі методу k -

найближчих сусідів, $t_{\text{НММ}}$- складність алгоритму визначення місця розташування на основі баєвського підходу.

Найбільш трудомісткими процедурами є процедури визначення місцерозположення методами k -найближчих сусідів, методом на основі баєвського підходу і процедура формування вимог безпеки T_{POLICY}.

Складність алгоритму визначення місцерозположення методом k - найближчих сусідів становить:

$$t_{kNN} \sim k \cdot N_{kNN}, \quad (2.18)$$

де k - число "сусідів", N_{kNN} - число точок сигнального простору.

Складність алгоритму визначення місцерозположення методом на основі баєвського підходу становить:

$$t_{HMM} \sim N_{AP} \cdot N_{Int} + k \cdot N_{HMM} \quad (2.19)$$

де N_{AP} - число точок доступу бездротової мережі; k - число найбільш ймовірних станів; N_{Int} - число інтервалів гістограми частот для функції щільності розподілу ймовірностей помилки вимірювань розташування; $N_{\text{НММ}}$ - число точок сигнального простору.

Складність алгоритму формування вимог безпеки залежить від кількості приміщень і заданого числа випробувань методу Монте-Карло. Таким чином,

$$T_{POLICY} \sim N_{MC} \cdot N_{Int} \cdot N_{Rooms}, \quad (2.20)$$

де N_{MC} - задане число випробувань для методу Монте-Карло; N_{Int} - число інтервалів гістограми частот для щільності розподілу ймовірностей помилки вимірювань місця розташування; N_{Rooms} - кількість приміщень. Таким чином, складність алгоритму за часом становитиме:

$$S_t = C_1(N_{AP} \cdot N_{Int} + k \cdot N_{HMM}) + C_2 \cdot N_{MC} \cdot N_{Int} \cdot N_{Rooms}, \quad (2.21)$$

де C_1 , C_2 , - константи.

Оцінювання тимчасової складності алгоритму проводилось на ПЕОМ з наступними технічними характеристиками: процесор: Intel® Core™2 Duo CPU E4600 @ 2,40 ГГц; Встановлена пам'ять (ОЗУ): 2,00 ГБ; Тип системи: 32-розрядна ОС; ОС: Windows 7 Professional SP 1.

В якості вихідні дані використовувалися:

1) технічні характеристики МАП:

– потужність передавача +0,07943282347242815 Вт;

– частота передавача 2,4 ГГц з підносійними, обумовленими стандартом 802.11n;

– параметри k_λ і Г , що характеризують сигнально-перешкодну обстановку, визначені рівні 0,53 і 12,77 відповідно;

2) розташування, рівні захищеності і інші параметри приміщень визначаються схемою приміщень, представленої на рис. 2.9, при розмірах будівлі 16,8 м × 38,0 м ;

3) точки доступу бездротової мережі в системі координат досліджуваної будівлі розташовані в такий спосіб: $AP_1 = (3{,}6\text{ м}; 19{,}2)\text{ м}$, $AP_2 = (3{,}6\text{ м}; 5{,}2\text{м})$, $AP_3 = (20{,}0\text{ м}; 12{,}0\text{ м})$, $AP_4 = (37{,}6\text{ м}; 5{,}2\text{ м})$, $AP_5(37{,}6\text{ м}; 19{,}2\text{ м})$;

4) політика безпеки МАП в ЗКМ визначена табл. 2.1;

5) матриця нормативів інформаційної швидкості для наданих користувачеві МАП послуг у відповідність з [43] визначена табл. 2.2.

Таблиця 2.2 - Нормативи інформаційної швидкості для наданих користувачу МАП послуг

послуга	Норматив, КБ/с
Робота в режимі відеоконференцзв'язку (два абонента)	384
Електронна поштова обмін	64
Робота в режимі VIP-клієнта	128
Передача мультимедійних повідомлень через мережу стільникового зв'язку	128
Прийом і передача захищених SMS повідомлень	64
захищена відеоконференцзв'язок	512
Захищена IP-телефонія	256
Захищений електронний поштовий обмін	64
Захищений доступ до передачі даних по бездротових каналах зв'язку Wi-Fi (802.11n)	10000

Розрахунок розташування МАП здійснювався в відповідність з виразами для методу трилатерації - (А.3) - (А.19), для методу k -найближчих сусідів - (А.20) - (А.25), для методу на основі баєвського підходу - (А.26) - (А.31).

Розрахунок ймовірності місцезнаходження МАП в спеціальному приміщенні здійснювався в відповідність з виразами (1.4) - (1.10).

Оцінювання інформаційної швидкості в радіоканалі МАП з урахуванням сигнально-перешкодної обстановки здійснюється відповіднодо виразу (2.14).

Розроблені алгоритми реалізовані в програмному комплексі, що складається з низкою програм для ЕОМ [44]. Оцінки тимчасової складності вказаних алгоритмів, отримані за допомогою даних програм, представлені в табл. 2.3.

Таблиця 2.3 - Оцінки тимчасової складності процедур алгоритму управління конфігурацією МАП

Алгоритм (процедура)	Параметр	Тимчасова

		складність, мс
Ініціалізація вихідних даних	$T_{\text{ініц}}$	0,01
Алгоритм визначення розташування - на основі методу трилатерації - на основі методу *k*-найближчих сусідів - на основі баєвського підходу	T_{LOK}	 0,98 1,01 2,92
Алгоритм визначення ймовірності місцезнаходження МАП в спеціальному приміщенні	T_{POLICY}	710
Алгоритм оцінювання інформаційної швидкості в бездротовому каналі доступу	T_V	0,3
Алгоритм формування оптимальної конфігурації МАП	T_{CONF}	1,12
Разом:	S_t	714,35

Аналіз таблиці показує, що найбільш обчислювальною є процедура визначення ймовірності МАП в спеціальному приміщенні, при цьому сумарна тимчасова складність алгоритму управління конфігурацією МАП не перевищує 714,35 мс.

Складність алгоритму по пам'яті ріняється $S_v = N_{AP} \cdot N_{Int} \cdot N_{HMM} + N_{Rooms}$. Така оцінка складності є поліноміальною. У процесі визначення місця розположення методом на основі баєвського підходу необхідно зберігати дані про всі приміщеннях, а також статистику умовних ймовірностей спостереження рівнів потужності сигналу МАП в N_{HMM} точках сигнального простору.

Збіжність . Критичними операціями в алгоритмі є:

– цикл з умовою, що реалізується блоками 3-8, рис. 2.2; блоками 2, 3, рис. В.4; блоками 2, 4, 5; блоками 3, 4, 6, 7,рис. В.5; блоками 2, 4, 5, 13, 15, 17, 18, рисунки В.6, Б.7; блоками 3, 7, 12, 15, рисунки В.8, В.9; блоками 2, 4, рис. 2.3;

– функція розподілу на змінну в блоках 4, 6, 8, 10, 13, рис. В.4; в блоці 10, рис. В.5 блоках 2, 3, рис. В.3; блоках 9, 16, рис. В.8, В.9;

– обчислення квадратного кореня в блоках 4, 6, 8, 10, 17, 13, рис. В.4.

На основі аналізу набору передумов для кожного кроку алгоритм можна вважати збіжність за умови коректності та несуперечливості вихідних даних.

Точність . Точність розробленого алгоритму визначається похибкою обчислень, яка в загальному випадку складається з $\delta_{\text{н}}$ – неусуненої похибки вихідних даних, $\delta_{\text{м}}$ -похибки методу і $\delta_{\text{в}}$ -похибки обчислювальної платформи, тобто

$$\delta = \delta_{\text{н}} + \delta_{\text{м}} + \delta_{\text{в}} \quad (2.22)$$

Похибка вихідних даних зележить від числа значущих цифр значень параметрів і визначається за формулою:

$$\delta_{\text{н}} = 10^{-N+1} \quad (2.23)$$

У розглянутому алгоритмі мінімальна довжина мантіси вихідних даних N=10. Таким чином, $\delta_{\text{н}} \approx 10^{-N+1} = 10^{-9}$.

Для оцінки похибки методу будемо керуватися наступними правилами:

1) При підсумовуванні чисел одного знака точність суми дорівнює найменшій точності будь-якого доданка:

$$\delta_{\text{м}}^{+} = sup(\delta_1, \delta_2, \dots, \delta_n) \quad (2.24)$$

2) При відніманні чисел відбувається збільшення максимальної відносної похибки одного з компонентів вираження в v раз, де

$$v = \frac{|a+b|}{|a-b|}, \quad (2.25)$$

тоді

$$\delta_{\text{м}}^{-} = sup(\delta_1, \delta_2, \dots, \delta_n) \cdot v \quad (2.26)$$

де a і b - величини, що входять в операцію віднімання.

3) Добуток і частка двох величин володіють похибкою, приблизно рівній сумі відносних похибок компонентів виразів:

$$\delta_{\text{м}}^{\times} \approx \sum_{i=1}^{n} \delta_1, \quad (2.27)$$

$$\delta_{\text{м}}^{\div} \approx \sum_{i=1}^{n} \delta_1, \quad (2.28)$$

4) Для оцінки похибки функцій використовуються наступні співвідношенням

$$\delta_{\text{м}}^{y} \approx v \cdot \delta_{\text{н}}(x), \quad (2.29)$$

де

$$v = \frac{|x| \cdot |f'(x)|}{|f(x)|} \quad (2.30)$$

де $y = f(x)$ – досліджувана функція; x - аргумент досліджуваної функції; y - розраховане значення функції.

Таким чином, розрахункова точність алгоритму становить 10^{-4}.

2.6 Висновки по другому розділу

1. Розроблено алгоритм управління безпекою МАП, що дозволяє забезпечити зміну програмно-апаратної конфігурації МАП в залежності від умов (атрибутів) доступу, що включають в себе, в тому числі, місце розташування МАП, і критеріїв якості послуг, що надаються. Відмінними особливостями даного алгоритму є:

– реалізація формальної моделі безпеки МАП, яка передбачає врахування умов (атрибутів) доступу, включаючи місце розташування МАП, вимоги мандатної рольової політик управління доступом;

– застосування методу Монте-Карло для підвищення достовірності визначення місця розташування МАП в спеціальному приміщенні на підставі обчисленого місця розташування методами трилатерации, k -найближчих сусідів і методу, заснованого на Баєвському підході;

– використання алгоритму оцінки інформаційної швидкості в каналі БМПД, що враховує сигнально-перешкодну обстановку, для вибору оптимальної, з точки зору вимог щодо якості послуг, що надаються, програмно-апаратної конфігурації МАП;

– формування оптимальної програмно-апаратної конфігурації МАП з точки зору виконання вимог політики безпеки в ЗКМ і якості послуг, що надаються, реалізоване у формі багатокритеріальної оптімізації цілочисельноого динамічного програмування.

2. Представлено опис циклу управління конфігурацією МАП з рівняннями стану і спостереження, обгрунтуванням мети управління.

3. Описано основні процедури, що входять до складу розробленого алгоритму. Досліджено основні властивості алгоритму і його процедур, включаючи тимчасову складність, складність по пам'яті і точність. Отримано їх чисельні оцінки, а також представлений чисельний приклад роботи алгоритму.

3 СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ

3.1 Рекомендації з оптимального взаємного розташування точок до-ступа мережі в системі визначення місця розташування

Ефективність підсистеми визначення місця розташування в системі управління безпекою мобільних абонентських пристроїв в корпоративних мережах з різними вимогами по захищеності визначається її параметрами, які повинні налаштовуватися в залежності від умов експлуатації. Для вибору оптимальних параметрів алгоритмів визначення місця розташування була проведена група експериментів, результати яких представлені в роботі [43]. В якості інструменту дослідження в експериментах використовувалася розроблена імітаційна модель [42, 43, 49]. Схема приміщень, досліджувана в експериментах, представлена на рис. 1.9.

Для методу трилатерації було досліджено вплив кількості використаних точок доступу і їх розташування на точність визначення місця розташування. Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to min, \\ \text{var } AP_j = (x_j, y_j), j = \overline{1, N_{AP}}, \\ \text{var } N_{AP} = 3 \dots 5, \end{cases} \quad (3.1)$$

де e_L -помилка визначення місця розташування, що обчислюється у відповідність з виразом (1.3), в якому $(\tilde{x}_{tr}, \tilde{y}_{tr})$ - обчислені методом трилатерації координати місця розташування МАП, а $(\tilde{x}, \tilde{y})$- реальні координати місця розташування МАП; N_{AP}точок доступу з заданими координатами $(x_j, y_j), j = \overline{1, N_{AP}}$.

Результати експериментів для трьох точок доступу представлені в табл. 3.1, для чотирьох - в табл. 3.2 і для п'яти - в табл. 3.3.

Таблиця 3.1 - Статистичні параметри помилки визначення місця розташування для різного розташування трьох точок доступу на карті приміщень

№ карти розташування точок доступу	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
1	7,533	4,063	23,669	0,069	0,101

2	8,877	5,11	30,573	0,036	0,133
3	4,984	10,378	52,716	0,212	0,284
4	5,45	3,759	56,847	0,068	0,098
5	5,924	4,623	25,037	0,055	0,125
6	5,297	3,456	22,087	0,097	0,094
7	5,883	4,379	26,92	0,026	0,119
8	7,705	4,712	25,493	0,079	0,125
9	6,484	3,766	27,166	0,078	0,102
10	6,088	4,387	32,627	0,115	0,12
11	5,561	4,221	28,042	0,031	0,115
12	9,538	3,66	29,606	0,047	0,096
13	9,547	4,471	29,685	0,115	0,119
14	15,548	7,393	39,889	1,616	0,198

а) б)

Рисунок 3.1 - Схема оптимального розташування трьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування: а) карта № 3, б) карта № 6

Таблиця 3.2 - Статистичні параметри помилки визначення місця розташування для різного розташування чотирьох точок доступу на карті приміщень

№ карти розташування точок доступу	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
1	5,592	3,43	20,495	0,023	0,078
2	5,305	3,351	26,896	0,054	0,089
3	6,499	4,167	20,79	0,024	0,112
4	5,024	2,89	21,372	0,037	0,078
5	4,904	3,213	19,442	0,05	0,087
6	5,132	3,271	22,431	0,09	0,088
7	4,967	3,341	21,898	0,121	0,089

8	5,806	3,447	23,277	0,072	0,09
9	8,505	3,057	24,891	0,096	0,078
10	15,467	7,591	38,175	1,496	0,201
11	5,742	3,484	18,007	0,041	0,091

Для чотирьох точок доступу найкраща точність визначення місця розташування досягається при взаємному розташуванні точок доступу так, як показано на рис. 3.2.

а) б)

Рисунок 3.2 - Схема оптимального розташування чотирьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування: а) карта № 5, б) карта № 7

Таблиця 3.3 - Статистичні параметри помилки місцерозположення для різного розташуванням п'яти точок доступу на карті приміщень

№ карти розташування точок доступу	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
1	4,986	2,865	24,135	0,1	0,077
2	5,792	3,549	23,549	0,054	0,066
3	5,837	3,994	23,574	0,094	0,108
4	6,251	3,849	26,811	0,126	0,104
5	6,193	3,931	23,195	0,029	0,105
6	5,823	3,02	23,631	0,08	0,075
7	6,375	3,696	21,159	0,03	0,098

Для п'яти точок доступу найкраща точність визначення місця розташування досягається при взаємному розташуванні точок доступу так, як показано на рис. 3.3.

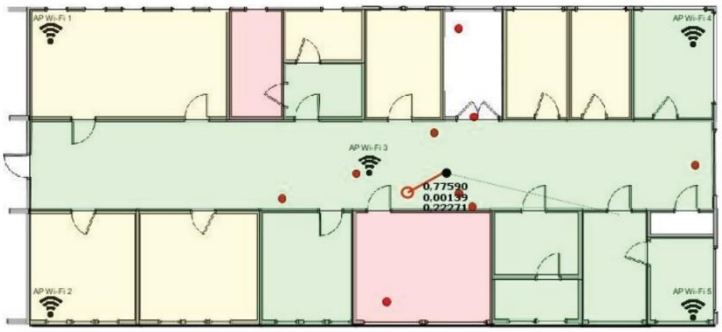


Рисунок 3.3 - Схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення

Експерименти, проведені в аналогічних умовах для методів k - найближчих сусідів і баєвського підходу, показали, що найкраща точність визначення місця розташування досягається при аналогічному розташуванні точок доступу як і для методу трилатерації.

3.2 Рекомендації по значенням параметрів методу k -найближчих в сусідів системі визначення місця розташування

В табл. 3.4 представлені результати експериментів, в яких дослід-валась залежність точності визначення місця розташування для методу k - найближчих сусідів в залежності від числа k .

Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10 \\ \operatorname{var}(x_i, y_i) \left| X^{N_{kNN}} = \left\langle \{(x_i, y_i), v_i\}, \mathrm{P}_{r_i}^{RSS} \right\rangle, i = \overline{1, N}_{kNN}, \right. \\ \operatorname{var} N_{kNN} \left| X^{N_{kNN}} = \left\langle \{(x_i, y_i), v_i\}, \mathrm{P}_{r_i}^{RSS} \right\rangle, i = \overline{1, N}_{kNN}, \right. \end{cases} \quad (3.2)$$

де e_L -помилка визначення місця розташування, що обчислюється у відповідність з виразом (1.3), в якому $(\tilde{x}_{kNN}, \tilde{y}_{kNN})$ - обчислені методом k - найближчих сусідів координати місця розташування МАП, а $(\tilde{x}, \tilde{y})$ - реальні координати місця розташування МАП ; k - число "сусідів" в сигнальному просторі; (x_i, y_i)- координати i -й точки карти сигнального простору; v_i - кут орієнтації в пропросторі МАП; $P_{r_i}^{RSS}$– рівень потужності сигналу від МАП;$i = \overline{1, N_{kNN}}$ - індекс точки вимірювань карти сигнального простору, а N_{kNN} - їх кількість.

Експерименти здійснювалися для п'яти точок доступу і карти приміщень, зображених на рис. 3.3.

Таблиця 3.4 - Статистичні параметри помилки позиціонування для методу k -бліжайшіх сусідів в залежності від числа k

Значення числа k	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
1	4,225	2,848	30,415	0,024	0,078
2	3,529	2,387	22,187	0,04	0,065
3	3,617	2,561	30,47	0,007	0,069
4	3,254	2,128	22,169	0,079	0,057
5	3,261	2,164	19,499	0,01	0,054
6	3,185	1,994	19,923	0,098	0,055
7	3,221	2,283	21,627	0,055	0,061
8	3,289	2,284	21,931	0,011	0,062
9	3,147	2,028	19,336	0,009	0,054
10	4,477	2,565	21,428	0,034	0,067

Як видно із таблиці найкраща точність визначення місцерозташування досягалася при значеннях $k = 6$ і $k = 9$.

На рис. 3.11 представлений графік залежності вибіркового середнього і середньоквадратичного відхилення (СКВ) для помилки визначення місцерозташування від числа "сусідів".

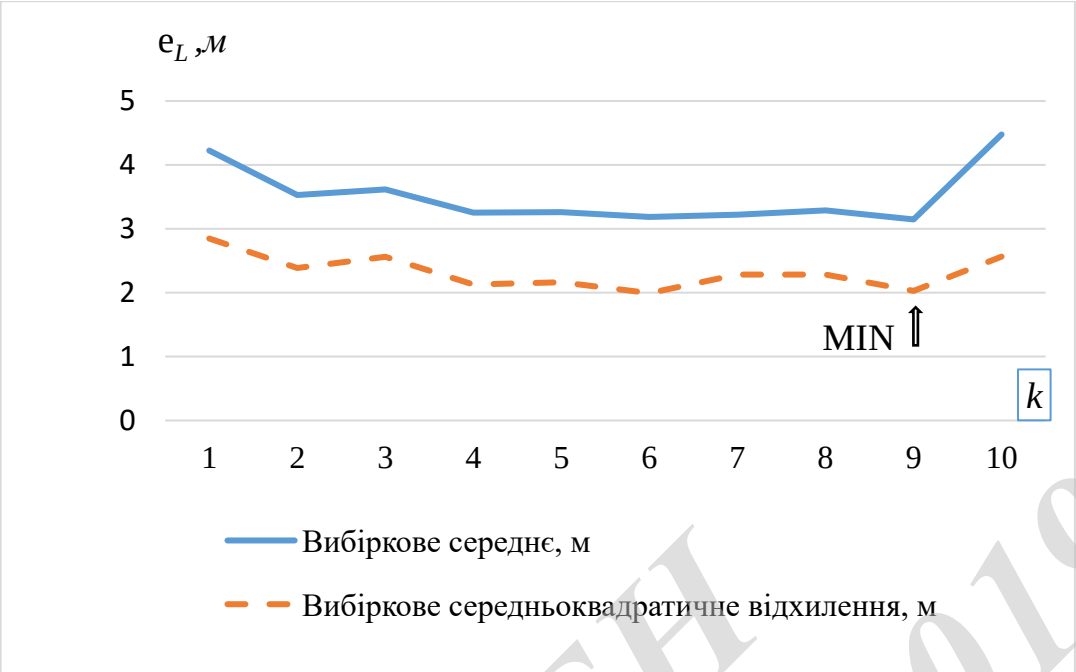


Рисунок 3.11 - Графік залежності вибіркового середнього і СКВ для помилки визначення місця розташування від числа "сусідів"

Для значень числа врахованих найближчих «сусідів» $k = 6$ і $k = 9$ були проведені експерименти з метою дослідження впливу розташування точок вимірювання рівня сигналу на карті сигнального простору. Розташування точок вимірювань в імітаційній моделі вибиралося в вигляді сітки квадратів або пря-мокутників, сторони яких визначалися кроком сітки по горизонталі і вер-тикалі. Наприклад, крок сітки карти сигнального простору $h = 1{,}5x1{,}5$ означає ширину і довжину прямокутника сітки, рівні 1,5м. У табл. 3.5 представлені результати даного експерименту.

Таблиця 3.5 - Статистичні параметри помилки визначення місця розташування для методу k -найближчих сусідів в залежності від кроку сітки карти сигнального простору

Крок сітки карти h, м	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
k 6					
0,5x0,5	3,27	2,33	22,995	0,073	0,064
1x1	3,185	1,994	19,923	0,098	0,055
1,5x1,5	3,162	2,072	22,075	0,003	0,056
2x2	3,067	2,058	22,306	0,007	0,051

2,5x2,5	3,36	2,079	14,773	0,043	0,053
3x3	3,484	2,205	17,341	0,023	0,06
k 9					
0,5x0,5	3,18	2,021	18,224	0,035	0,037
1x1	3,147	2,028	19,336	0,009	0,054
1,5x1,5	2,603	1,702	21,212	0,023	0,046
2x2	3,104	2,181	22,769	0,034	0,06
2,5x2,5	3,291	1,894	14,394	0,072	0,049
3x3	4,472	2,393	14,033	0,067	0,065

Графік залежності статистичних параметрів помилки визначення місцерозположення від кроку сітки вимірів карти сигнального простору представлений на рис. 3.12.

Із таблиці і рисунка видно, що найкраща точність визначення місцерозположення для методу k -найближчих сусідів досягається при значеннях кроку сітки вимірів карти сигнального простору рівного $h = 1{,}5x1{,}5$ і $h = 2{,}0x2{,}0$м як при k=6, так і k=9.

Найкращі значення статистичних параметрів помилки визначення місцерозположення в проведених експериментах були досягнуті при значеннях k=9 і $h = 1{,}5x1{,}5$м.

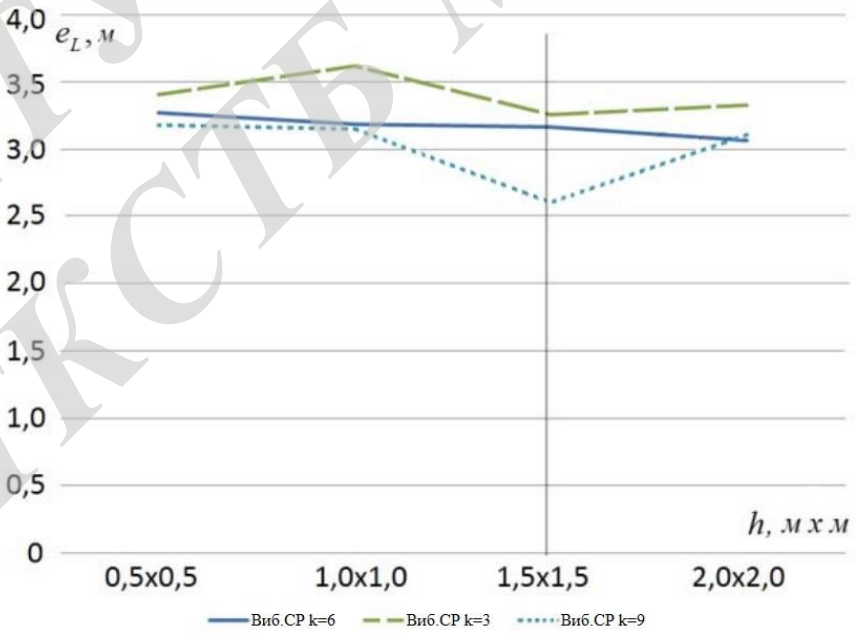


Рисунок 3.12 - Графік залежності помилки визначення місця розташування від кроку сітки вимірів карти сигнального простору

3.3 Рекомендації по значенням параметрів методу на основі баєвського підходу в системі визначення місця розташування

Для дослідження ефективності підсистеми визначення місця розташування на основі баєвського підходу були проведені експерименти з метою вибору оптимальних параметрів

– для числа "сусідів" - кількості найбільш ймовірних станів, що враховуються при обчисленні розташування;

– розташування точок вимірювань на карті сигнального простору;

– кількість вимірювань в кожній точці карти вимірювань при формуванні статистики розподілу ймовірностей рівнів потужності сигналу МАП.

Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10 \\ \operatorname{var}(x_i, y_i) \left| X^{N_{HMM}} = \left\langle (x_i, y_i), \mathrm{P}_{r_i}\left[\lambda_i / (x_i, y_i)\right]\right\rangle, i = \overline{1, N}_{HMM}, \right. \\ \operatorname{var} N_{HMM} \left| X^{N_{HMM}} = \left\langle (x_i, y_i), \mathrm{P}_{r_i}\left[\lambda_i / (x_i, y_i)\right]\right\rangle, i = \overline{1, N}_{HMM}, \right. \end{cases} \quad (3.3)$$

де e_L -помилка визначення місця розташування, що обчислюється у відповідності з виразом (1.3), в якому $(\tilde{x}_{HMM}, \tilde{y}_{HMM})$ - обчислені методом на основі баєвського підходу координати місця розташування МАП, а $(\tilde{x}, \tilde{y})$- реальні координати розташування МАП; k - число найбільш ймовірних станів;

$(\mathrm{x}_i, \mathrm{y}_i)$- координати i -й точки карти сигнального простору; $P_{r_i}[\lambda_i / (x_i, y_i)]$- умовна ймовірність отримання вимірювань сигналу передавача МАП зі статистичним розподілом λ_i в точці з координатами (x_i, y_i); N_{HMM} - кількість точок сигнального простору навчальної вибірки.

В табл. 3.6 представлені результати експерименту, в якому дослід-валась залежність статистичних параметрів помилки визначення місця розташування від числа "сусідів" - кількості найбільш ймовірних станів, що враховуються при обчисленні розташування, на основі баєвського підходу.

Таблиця 3.6 - Статистичні параметри помилки визначення місця розташування для методу на основі баєвського підходу в залежності від числа k

Значення числа k	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
1	3,86	2,309	16,367	0,124	0,063

2	3,376	2,076	13,538	0,082	0,056
3	2,445	1,448	9,764	0,024	0,039
4	2,512	1,616	11,514	0,07	0,043
5	2,466	1,705	11,458	0,033	0,042
6	2,689	1,769	12,948	0,039	0,047
7	2,641	1,84	11,8	0,018	0,05
8	3,195	2,084	10,996	0,034	0,056
9	2,62	1,809	11,17	0,02	0,041
10	2,651	1,812	11,246	0,01	0,049

Графік залежності статистичних параметрів помилки визначення місця розташування від числа "сусідів" - кількості найбільш ймовірних станів, що враховуються при обчисленні розташування, представлений на рис. 3.13.

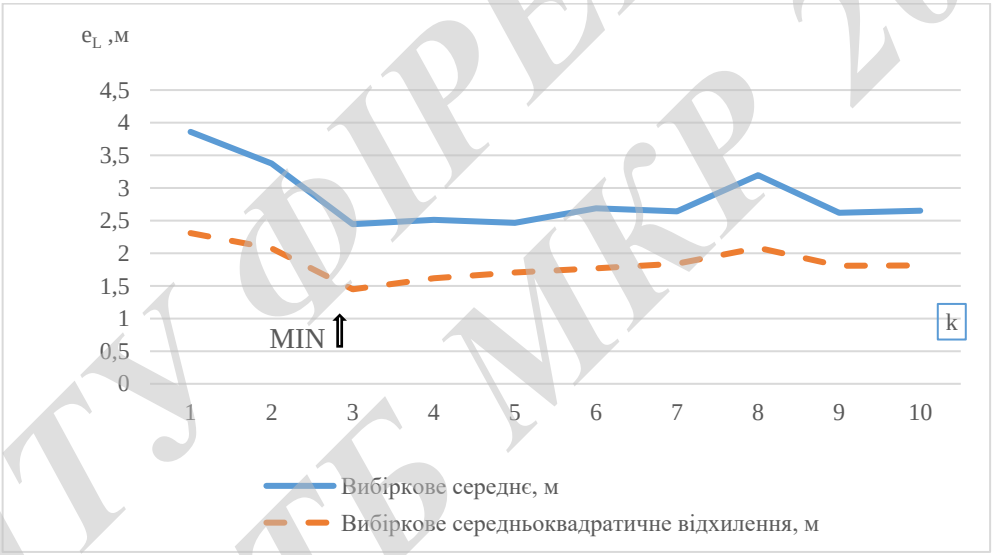


Рисунок 3.13 - Графік залежності вибіркового середнього і СКВ для помилки визначення місця розташування від кількості найбільш ймовірних станів

З таблиці і рисунка видно, що найкраща точність визначення місцерозположення для баєвського підходу досягається при значенні $k = 3$.

В табл. 3.7 представлені результати експерименту, в якому дослід-валась залежність статистичних параметрів помилки визначення місця розташування від кроку сітки карти сигнального простору для методу на основі баєвського підходу.

Графік залежності статистичних параметрів помилки визначення місцерозположення від кроку сітки вимірів карти сигнального простору представлений на рис. 3.14.

Таблиця 3.7 - Статистичні параметри помилки визначення місця розташування для методу на основі баєвського підходу в залежності від кроку сітки карти сигнального простору

Крок сітки карти h, м	Вибіркове середнє, м	Вибіркове середньоквадратичне відхилення, м	Максимальне значення, м	Мінімальне значення, м	Довірчий інтервал для середнього
0,5x0,5	2,669	1,662	12,333	0,025	0,044
1x1	2,828	1,747	14,438	0,041	0,044
1,5x1,5	2,728	1,788	11,915	0,054	0,047
2x2	2,662	1,657	11,419	0,03	0,045
2,5x2,5	3,304	2,149	13,44	0,05	0,058
3x3	3,703	2,394	14,505	0,076	0,064

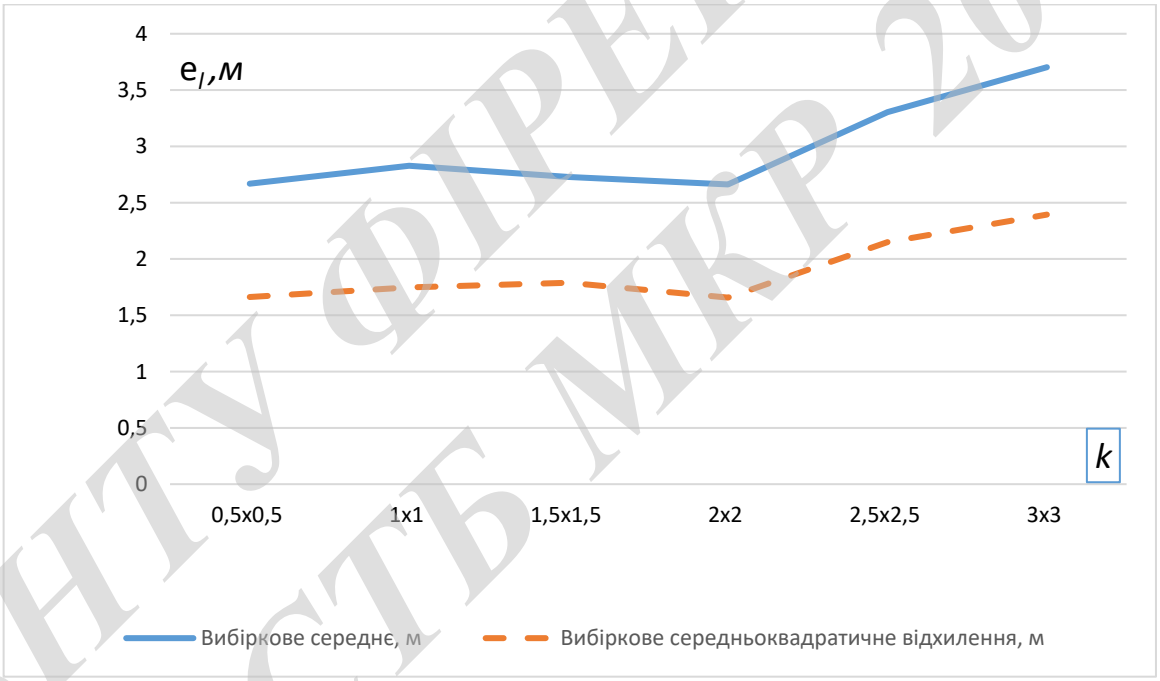


Рисунок 3.14 - Графік залежності вибіркового середнього і СКВ для помилки визначення місця розташування від кроку сітки вимірів карти сигнального простору

З таблиці і рисунка видно, що найкраща точність визначення місцерозположення для методу на основі баєвського підходу досягається при значеннях кроку сітки вимірів карти сигнального простору рівного $h = 1{,}5x1{,}5$м і $h = 2{,}0x2{,}0$м. Таким чином, результати для даного методу збігаються з аналогічним експериментом для методу k -найближчих сусідів.

В табл. 3.8 і на рис. 3.15 представлені результати експерименту, в якому досліджувалася залежність статистичних параметрів помилки визна-лення

місця розташування від кількості вимірювань M в кожній точці карти вимірювань при формуванні статистики розподілу ймовірностей рівнів потужності сигналу МАП для методу на основі баєвського підходу.

З таблиці і рисунка видно, що найкраща точність визначення місцерозположення для методу на основі баєвського підходу досягається при значеннях кількості вимірювань рівного $M = 30$, при цьому близькі значення для виборочного середнього помилки визначення місця розташування отримані для $M = 110$.

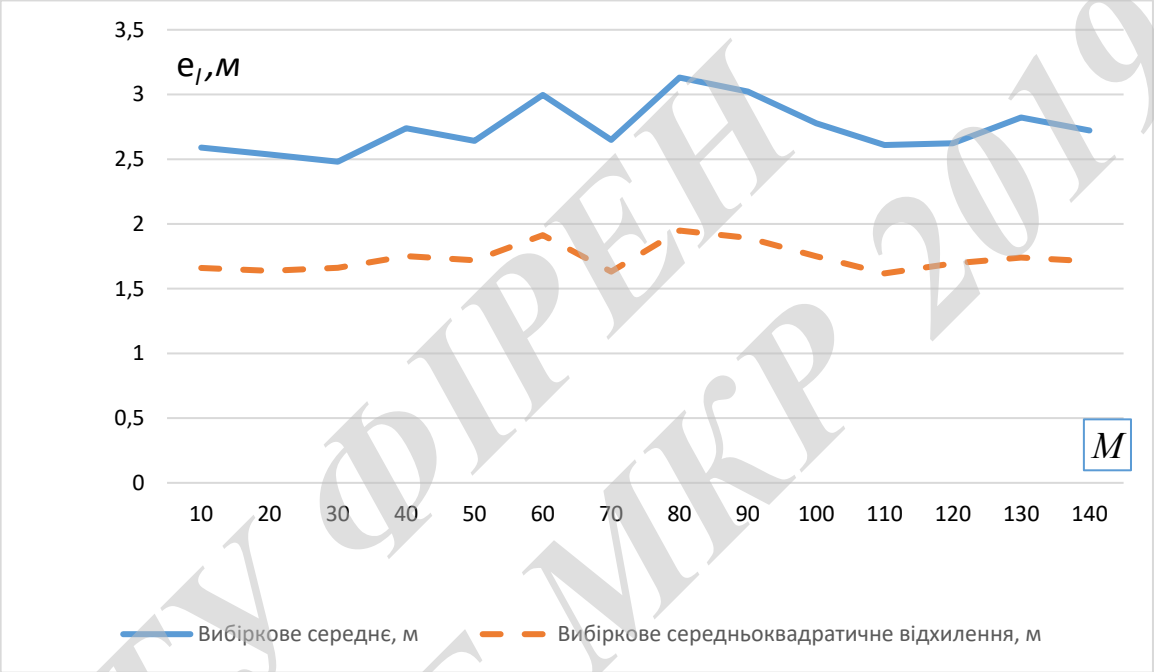


Рисунок 3.15 - Графік залежності помилки визначення місця розташування від кількості вимірювань в кожній точці карти вимірювань при формуванні статистики розподілу ймовірностей рівнів потужності сигналу МАП

Таблиця 3.8 - Статистичні параметри помилки визначення місця розташування для методу на основі баєвського підходу в залежності від кількості вимірювань M в кожній точці карти вимірювань

Кількість вимірювань M	Вибіркове середнє, M	Вибіркове середньоквадратичне відхилення, M	Максимальне значення, M	Мінімальне значення, M	Довірчий інтервал для середнього
10	2,59	1,66	10,855	0,031	0,045
20	2,537	1,638	12,393	0,012	0,044
30	2,481	1,661	12,596	0,025	0,045
40	2,739	1,751	11,709	0,019	0,047
50	2,642	1,72	11,966	0,063	0,045

60	2,997	1,913	13,744	0,053	0,052
70	2,649	1,632	11,509	0,026	0,044
80	3,131	1,949	12,307	0,048	0,052
90	3,023	1,893	12,842	0,031	0,051
100	2,778	1,75	11,938	0,051	0,048
110	2,61	1,618	12,347	0,005	0,043
120	2,623	1,695	11,726	0,022	0,046
130	2,822	1,74	12,191	0,038	0,047
140	2,722	1,712	12,316	0,055	0,046

3.4 Висновки по третьому розділу

1. Проведена група експериментів, що дозволяють обґрунтувати вибір опти-мальних параметрів підсистеми визначення місця розташування, які використовують різні технології визначення місця розташування, а також параметри підсистеми визначення рівня захищеності приміщення на основі обчисленого розташування і методу Монте-Карло.

2. Обґрунтовано оптимальні параметри підсистем визначення місцерозташування для заданої карти приміщень:

1) метод трилатерації:

– кількість точок доступу - 5;

– оптимальне розташування точок доступу так, як показано на рис. 3.3;

2) метод k -найближчих сусідів:

– число врахованих найближчих «сусідів» $k = 6$ або $k = 9$;

– крок сітки карти сигнального простору $h = 1{,}5x1{,}5$;

– кількість точок доступу - 5;

– оптимальне розташування точок доступу так, як показано на рис. 3.3;

3) метод на основі баєвського підходу:

– число врахованих найближчих «сусідів» $k = 3$;

– крок сітки карти сигнального простору $h = 1{,}5x1{,}5$;

– кількість вимірювань в кожній точці сигнального простору з відомого-координатами $M \geq 30$;

– кількість точок доступу - 5;

– розташування точок доступу оптимально для карти, зображеної на рис. 3.3.

3. Найбільш точним методом визначення місця розташування є метод, заснований на баєвському підході в сукупності з методом Монте-Карло.

4. Оптимальними параметрами для методу Монте-Карло при визначенні рівня захищеності приміщення є:

– кількість випробувань $M = 1000$;

– емпіричний закон розподілу ймовірностей.

5. За допомогою параметра порогу прийняття рішення можна регулювати величину помилок 1-го і 2-го роду при визначенні рівня захищеності приміщення. При цьому виконання умови $P_\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le P_\beta^{\text{доп}}$ в разі, коли $P_\beta^{\text{доп}} = 0{,}01$, можна досягти лише при завданні граничних параметрів підсистеми визначення місця розташування.

6. Розроблено науково-технічні пропозиції щодо складу і місця визначення системи управління безпекою МАП до послуг корпоративних мереж з різними вимогами по захищеності.

7. Здійснено комплексну оцінку ефективності розроблених пропозицій з отриманням чисельних значень для оцінки часу, необхідного для зміни конфігурації МАП, ймовірності загрози порушення конфіденційності при використанні керованих МАП, ресурсоємності запропонованої системи управління безпекою МАП, своєчасності доступу до послуг при використанні керованих МАП .

8. Отримана чисельна оцінка ступеня досягнення мети магістерського дослідження, що дозволяє стверджувати те, що мета досягнута.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Розрахунок витрат на проведення НДР з дослідження характеристик керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах

В техніко-економічному обґрунтуванні представленому в першому розділі даної магістерської кваліфікаційної роботи було приблизно обґрунтовано доцільність проведення НДР. Тому в даному розділі будуть проведені більш детальні розрахунки витрат на проведення НДР з дослідження характеристик керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах.

Для економічного розрахунку проведення НДР потрібно скласти кошторис витрат, який передбачає розрахунок визначених основних статей витрат.

Основна заробітна плата дослідників та розробників, яка розраховується за формулою [66]:

$$З_о = \frac{M}{T_р} \cdot t \text{ ,} \qquad (4.1)$$

де M – місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ – число робочих днів в місяці, 22 дні;

t – число днів роботи розробника (дослідника).

Проведені розрахунки зводимо до таблиці.

Таблиця 4.1 – Основна заробітна плата дослідників та розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
1. Керівник проекту	8250,90	375,00	66	24750,10
2. Ст. науковий співробітник	6500,00	295,45	66	19500,00
3. Інженер	7200,00	327,27	58	18981,82

4. Консультант- аналітик служби цифрової безпеки	6300,70	286,36	22	6300,70
5. Аналітик з питань математичного моделювання	5480,20	249,09	11	2740,10
6. Технік	4621,50	210,00	44	9240,00
Разом				81511,92

Витрати на основну заробітну плату робітників ($З_р$), що здійснюють підготовку устаткування та пристроїв необхідних для досліджень, підготовку та формування інформаційних потоків, баз даних тощо, розраховуються на основі норм часу, які необхідні для виконання даної роботи, за формулою [66]:

$$З_р = \sum_{1}^{n} t_i \cdot С_i \cdot К_с, \quad (4.2)$$

де t_i - норма часу (трудомісткість) на виконання конкретної роботи, годин;

n - число робіт по видах та розрядах;

$К_с$ - коефіцієнт співвідношень, який установлений в даний час Генеральною тарифною угодою між Урядом України і профспілками, $К_с = 1$;

Ci - погодинна тарифна ставка робітника відповідного розряду, який виконує відповідну роботу, грн./год.

C_i визначається за формулою [66]:

$$С_i = \frac{М_м \cdot К_i}{Т_р \cdot Т_{зм}}, \quad (4.3)$$

де, $М_н$ - мінімальна місячна оплата праці, грн., $М_н = 4173{,}00$ грн.;

$К_i$ - тарифний коефіцієнт робітника відповідного розряду;

$Т_р$ - число робочих днів в місяці, $Т_р = 22$ дні;

$Т_{зм}$ - тривалість зміни, $Т_{зм} = 8$ годин.

Проведені розрахунки внесемо до таблиці.

Таблиця 4.2 – Витрати на основну заробітну плату працівників

Найменування робіт	Трудомі ст-кість, нормо-годин	Розряд роботи	Тарифни й коефіціє нт	Погодинн а тарифна ставка, грн.	Величина оплати, грн.
1. Встановлення офісного обладнання	6,20	2	1,1	26,08	161,70
2. Інсталяція програмного забезпечення	9,18	4	1,35	32,01	293,84
3. Компіляція програмних модулів	199,38	5	1,7	40,31	8036,46
4. Відлагодження програмних модулів	41,40	5	1,7	40,31	1668,73
5. Формування радіоелектронної моделі апаратного комплексу	92,00	2	1,1	26,08	2399,47
Разом					12560,10

Додаткова заробітна плата розробників, дослідників та працівників, які приймали участь в дослідженнях та розробці НДР розраховується як 10 % від основної заробітної плати розробників та працівників:

$$З_д = З_о \text{ *· } 10 / 100\% \quad (4.4)$$

$$З_д = (81511,92 + 12560,10) \text{ *· } 10 / 100 \% = 9407,19 \text{ (грн.)}$$

Нарахування на заробітну плату дослідників та робітників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати:

$$Н_з = (З_о + З_д) \cdot * 22 / 100\% \quad (4.5)$$

$$Н_з = (81511,92 + 12561,10 + 9407,19) * 22 / 100\% = 22765,39 \text{ (грн.)}$$

Витрати на матеріали на даному етапі проведення НДР пов'язані з використанням макетних моделей елементів та моделювання роботи і досліджень за допомогою комп'ютерної техніки.

Витрати на матеріали, що були використані при проведенні досліджень, розраховуються по кожному виду матеріалів за формулою [66]:

$$M = \sum_{1}^{n} H_i \cdot Ц_i \cdot K_i \quad , \tag{4.6}$$

де, - H_i - витрати матеріалу *i*-го найменування, кг;

$Ц_i$ - вартість матеріалу *i*-го найменування, грн./кг.;

K_i - коефіцієнт транспортних витрат, K_i = 1,1;

n - кількість видів матеріалів.

Проведені розрахунки зводимо до таблиці.

Таблиця 4.3 – Витрати на основні матеріали

Найменування матеріалу, марка, тип, сорт	Одиниця виміру	Ціна за одиницю, грн.	Витрачено	Вартість витраченого матеріалу, грн.
Папір канцелярський	уп.	92,00	1	92,00
Компакт-диски	шт.	10,10	5	50,50
Канцелярські товари	компл.	136,00	4	544,00
Офісне начиння	комплект	194,00	2	388,00
Тонер для принтера	кг	5998,00	0,02	119,50
Всього				1183,00

З врахуванням транспортних витрат вартість матеріалів складе

М = 1183,00 * 1,11 = 1313,13 грн.

Витрати на комплектуючі при проведенні досліджень з керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах відсутні.

Амортизація обладнання для проведення досліджень

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

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.7)$$

де $Ц_б$ – балансова вартість обладнання, приміщень тощо, які використовувались для розробки нового технічного рішення, грн.;

$t_{вик}$ – термін використання обладнання, приміщень під час розробки, місяців;

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

Проведені розрахунки необхідно звести до таблиці.

Таблиця 4.4 - Величина амортизаційних відрахувань

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, міс.	Величина амортиза-ційних відрахувань, грн
Програмно-аналітичний комплекс	12050,00	4	3	753,00
Програмний продукт моделювання мереж та програмний продукт автоматизованого визначення геометричних параметрів	35500,00	3	3	2958,33
Офісна оргтехніка	7652,00	4	3	478,15
Дослідницька лабораторія	425010,00	20	3	5312,70
Всього				9502,18

Витрати на силову електроенергію на проведення досліджень розраховують за формулою [66]:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (4.8)$$

де, *В* — вартість 1 кВт-години електроенергії, *В* = 2,21 грн./кВт –година;

П — встановлена потужність обладнання, кВт.;

Ф — фактична кількість годин роботи обладнання, годин. ;

$К_п$ — коефіцієнт використання потужності.

Всі проведені розрахунки зведемо до таблиці

Таблиця 4.5 – Витрати на електроенергію при проведенні досліджень

Найменування обладнання	Кількість годин роботи обладнання, год.	Встановлена потужність, кВт	Коефіцієнт використання потужності	Величина оплати
Обчислювальний комплекс	464,0	0,87	1	901,84
Офісне обладнання	50,0	1,71	1	194,37
Всього				1096,21

Інші витрати охоплюють: загальновиробничі витрати, адміністративні витрати, витрати на відрядження, матеріали, окремі непередбачені комплектуючі, зв’язок, витрати на інтернет-послуги тощо.

Інші витрати доцільно приймати як 200...300% від суми основної заробітної плати дослідників та робітників.

Величина інших витрат складе:

$$I = (81511,92 + 12560,10) * 200 / 100 = 188143,00 \text{ (грн.)}$$

Загальні витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи з керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах:

В =81511,92 + 12560,10 + 9407,19 + 22765,39 + 1313,13 + 9502,18 + 1096,21 +188143,00 = 326299,12 (грн.)

4.2 Визначення коефіцієнта наукової значимості отриманих результатів НДР

Коефіцієнт наукової значимості результатів проведеної НДР $K_{ЗН}$ можна підрахувати за формулою [67]:

$$K_{ЗН} = \frac{\sum_{1}^{3} b_i \cdot d_i}{\sum_{1}^{3} b_{\max} \cdot d_i}, \quad (4.9)$$

де b_i - значимість отриманих результатів: b_1 - ступінь наукової новизни, b_2 - рівень теоретичної обґрунтованості, b_3 - ступінь експериментальної перевірки результатів.

Бальна оцінка отриманих результатів наведена в таблиці.

Максимальне значення отриманих результатів можна прийняти в межах 7…10 балів;

d_i - питома вага кожної характеристики, значення якої наведено в таблиці;

3 – кількість характеристик, за якими була зроблена оцінка результатів науково-дослідної роботи.

Таблиця 4.6 – Показники для оцінювання наукової значимості результатів виконання НДР

Характеристики	Питома вага характеристик	Бальна оцінка характеристик		
		Ступінь новизни b_1	Рівень теоретичної обґрунтованості b_2	Ступінь експериментальної перевірки результатів b_3
		1	3…5	7…10

	0,500	Часткове удосконалення виробів, технологій, матеріалів, програмного продукту, тощо	Суттєве удосконалення виробів, технологій, матеріалів, програмного продукту, тощо	Нові напрямки в розробці виробів, технологій, матеріалів, програмного продукту, тощо. Створення принципово нової техніки
	0,333	Позитивне рішення на основі зроблених узагальнень	Установлення залежностей, які використовувались в інших випадках	Відкриття нових шляхів рішення задачі
	0,167	Експериментальна перевірка не робилась	Результати перевірялись на невеликій кількості даних	Результати перевірені на великій кількості даних

Підставляючи числові дані $d_1 = 0{,}5$, $d_2 = 0{,}333$, $d_3 = 0{,}167$, $b_{\max} = 10$ у вираз () оцінимо наукову значимість отриманих результатів:

$$K_{ЗН} = \frac{3 \cdot 0{,}5 + 5 \cdot 0{,}333 + 9 \cdot 0{,}167}{3 \cdot 0{,}5 + 7 \cdot 0{,}333 + 10 \cdot 0{,}167} = 0{,}8 .$$

4.3 Внесок магістранта-дослідника в досягнення отриманих результатів НДР

Внесок дослідника в досягнення отриманих результатів НДР можна розрахувати за формулою [67]:

$$V = \frac{k_{TBI} \cdot З_i}{\sum_{1}^{n} k_{TBI} \cdot З_i}, \qquad (4.10)$$

де $k_{ТВІ}$ - коефіцієнт творчої участі кожного виконавця НДР, який оцінюється наступним чином: проведення досліджень – 3 бали, робоче проектування – 1,5 бали, освоєння – 1,0 бал.

Якщо виконавець приймав участь в декількох видах робіт, то береться сума відповідних балів;

$З_i$ - заробітна плата кожного виконавця НДР;

n - кількість всіх виконавців НДР.

Розраховуємо внесок дослідника:

$$V = \frac{3 \cdot 7200,00}{3 \cdot (8250,90 + 6500,00) + 1,5 \cdot (6300,00 + 5480,00) + 1,5 \cdot 4621,00} = 0,32$$

що загалом складає 32%

4.4 Висновки по четвертому розділу

Запланована науково-дослідна робота з проведення досліджень з керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах вимагає вкладення для проведення досліджень приблизно 396299,00 грн.

Отримані результати досліджень методу експлуатаційного керування інфокомунікаційними мережами мають високий рівень наукової значимості (в межах 0,80), що свідчить про доцільність проведення досліджень та високу значимість науково-дослідної роботи в технічному та економічному плані.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Забезпечення захисту працівників під час трудового процесу від небезпечних та шкідливих виробничих факторів, які справляють негативний вплив на здоров'я, життя та працездатність людини, гарантування належних умов праці є основними завданнями охорони праці, як складової безпеки життєдіяльності.

В даному розділі наводиться аналіз небезпечних, шкідливих [68] і уражаючих для людини і навколишнього середовища чинників, які утворюються при проведенні дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах. В ньому розглядаються, зокрема, технічні рішення з гігієни праці та виробничої санітарії, визначення допустимої сили струму в провіднику (антені), при якій напруженості ЕМВ на робочому місці знаходяться в межах норми, технічні рішення з промислової та пожежної безпеки під час проведення дослідження, безпека в надзвичайних ситуаціях.

5.1 Технічні рішення з гігієни праці та виробничої санітарії

5.1.1 Мікроклімат та склад повітря робочої зони

Визначаємо для приміщення для проведення дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах, категорію важкості робіт за фізичним навантаженням – легка Іб.

У відповідності із [69] допустимі параметри температури, відносної вологості та швидкості руху повітря у робочій зоні для теплого та холодного періодів року приведені у таблиці 5.1 додатку З.

При опроміненні менше 25% поверхні тіла людини, допустима інтенсивність теплового опромінення – 100 Вт/м^2.

Вміст шкідливих речовин в повітрі робочої зони не повинен перевищувати гранично допустимих концентрацій (ГДК) у повітрі робочої зони і підпадає під систематичний контроль для запобігання можливості перевищення ГДК, значення яких для роботи з ЕОМ наведено в таблиці З.2 додатку З.

При використанні ЕОМ джерелом зараження повітря є також іонізація молекул речовин, що містяться у повітрі. Рівні позитивних та негативних іонів мають відповідати [72] та наведені в таблиці З.3 додатку З.

З метою встановлення необхідних за нормативами параметрів мікроклімату та складу повітря робочої зони передбачено:

1) в приміщенні повинна бути встановлена система опалення для холодного і кондиціонування для теплого періодів року;

2) застосування вентиляції, яка видаляє забруднення або нагріте повітря з приміщення, а також за допомогою неї контролюється швидкість руху повітря і вологість.

5.1.2 Виробниче освітлення

Для забезпечення раціональних гігієнічних умов на робочих місцях значні вимоги пред'являються щодо кількісних та якісних показників освітлення.

З погляду задач зорової роботи в приміщенні, в якому проводиться робота з дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах, відповідно до [70] знаходимо, що вони відносяться до IV розряду зорових робіт. Вибираємо контраст об'єкта з фоном – великий та характеристику фону – середню, яким відповідає підрозряд зорових робіт *г*.

Нормовані значення коефіцієнта природного освітлення (КПО) та мінімальні значення освітленості для штучного освітлення приведені в таблиці З.4 додатку З.

Так як приміщення розташоване у м. Вінниця (2-га група забезпеченості природним світлом), а світлові пройми орієнтовані за азимутом 315°, то за таких умов КЕО визначатиметься за виразом [70, 71]

$$e_N = e_н m_N \, [\%], \tag{5.1}$$

де $e_н$ – табличне значення КЕО для бокового освітлення, %;

m_N – коефіцієнт світлового клімату;

N – порядковий номер групи забезпеченості природним світлом.

Підставляючи відомі значення одержимо нормовані значення КПО для бокового та суміщеного освітлення:

$$e_{N.б} = 1,5 \cdot 0,9 = 1,4\ (\%);$$
$$e_{N.с} = 0,9 \cdot 0,9 = 0,8\ (\%).$$

Для забезпечення нормативних значень показників освітлення передбачено:

1) за недостатнього природного освітлення у світлу пору доби доповнення штучним за допомогою газорозрядних ламп з утворенням системи суміщеного освітлення;

2) застосування загального штучного освітлення у темну пору доби.

5.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що при використанні пристроїв крім усього іншого устаткування використовується обладнання, робота якого генерує шум та вібрацію, потрібно передбачити шумовий та вібраційний захист.

Встановлено, що приміщення, в якому відбувається робота з дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах може містити робочі місця із шумом та вібрацією, що створюється вентиляторами блоку живлення ЕОМ і кулерами мікропроцесора, відеокарти.

З метою попередження травмування працюючих від дії шуму він підлягає нормуванню. Основним документом стосовно промислового шуму, що діє в Україні, є [72], згідно з яким допустимі рівні звукового тиску, рівні звуку та еквівалентні рівні шуму на робочих місцях в промислових приміщеннях не мають бути більшими ніж значення, що наведено у таблиці Х.5 додатку Х. Норми виробничих вібрацій наведені в таблиці Х.6 додатку Х для локальної вібрації.

З метою поліпшення віброакустичного клімату у приміщенні запропоновано:

1) постійне змащування підшипників вентиляторів блоку живлення комп’ютера і кулерів мікропроцесора та відеоадаптера;

2) передбачено використовувати в приміщені штори із щільної тканини.

5.1.4 Виробничі випромінювання

Проведений аналіз умов праці показав, що приміщення, в якому проводиться робота з дослідження може містити електромагнітні випромінювання.

Гранично допустимі рівні електромагнітних полів наведені в табл. 5.1.

Таблиця 5.1 – Гранично допустимі значення електромагнітних полів на робочих місцях згідно [81]

Параметри та одиниці вимірювання	Граничні значення в діапазонах частот					
	1-10 кГц	10-60 кГц	0,06-3 МГц	3-30 МГц	30-50 МГц	50-300 МГц
$E_{ГД}$, В/м	1000	700	500	300	80	
$ЕН_{Егд}$, $(В/м)^2 \cdot год$	120000	40000	20000	7000	800	
$H_{ГД}$, А/м	75	57	50	–	3,0	–
$ЕН_{Нгд}$, $(А/м)^2 \cdot год$	675	390	200	–	0,72	–

З метою забезпечення захисту та досягнення нормованих рівнів випромінювань потрібно застосовувати екранні фільтри та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

Виконати розрахунок допустимої сили струму в провіднику (антені) довжиною L = 4 м, при якій напруженість електромагнітного поля на робочому місці, віддаленому на r = 0,3 м, знаходиться в межах норми, якщо частота поля f = 35 МГц.

Допустиму силу струму в провіднику (антені) будемо визначати як найменшу із допустимих сил струму для джерел електричної та магнітної складових ЕМВ, відповідно

$$I = \min\{I_E, I_H\} \text{ [А]}, \qquad (5.2)$$

де I_E – допустима сила струму в провіднику (антені) для джерела електричного поля, А;

I_H – допустима сила струму в провіднику (антені) для джерела магнітного поля, А.

Біля джерела ЕМВ виділяють ближню зону (зону індукції), що знаходиться на відстані $r \le \lambda / 2\pi$, і далеку зону (зону випромінювання), для якої $r > \lambda / 2\pi$, де λ – довжина хвилі, м.

Довжину хвилі можна визначити за формулою

$$\lambda = \frac{c}{f} \text{ [м]}, \tag{5.3}$$

де c – швидкість світла в вакуумі, м/с ($c = 3 \cdot 10^8$ м/с);

f – частота електромагнітного поля, Гц.

Підставляючи відомі значення у формулу (5.3), одержимо:

$$\lambda = \frac{3 \cdot 10^8}{35 \cdot 10^6} = 8{,}57 \text{ (м)}.$$

Оскільки $r = 0{,}3$ м $< \lambda / 2\pi = 8{,}57 / 2\pi = 1{,}3646$ м, то допустиму силу струму I_E в провіднику (антені) для ближньої зони можна визначити з формули

$$E_{бл} = \frac{I_E L}{4\pi^2 f \varepsilon r^3} \text{ [В/м]} \tag{5.4}$$

звідки

$$I_E = \frac{E_{бл} 4\pi^2 f \varepsilon r^3}{L} \text{ [А]}, \tag{5.5}$$

де $E_{бл}$ – напруженість електричного поля для ближньої зони, В/м;

ε – діелектрична проникність середовища, Ф/м (для повітря $\varepsilon = 1$ Ф/м);

L – довжина провідника (антени), м.

Допустиму силу струму в провіднику (антені) від джерела магнітного поля для ближньої зони можна визначити з формули

$$H_{бл} = \frac{I_H L}{4\pi r^2} \text{ [А/м]}, \tag{5.6}$$

звідки

$$I_H = \frac{4\pi r^2 H_{бл}}{L} \text{ [А]}, \tag{5.7}$$

де $H_{бл}$ – напруженість магнітного поля ближньої зони, А/м;

r – віддаленість робочого місця, м;

L – довжина провідника (антени), м.

Для діапазону частот 30…50 МГц $E_{ГД}$ = 80 В/м, $H_{ГД}$ = 3 А/м.

Підставляючи відомі значення у формули (5.5, 5.7, 5.2), одержимо:

$$I_E = \frac{80 \cdot 4 \cdot 3{,}14^2 \cdot 35 \cdot 10^6 \cdot 1 \cdot 0{,}3^3}{4} = 745385760 \text{ (А)};$$

$$I_H = \frac{4 \cdot 3{,}14 \cdot 0{,}3^2 \cdot 3}{4} = 0{,}85 \text{ (А)};$$

$$I = \min\{745385760;\ 0{,}85\} = 0{,}85 \text{ (А)}.$$

Отже, допустима сила струму в провіднику (антені) в умовах дії ЕМВ складатиме 0,85 А.

5.2 Технічні рішення щодо промислової та пожежної безпеки під час проведення дослідження

На теперішньому етапі розвитку техніки, автоматизації розробок та досліджень широкого використання на робочому місці набули ЕОМ. Велика кількість прикладних програм перетворює ЕОМ на основне знаряддя праці радіоінженера.

5.2.1 Безпека щодо організації робочих місць

Оснащені відеодисплейним терміналом робочі місця зобов’язані розташовуватись на відстані не менше як 1,5 м від стіни з вікнами, від інших стін – на віддалі 1 м, одне від одного на відстані не менше ніж 1,5 м. У випадку розміщення робочих місць необхідно виключити ймовірність прямого засвічування екрану джерелом природного освітлення. Робоче місце раціонально розташовувати так, щоб природне світло падало на нього збоку, переважно з лівого [74].

Розташовувати відеодисплейний термінал на робочому місці необхідно так, щоб поверхня екрана має знаходитись на відстані 0,4-0,7 м від органів зору користувача. Висота робочої поверхні столу під час виконання роботи сидячи має налаштовуватись в межах 0,68-0,8 м. Робочий стіл повинен мати простір

для ніг висотою не менше 0,6 м, шириною не менше ніж 0,5 м, глибиною на рівні колін не менше 0,45 м та на рівні витягнутої ноги не менше ніж 0,65 м [75].

5.2.2 Електробезпека

Основними причинами ураження електричним струмом в цьому приміщенні можуть бути: робота під напругою під час проведення ремонтних робіт, несправність електрообладнання, випадковий дотик до металевих частин, що опинилися під напругою або струмоведучих частин. У відповідності до [76] це приміщення відноситься до приміщень із підвищеною небезпекою ураження електричним струмом в наслідок наявності високої (понад 75 %) відносної вологості. Через це безпека експлуатації електрообладнання має забезпечуватись рядом заходів, які включають використання ізоляції струмоведучих частин, захисного заземлення, захисних блокувань та ін [77].

5.2.3 Пожежна безпека

Відповідно до [78] приміщення, де проводиться робота з дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах, відноситься до категорії пожежної небезпеки Б. Дане приміщення відноситься до 2-го ступеня вогнестійкості, в якому приміщення знаходяться в будівлі з носійними та огороджувальними конструкціями з природних або штучних кам’яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості конструкцій розглядуваного приміщення наведені в табл. З.7. в табл. З.8 наведено протипожежні норми проектування будівель і споруд.

Встановлюємо, що приміщення, в якому проводиться робота з дослідження, має бути обладнане двома вогнегасниками, пожежним щитом, а також ємністю з піском [79].

5.3 Безпека у надзвичайних ситуацій. Дослідження стійкості роботи корпоративної інфокомунікаційної мережі в умовах дії загрозливих чинників надзвичайних ситуацій

Якщо через радіоелементи корпоративної інфокомунікаційної мережі проходить потік гамма-випромінювання в них з'являються вільні носії електричних зарядів, в результаті переміщення яких виникає хибний імпульс, що приводить до неправильної роботи пристрою.

При ядерному вибуху чи аварії на радіаційно-небезпечних об'єктах виникають іонізуюче та електромагнітне випромінювання. Іонізуюче випромінювання може вносити в матеріали зворотні та незворотні зміни.

Незворотні зміни в матеріалах викликаються порушенням структури кристалічної решітки речовини в наслідок виникнення дефектів, а також в результаті проходження різних фізико-хімічних процесів. Такими процесами є: радіаційний нагрів; окислювальні хімічні реакції, що призводять до окислення контактів; газовиділення і утворення пилоподібних продуктів, котрі можуть викликати вторинні фактори впливу.

В комп'ютерній апаратурі радіація викликає оборотні і необоротні процеси, внаслідок яких можуть бути порушення роботи елементів схеми, що приведе до пошкодження апаратури.

Якщо потік гамма-опромінення проходить через елементи КС, то в них виникають вільні носії електричних зарядів, внаслідок переміщення яких виникає хибний імпульс, який може призвести до включення пристрою.

Найбільш чутливі до дії радіації напівпровідники, оптичні прилади і фотоматеріали. В елементній базі мережі внаслідок дії іонізуючих випромінювань можлива зміна майже всіх електричних та експлуатаційних характеристик, залежних від проходження процесів іонізації і порушення структури матеріалів.

На утворення електромагнітних випромінювань витрачається невелика частина ядерної енергії, однак вони здатні викликати потужні імпульси у провідниках ліній зв'язку, сигналізації, керування, електропередачі, в антенах радіостанцій і т.д.

Вплив електромагнітного імпульсу може привести до згоряння чуттєвих електронних і електричних елементів, зв'язаних з великими антенами або відкритими проводами, а також до серйозних порушень у цифрових і контрольних пристроях, зазвичай без необоротних змін. Отже, вплив електромагнітних імпульсів (ЕМІ) необхідно враховувати для всіх електричних і електронних систем. Для найбільш важливих пристроїв треба застосовувати міри захисту і підвищувати їхню стійкість до ЕМІ.

Особливістю ЕМІ як вражаючого фактора є його здатність поширюватися на десятки і сотні кілометрів у навколишньому середовищі і по різних комунікаціях (мережам електропостачання і кабельними зв'язкам і т.д.). Тому електромагнітні випромінювання можуть мати вплив там, де ударна хвиля, світлове випромінювання і проникаюча радіація втрачають своє значення як вражаючі фактори.

5.3.1 Дослідження стійкості роботи корпоративної інфокомунікаційної мережі в умовах дії іонізуючих випромінювань

За критерій стійкості роботи РЕС приймають такі максимальні значення рівня радіації, або дози опромінення, при яких РЕС буде ще працювати з потрібною якістю.

Дослідження стійкості роботи корпоративної інфокомунікаційної мережі ведеться у такій послідовності:

1. Аналізується елементна база.

2. По табличним даним для кожного елементу визначаються $Д_{гр}$ які заносяться до табл. 5.2.

Таблиця 5.2

Блоки	Елементна база	$Д_{грі}$ (Р)	$Д_{гр}$ (Р)
Блок живлення	Транзистор КП350 Б	10^4	10^4
	Мікросхема ML700IGM	10^5	
	Конденсатор керамічний	10^6	
Приймально-передавальний блок	Мікросхема NXP H788	10^4	
	Кварцовий резонатор ТХС	10^{10}	

3. По мінімальному значенню $Д_{гр}$ визначається границя стійкості роботи апаратури у цілому в нашому випадку $Д_{гр}=10^4$ Р.

Врахувавши рівень захищеності апаратури:

$$Д_{гр.к}=Д_{гр}\cdot К_{посл.}=10^4\cdot 4 = 4\cdot 10^4 \text{ Р}.$$

4. Визначається час нормального функціонування приладу в заражені зоні за формулою:

$$t_к=t_р+t_п=6144+1=6145 \text{ год}.$$

Можлива доза опромінення при використанні приладу на зараженій території визначається за формулою:

$$Д_М = \frac{2 \cdot P_1 \cdot (\sqrt{t_к} - \sqrt{t_п})}{K_{осл}} \cdot , \quad (5.8)$$

Де $t_к$, $t_п$ – час початку і кінця знаходження приладу на зараженій території, год.

P_1 – рівень радіації через одну годину після зараження, Р/год.

Тоді

$$Д_М = \frac{2 \cdot 3{,}3 \cdot (\sqrt{6145} - \sqrt{1})}{4} = 127{,}7\ Р. \cdot$$

Допустимий час стійкої роботи:

$$t_к = t_д = \left(\frac{Д_{гр.\min} \cdot K_{посл} + 2 \cdot p_{1.\max} \cdot \sqrt{t_п}}{2 p_{1.\max}} \right)^2 = \left(\frac{10^4 \cdot 4 + 2 \cdot 3{,}3 \cdot \sqrt{1}}{2 \cdot 3{,}3} \right)^2 = 10^8\ год.$$

Отже, порівнявши $Д_{гр}$ та $Д_м$ можна зробити висновок: корпоративна інфокомунікаційна мережа може надійно працювати на зараженій території, в приміщенні з коефіцієнтом ослаблення $К_{осл}$=4, так як границя стійкості роботи мережі перевищує його можливу дозу опромінення.

5.3.2 Дослідження стійкості роботи корпоративної інфокомунікаційної мережі в умовах дії електромагнітного імпульсу

За критерій стійкості роботи системи в цих умовах береться коефіцієнт безпеки:

$$K_Б = 20 \cdot \lg \frac{U_Д}{U_В} \geq 40\ [дБ]; \quad (5.9)$$

де $U_Д$ - допустиме коливання напруги живлення;

$U_В$ - напруги наведення в вертикальних струмоведучих частинах.

Початковими даними для оцінки стійкості є вертикальна складова напруженості електромагнітного поля:

$E_в$=10,17 (кВ/м);

Напруги живлення :

$U_ж$=5 (В) ;

Послідовність оцінки:

Визначається горизонтальна складова напруженості електромагнітного поля:

$$E_Г = 10^{-3} \cdot E_В = 10^{-3} \cdot 10{,}17 \cdot 10^3 = 10{,}17 \text{ (В/м)};$$

На друкованій платі визначаються максимальні довжини струмопровідних частин: $l_{В1} = 1{,}8$ м, $l_{Г1} = 1{,}2$ м.

Напруги наведення в вертикальних і горизонтальних струмопровідних частинах:

$$U_{В1} = E_Г \cdot l_В = 10{,}17 \cdot 10^3 \cdot 1{,}8 = 18{,}306 \text{ (В)};$$

$$U_{Г1} = E_{В1} \cdot l_Г = 10{,}17 \cdot 1{,}2 = 12{,}204 \text{ (В)};$$

Допустиме коливання напруги живлення:

$$U_Д = U_Ж + \frac{U_Ж \cdot N}{100} = 5 + \frac{5}{100} \cdot 5 = 5{,}25\,(В);$$

де N - відсоток відхилення.

По формулі (5.2) визначаємо коефіцієнти безпеки:

$$K_{БВ1} = 20 \cdot \lg \frac{U_Д}{U_{В1}} = 20 \cdot \lg \frac{5{,}25}{18{,}306} = 3{,}27 \le 40\,(дБ);$$

$$K_{БГ1} = 20 \cdot \lg \frac{U_Д}{U_{Г1}} = 20 \cdot \lg \frac{5{,}25}{12{,}204} = 66{,}79 \ge 40\,(дБ);$$

В нашому випадку $K_{БВ1} < 40$ дБ, отже апаратура нестійка до впливу електромагнітного імпульсу, і потрібно вжити заходи по підвищенню її надійності, а саме забезпечити екранування приладу.

Розрахунок захисного екрану проводиться у такому порядку: Визначається перехідне гасіння енергії електромагнітного поля екраном (А, дБ). У якості екрану використовуємо корпус пристрою який виконаний із сталі:

$$A = 5{,}02 \cdot t \cdot \sqrt{f}\ [дБ] \qquad (5.10)$$

де *t*- товщина стінки екрану

f – частота f=15000 Гц

Знаходимо товщину екрану:

$$t = \frac{36{,}7}{5{,}02 \cdot \sqrt{15000}} = 0{,}06 \text{ см.}$$

Необхідне перехідне гасіння енергії

$$А_{необ}=40-К_{БВ1}=40-3,3=36,7 \text{ дБ}.$$

Враховуючи конструктивну особливість пристроїв корпоративної інфокомунікаційної мережі, а саме те що його корпус виготовлено зі сталі, встановлення додаткового екранування не є доцільним так як функцію екрана виконує корпус товщиною 1 мм.

Тоді перехідне гасіння енергії яке буде чинити сталевий екран:

$$А=5,2\ 0,1\ \sqrt{15000}=63,6 \text{ (дБ)};$$

5.4 Висновки до розділу

В результаті виконання цього розділу було розглянуто такі питання охорони праці та безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення допустимої сили струму в провіднику (антені), при якій напруженості ЕМВ на робочому місці знаходяться в межах норми, технічні рішення з промислової та пожежної безпеки під час проведення дослідження безпеки мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах, безпека у надзвичайних ситуаціях.

А також нами було оцінено роботу інформаційно-корпоративної інфокомунікаційної мережі в умовах дії іонізуючого та електромагнітного імпульсу та одержано наступні результати. Інформаційна мережа може надійно працювати на території зараженій іонізуючим випромінюванням при рівні радіації 127,7 Р/год., а також стійко переносити електромагнітний імпульс напруженістю 2 кВ/м, за умови використання екрануючого пристрою.

ВИСНОВОК

В магістерській роботі отримано рішення актуального завдання по розробленню алгоритму і заснованої на ньому системи управління безпекою МАП, що базуються на запропонованій формальній моделі безпеки МАП, в сукупності дозволяють підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних інфокомунікаційних мереж з різними вимогами по захищеності при використанні єдиного МАП за рахунок обліку атрибутів доступу, включаючи розташування МАП, вимог за якістю наданих послуг, а також політик безпеки захищеності корпоративних мереж.

Новизна запропонованого підходу полягає в розробці та обґрунтуванні коректності формальної моделі безпеки МАП, що відрізняється від відомих урахуванням оцінки його місцезнаходження в спеціальному приміщенні, інших атрибутів доступу, а також реалізацією вимог мандатної і рольової політик безпеки в корпоративних мережах з різними вимогами щодо єдиного МАП і розробці на базі даної моделі нового алгоритму управління небезпекою МАП, що відрізняється від відомих визначенням оптимальної, з точки зору забезпечення до конфіденціальності інформації і якості що представляють користувачу послуги, програмно-апаратної конфігурації МАП.

В рамках проведення досліджень були отримані наступні результати:

1) проведено аналіз стану наукових досліджень і технічних рішень в області захисту інформації при використанні МАП, виявлені недостатки сучасних формальних моделей безпеки комп'ютерних систем стосовно забезпеченняд безпеки інформації при використанні МАП, включаючи існуючі технічні та програмно-апаратні рішення; для рішення завдання віддаленого управління, а також сполучення контурів обробки інформації з різними вимогами по захищеності в сучасних МАП пропонується використовувати агентно-орієнтований підхід, який є елементом штучного інтелекту і побудований на основі клієнт-серверної архітектури;

2) вдосконалена модель безпеки МАП, що відрізняється від відомих вчених його місцезнаходження в корпоративних мережах з різними вимогами по захищеності; обгрунтований вибір технологій, на основі яких доцільна побудова системи визначення місця розташування МАП, а також запропонований підхід, що дозволяє підвищити достовірність визначення місцезнаходження МАП спеціальних приміщеннях; здійснено апробацію

моделі за допомогою іміта-ційного моделювання, а також проведена всебічна оцінка її якості, що включає в себе перевірку адекватності, чутливості і стійкості; отримані оцінки параметрів приватних моделей, які впливають на достовірність визначення місця розташування МАП;

3) вдосконалений алгоритм управління безпекою МАП, що враховує атрибути доступу мобільних користувачів; описана оптимізаційна задача, яка вирішується в алгоритмі і охарактеризована як задача багатокритеріальної оптимізації цілочисленного динамічного програмування; представлено описання циклу управління конфігурацією МАП з рівняннями стану і спостереження, обгрунтуванням мети управління; описані основні процедури, що входять до складу алгоритму; досліджено основні властивості алгоритму і його процедур, включаючи тимчасову складність, складність по пам'яті і точність. Отримано їх чисельні оцінки, а також представлений чисельний приклад роботи алгоритму;

4) сформовані науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах з різними формами і вимогами щодо захищеності; проведена група експериментів і обгрунтувати вибір оптимальних параметрів підсистеми визначення місця розташування; здійснено комплексну оцінку ефективності розроблених пропозицій з отриманням чисельних значень для оцінки часу, необхідного для зміни конфігурації МАП, ймовірності загрози порушення конфіденційності при використанні керованих МАП, ресурсоємності запропонованої системи управління безпекою МАП, своєчасності доступу до послуг; отримана чисельна оцінка ступеня досягнення мети магістерського дослідження, яка дозволяє стверджувати те, що мета досягнута.

Магістерська відповідає пунктам "2. Методи, апаратно-програмні та організаційні засоби захисту систем (об'єктів) формування та надання користувачам інформаційних ресурсів різного виду.", "8. Моделі протидії загрозам порушення інформаційної безпеки для будь-якого виду інформаційних систем.", " 13. Принципи та рішення (технічні, математичні, організаційні та ін.) зі створення нових і вдосконалення суспільством засобів захисту інформації та забезпечення інформаційної небезпеки. " паспорта наукової спеціальності 05.13.19 "Методи і системи захисту інформації, інформаційна безпека" (технічні науки).

Напрямком подальших досліджень вважаєм

– дослідження перспективних технологій визначення місцерозположення користувачів МАП в приміщеннях всередині будівлі з метою зниження помилок;

– дослідження технологій агентно-орієнтованого підходу для оптимізації інформаційної взаємодії контролерів бездротових мереж з передачі керуючої інформації;

– вдосконалення підходів щодо управління конфігурацією сучасних мобільних пристроїв з метою створення можливості реалізації розробити конструкцію працьованих підходів щодо управління доступом стосовно до послуг, що використовують конфіденційні відомості.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вишнякова, О. А. Математическая модель обнаружения точки беспроводного доступа по измерениям можности излучения разнесенными наблюдателями / О. А. Вишнякова, Д. Н. Лавров, С. Ю. Лаврова // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. – Омск : Изд-во ОмГУ. – 2013. – No 2(28). – С.49–59.

2. Вопросы безопасности мобильных устройств / А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский // Безопасность информационных технологий Москва : Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации, 2012. – С. 5–7.

3. Ворошилин, Е. П. Моделирование процессов и явлений в системах святи : методическое пособие для самостоятельной работы магистров направления 210700.68 "Инфокоммуникационные технологии и системы связи" / Е. П. Ворошили // ТУСУР, 2012.

4. Выборнов, О. В. Прогнозирование потенциальной нагрузки секторов сетей широкополосного доступа на основе анализа отношения сигнал/помеха с использованием геоинформационных технологий / О .В. Выборнов, А. М. Измайлов, С. В. Козлов, В Н. Лаврушев, Е. А. Спирина // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2013. – Выпуск No 4. – С. 130–135.

5. Выборнов, О. В. Тестирование ЭМС оборудования стандарта 802.11n фирмы InfiNet / О. В. Выборнов, А. М. Измайлов, С. В. Козлов, Е. А. Спирина // Вестник КГТУ им. А. Н. Туполева. – 2012. – Выпуск No 2 (68). – С. 160–163.

6. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978-5-9912-0328-9.

7. Десницкий, В. А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления : автореф. дис. ... канд. техн.. наук : 05.13.19 / Десницкий Василий Алексеевич ; [Санкт-Петербургский ин-т информатики и автоматизации РАН]. – Санкт-Петербург, 2013. – 22 с. – Библиогр.: с. 21–22.

8. Маркин, Д. О. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 9. – С. 39–50.

9. Маркин, Д. О. Исследование эффективности алгоритмов определения

местоположения мобильных устройств внутри помещений / Д. О. Маркин // Вестник РГРТУ. – 2015. – No 54-1. – С. 32–39.

10. Маркин, Д. О. Методика обнаружения и способы противодействия распределенной атаке типа "отказ в обслуживании", основанной на использовании SEO-технологий / Д. О. Маркин, М. А. Сазонов // Информация и безопасность. – 2014. – No 2 (7) – С.208–211.

11. Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – No 4 (22). – С. 21–31.

12. Маркин, Д. О. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 10. – С. 40–51.

13. Маркин, Д.О. Модель доступа к информационным системам / Д. О. Маркин, М. А. Сазонов // Телекоммуникации. – 2013. – No 9. – С. 27–31.

14. Маркин, Д.О. Модель и алгоритм адаптивного управления профілем защиты мобильного устройства / Д. О. Маркин, В. В. Комашинский // XII Всероссийское совещание по проблемам управления ВСПУ-2014. Москва, 16-19 июня 2014 г. : Труды. [Электронный ресурс] Москва : Институт проблем управления им. В. А. Трапезникова РАН, 2014. 9616 с. Электрон. текстовые дан. (1074 файл.: 537 МБ). 1 электрон. опт. диск (DVD-ROM). Файл 7449. ISBN 978-5-91450-151-5.

15. Маркин, Д. О. Модель определения местоположения пользователей мобильных устройств внутри помещений на основе сигналов беспроводной сети доступа / Д. О. Маркин, В. В. Комашинский // Перспективные информационные технологии (ПИТ 2015), Том 2: труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2015. – С. 305–309. ISBN 978-5-93424-735-6.

16. Маркин, Д. О. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний / Д. О. Маркин, С. М. Макеев // Известия Тульского государственного университета. Технические науки. – 2016. – No 2. – С. 150–165.

17. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции [Текст] + [Электронный

ресурс] / под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2016. – С. 105–110. ISBN 978-5-89838-886-10.

18. Xin Jin RABAC: Role-Centric Attribute-Based Access Control / Xin Jin, Ravi Sandhu, Ram Krishnan // In MMM-ACNS. – 2012.

19. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978- 5-9912-0328-9.

20. Десницкий, В. А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления : автореф. дис. канд. техн.. наук : 05.13.19 / Десницкий Василий Алексеевич ; [Санкт-Петербургский ин-т информатики и автоматизации РАН]. – Санкт-Петербург, 2013. – 22 с. – Библиогр.: с. 21– 22.

21. Озарнов, И. Интеграция сервисов идентификации и контроля доступа. Решение Cisco Identity Services Engine (ISE) / И. Озарнов, Г. Симонов : Презентация доклада, 2012. – 47 с.

22. Салех, Х. М. Мобильные системы предоставления информационных сервисом позиционирования объектов : автореф. дис. ... канд. техн. наук : 05.13.01 / Салех Хади Мухаммед; [Владимирский гос. ун-т]. – Владимир, 2013. – 20 с. – Библиогр.: с. 19–20

23. Сидак, А. А. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи /А. А. Сидак, А. В. Ильин, А. В. Кубарев, // Вопросы кибербезопасности. – 2014. – № 3 (4). – С. 29–34.

24. Чернов, Д. В. О моделях логического управления доступом на основе атрибутов // Математические основы компьютерной безопасности. – 2012. – № 3 (17). – С. 79–82.

25. ViPNet Client для iOS и Android / ОАО "ИнфоТеКС [Електронний ресурс]. – 2019. – Режим доступу: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=2870.

26. ViPNet Terminal / ОАО "ИнфоТеКС" [Електронний ресурс]. – 2019. – Режим доступу: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=5521.

27. Real Time Location System (RTLS) RFID-over-Wi-Fi Technology | Ekahau / Inc. Ekahau // Ekahau [Електронний ресурс]. – 2019. – Режим доступу: http://www.ekahau.com/real-time-location-system/technology.

28. Hur, J. Attribute-based access control with efficient revocation in data outsourcing systems / J. Hur, D.K. Noh // IEEE Trans. Parallel Distrib. Syst. – 2011. № 22 (7). – P. 1214–1221.

29. Hybrid WSN and RFID indoor positioning and tracking system / Zhoubing

Xiong1, Zhenyu Song1, Andrea Scalera2, Enrico Ferrera2, Francesco Sottile2, Paolo Brizzi2, Riccardo Tomasi2, Maurizio A Spirito2 // EURASIP Journal on Embedded Systems [Електронний ресурс]. – 2019. – Режим доступу: http://jes.eurasipjournals.com/content/2013/1/6.

30. IEEE 802.11, The Working Group Setting the Standards for Wireless / The Institute of Electrical and Electronics Engineers : [Електронний ресурс]. – 2019. – Режим доступу: http://www.ieee802.org/11/.

31. Google Tango Project / Google Inc. [Електронний ресурс]. – 2019. – Режим доступу: https://get.google.com/tango/.

32. Талисман 395 – защищённый телефон стандарта GSM / СовТехКом Ин- формационная безопасность [Електронний ресурс]. – 2019. – Режим доступу: http://www.sovtechcom.ru/product/talisman-395.html.

33. Специальный микросотовый телефон М-549М / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_24.htm.

34. Специальный сотовый телефон SMP-АТЛАС/2 / ФГУП "НТЦ "АТ-ЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_17.htm.

35. Система однонаправленной передачи данных ДИ-ОД / АО ЦНИИ ЭИСУ [Електронний ресурс]. – 2019. – Режим доступу: [Електронний ресурс]. – 2019. – Режим доступу: http://cniieisu.ru/index.php/produsti-i-uslugi/17-produkciya/apparatnoe-obes-pechenie/odnonapravlennyj-informatsion nyj-shlyuz-di-od.

36. Специализированный терминал мобильной связи (СТМС) "Сапфир-К" / НИИ Автоматики Сапфир-К [Електронний ресурс]. – 2019. – Режим доступу: http://niia.ru/document/sapfir.htm.

37. Однонаправленный шлюз "Атликс-Шлюз-К" / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_26.htm.

38. Мобильный вычислительный комплекс "ИНФОПРО" МВК-2 / ЗАО "Инфопро" [Електронний ресурс]. – 2019. – Режим доступу: http://www.infopro.ru/vt.php?id=48.

39. Мобильное защищенное автоматизированное рабочее место доступа в сеть Интернет / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_27.htm.

40. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII

Всероссийской научно-практической конференции / под ред. О.М. Голембиовской, М.Ю

41. Континент Т-10 / Код безопасности [Електронний ресурс]. – 2019. – Режим доступу: http://securitycode.ru/products/kontinent_t_10/.

42. Крипто БД: защита баз данных Oracle // ООО "Алладин Р.Д." [Електронний ресурс]. – 2019. – Режим доступу: https://www.aladdin-rd.ru/catalog/cryptobd/.

43. КАМИ-Терминал / Научно-технический центр КАМИ [Електронний ресурс]. – 2019. – Режим доступу: http://www.kami.ru/ Solutions/КАМИ-Терминал.

44. Инструмент имитационного моделирования AnyLogic [Електронний ресурс]. – 2019. – Режим доступу: http://www.anylogic.ru /overview.

45. Заяц, А. Обзор и тестирование смартфона Caesar A9600, а также знаком- ство с MT6589 - четырехядерной SoC MediaTek для бюджетных решений [Електронний ресурс]. – 2019. – Режим доступу: http://ixbt.com/md/pda/.

46. Аппаратура 605 / ОАО "Концерн "Автоматика" [Електронний ресурс]. – 2019. – Режим доступу: http://oaoka.ru/Vremennyj_katalog /Zacshicshennye_telefonnye_apparaty/Apparatura_605.htm.

47. Артамонов, В. А. Безопасность мобильных устройств, систем и приложений // Проект ИТ-защита [Електронний ресурс]. – 2019. – Режим доступу: http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_ Artamonov.pdf.

48. Методичні рекомендації з комерціалізації розробок, створених в результаті науково-технічної діяльності – К.: Наказ Державного комітету України з питань науки, інновацій та інформатики (Лист № 1/06-4-97 від 13.09.2010 р.).

49. Козловський В. О. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт. – Вінниця: ВНТУ, 2012.

50. Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 75 с.

51. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

52. Правила улаштування електроустановок. 2-е вид., перероб. і доп. – Х: "Форт", 2009. – 736 с.

53. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.

54. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.

55. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.

56. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

57. Норми радіаційної безпеки України (НРБУ-97), МОЗ України. – К., 1997.

58. Методичні вказівки до виконання студентами-магістрантами наукового напрямку економічної частини магістерських кваліфікаційних робіт / Уклад. В.О. Козловський – Вінниця: ВНТУ, 2012. – 22 с.

59. Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – Вінниця : ВДТУ, 2003. – 75с.

60. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.

61. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

62. ДБН В.2.5-28-2006. Природне і штучне освітлення.

63. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.

64. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

65. ДСН 3.3.6.039-99. Державні санітарні норми виробничої та загальної вібрацій.

66. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.

67. Березюк О. В. Охорона праці. Підсумкова державна атестація спеціалістів, магістрів в галузях електроніки, радіотехніки, радіоелектронних апаратів та зв’язку : навчальний посібник / О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2017. – 104 с.

68. Правила улаштування електроустановок. 2-е вид., перероб. і доп. – Х: "Форт", 2009. – 736 с.

69. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.

70. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.

71. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.

72. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

73. ДСанПіН 3.3.6-096-2002. Державні санітарні норми і правила при

роботі з джерелами електромагнітних полів.

74. Палагнюк Д. М. Моніторинг за збором відходів на базі ps технологій / Д. М. Палагнюк, О. В. Березюк // Матеріали II Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання“, 25-26 квітня 2019. — Т. : ТНТУ, 2019. — С. 100–101.

75. Палагнюк Д. М. Принципи забезпечення інформаційної безпеки / Д. М. Палагнюк, О. В. Березюк, Д. С. Тищук, // Матеріали науково-практичної конференції "Якість і безпека. Сучасні реалії", 14-15 березня 2018 р. – Вінниця : ВНТУ, 2018. – С. 19-22.

76. Бєлов В. С. Самоорганізація безпровідної сенсорної Mesh-мережі / В. С. Бєлов, Д. М. Палагнюк // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2018/paper/view/4505.

77. Палагнюк Д. М. Інфокомунікаційні мережі на основі SHDSL технології / Д. М. Палагнюк, М. В. Васильківський // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2831.

78. Палагнюк Д. М. Еволюція стандартів IEEE802.11x / Д. М. Палагнюк, В. С. Бєлов // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2569.

79. Палагнюк Д. М. Система дистанційного моніторингу / Д. М. Палагнюк, С. Т. Барась // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2018/paper/view/5405.

80. Палагнюк Д. М. Оптичні цифрові елементи обробки сигналів / Д. М. Палагнюк, О. О. Якімцев, О. О. Дрючин // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2018/paper/view/5219.

81. Палагнюк Д. М. Використання dp-qpsk модуляції в когерентних восп / Д. М. Палагнюк, М. В. Васильківський // Матеріали XLVI науково-технічної конференції підрозділів ВНТУ, Вінниця, 22-24 березня 2017 р. Режим доступу : https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/3130.

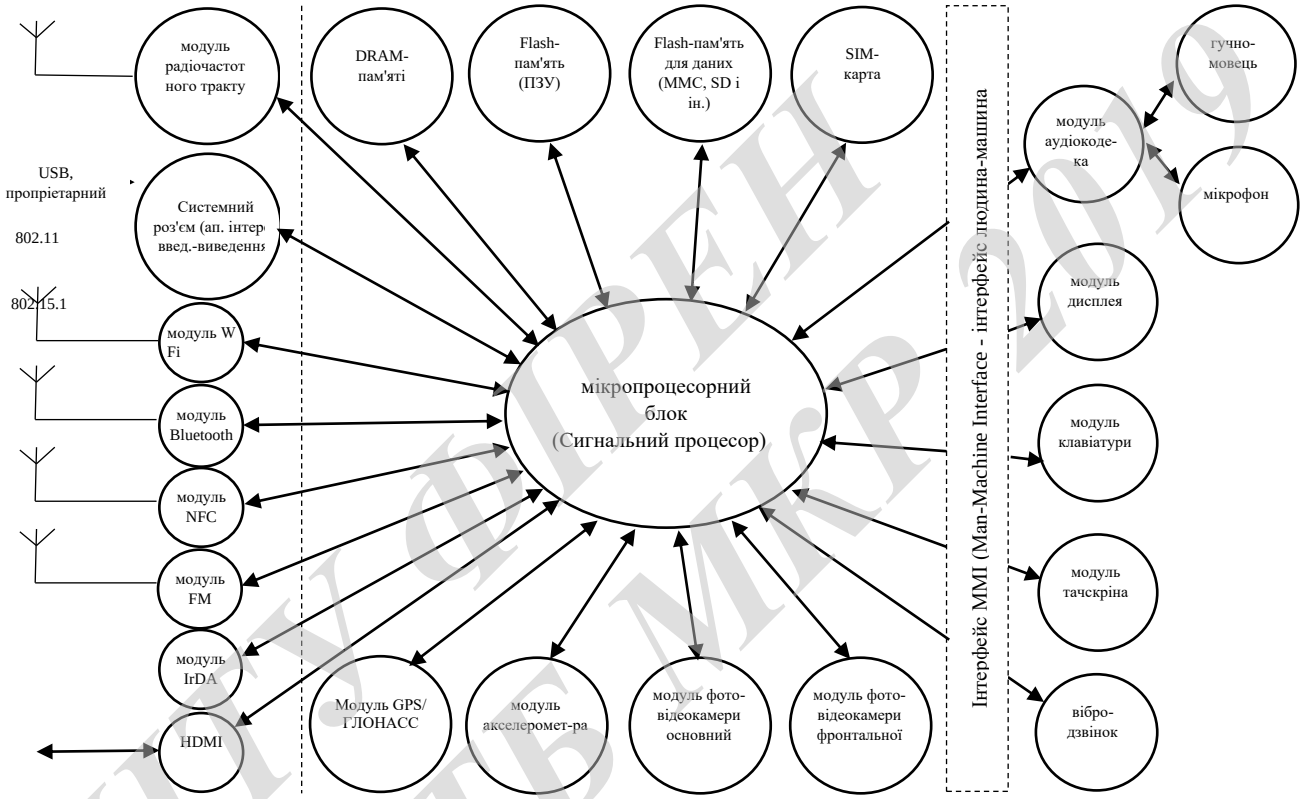
ДОДАТКИ

Додаток А
(обов’язковий)

Технічне завдання

Додаток Б
(обов’язковий)

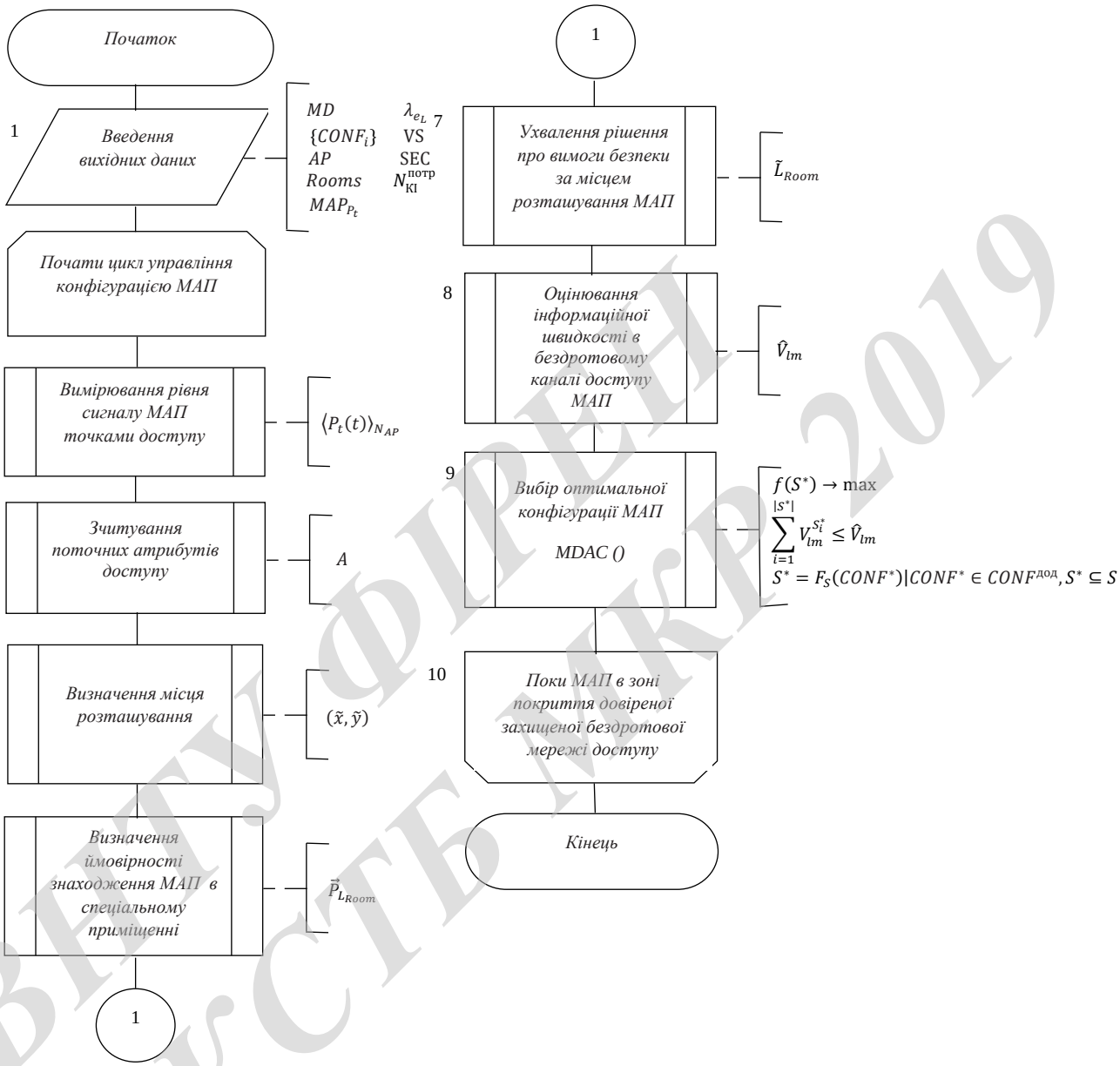
Типовий склад сучасного МАП



					08-34. МКР.008.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Палагнюк Д.М.			Типовий склад сучасного МАП	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

Додаток В
(обов’язковий)

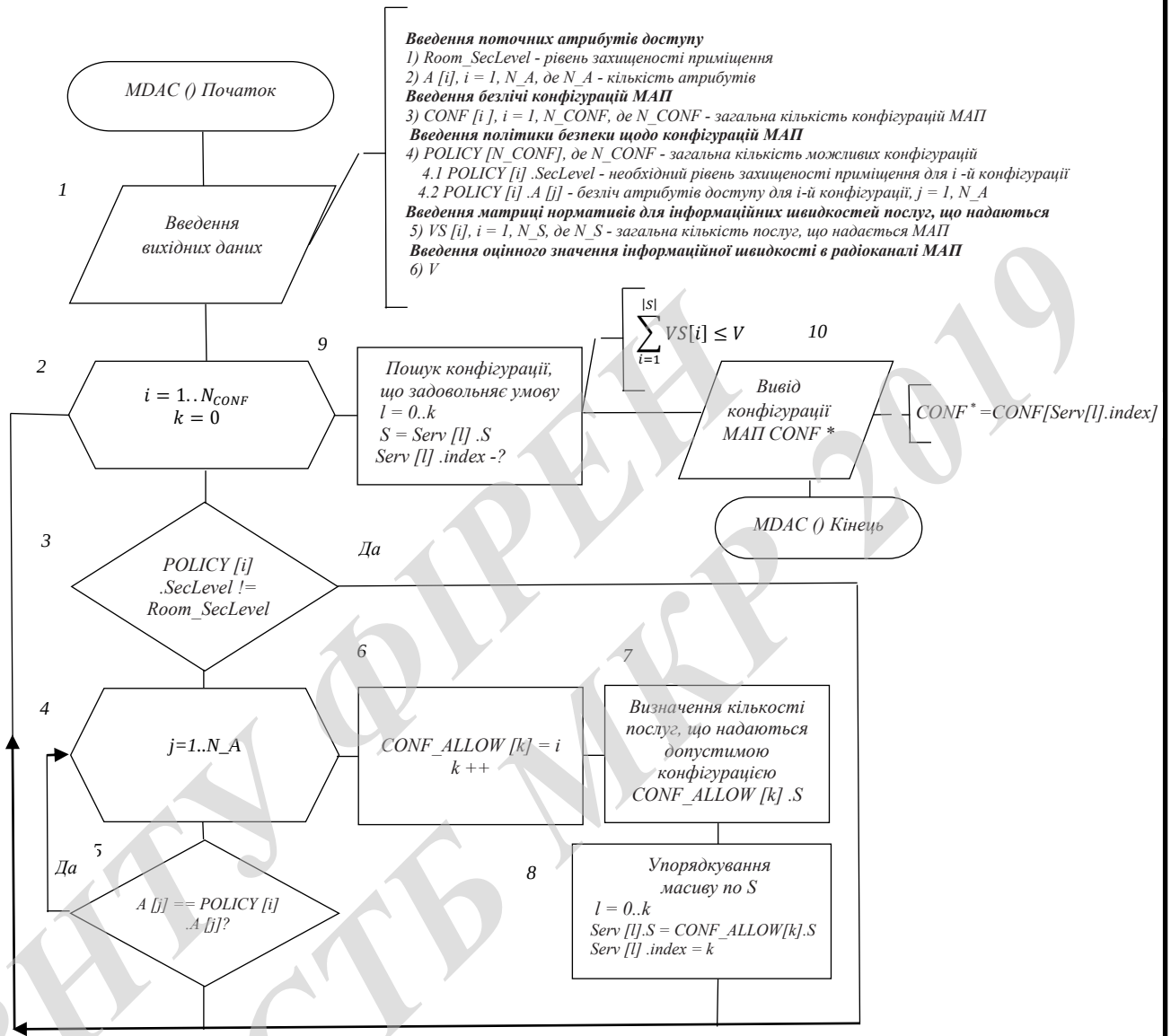
Узагальнена блок-схема алгоритму управління безпекою МАП



					08-34. МКР.008.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Палагнюк Д.М.			Узагальнена блок-схема алгоритму управління безпекою МАП	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

Додаток Г
(обов’язковий)

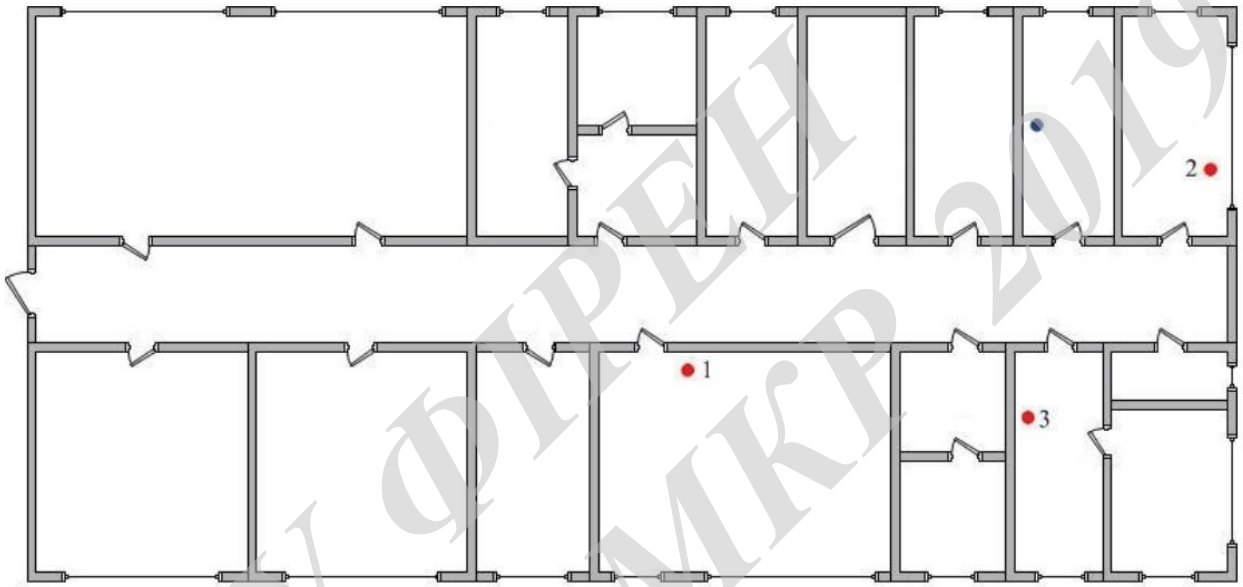
Блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП



					08-34. МКР.008.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Палагнюк Д.М.			Блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

Додаток Д
(обов’язковий)

Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу

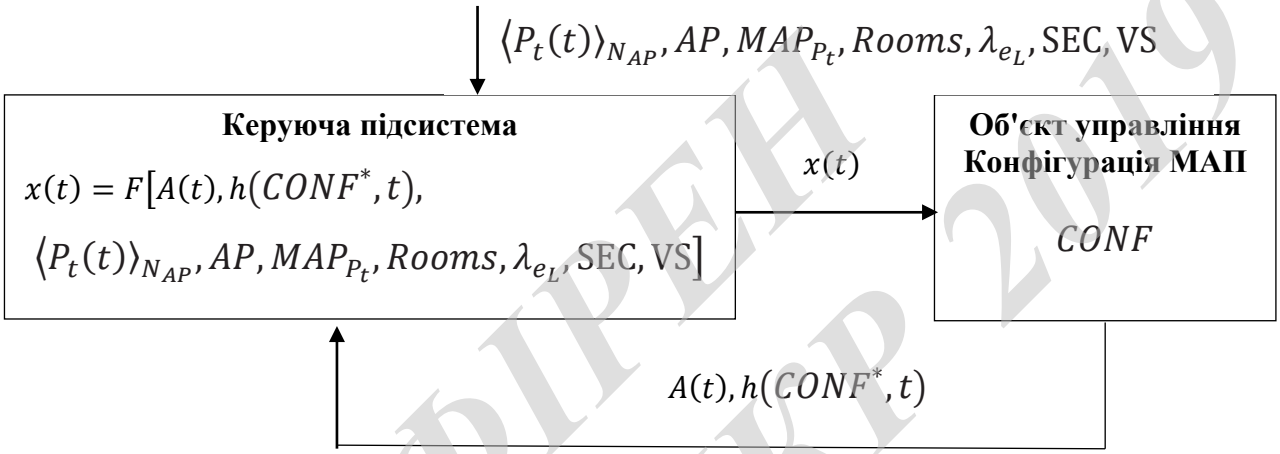


- базові станції
- точка вимірювання рівня сигналу

					08-34. МКР.008.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Палагнюк Д.М.			Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

Додаток Е
(обов’язковий)

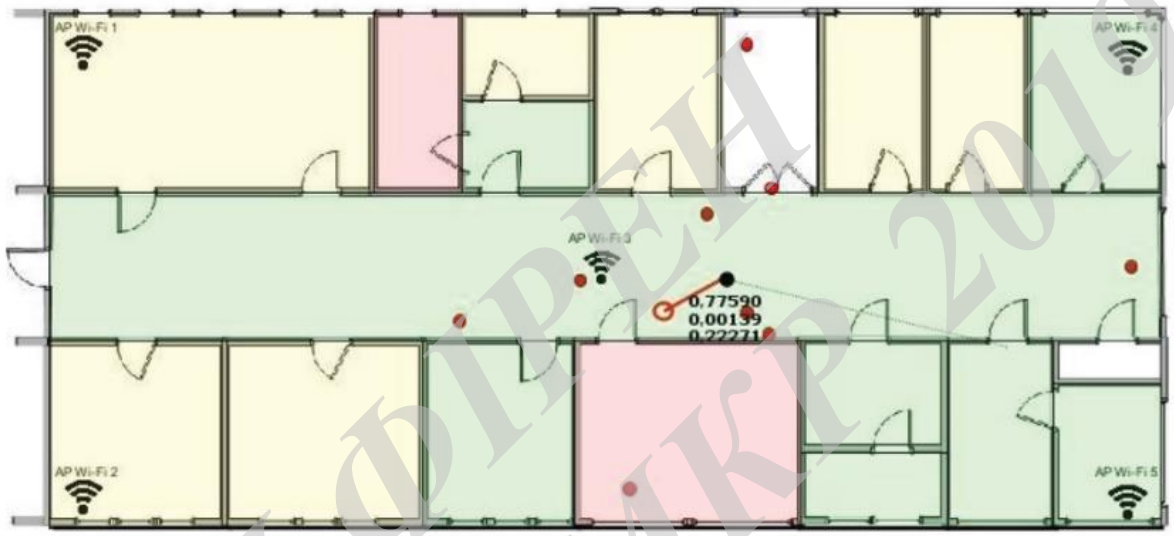
Схема управління конфігурацією МАП



					08-34. МКР.008.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Палагнюк Д.М.			Схема управління конфігурацією МАП	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

Додаток Є
(обов’язковий)

Схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення



					08-34. МКР.008.00.000 Е8			
Змн.	Лист	№ докум.	Підпис	Дата				
Розроб.		Палагнюк Д.М.			Схема оптимального розташування п'яти точок доступу на досліджуваній схемі з мінімальною помилкою	Літ.	Арк.	Аркушів
Перевір.		Городецька О.С.					1	1
Реценз.		Тимчик С.В.				ВНТУ, гр. ТКС-18м		
Н. Контр.		Городецька О.С.						
Затверд.		Бортник Г.Г.						

Додаток З

Допустимі значення виробничих факторів

Таблиця 3.1 – Допустимі показники мікроклімату

Період року	Категорія робіт	Температура повітря, °С для робочих місць		Відносна вологість повітря, %	Швидкість руху повітря, м/с
		постійних	непостійних		
Холодний	Іб	20-24	17-25	75	≤0,2
Теплий		21-28	19-30	60 при 27°С	0,1-0,3

Таблиця 3.2 – ГДК шкідливих речовин [71]

Назва шкідливої речовини	ГДК, мг/м^3	Агрегатний стан	Клас небезпеки
Озон	0,1	Пара	4
Оксиди азоту	5	Пара	2
Пил	4	Аерозоль	2

Таблиця 3.3 – Кількість іонів в 1 см^3 повітря приміщення під час роботи на ЕОМ

Рівні	Мінімально необхідні	Оптимальні	Максимально допустимі
позитивний	400	1500-3000	50000
негативний	600	3000-5000	50000

Таблиця 3.4 – Нормовані значення коефіцієнта природного освітлення і мінімальні освітленості для штучного освітлення

Характеристика зорової роботи	Найменший розмір об’єкта розрізнення, мм	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об’єкта розрізнення з фоном	Характеристика фону	Освітленість при штучному освітленні, лк			КПО для бокового освітлення, %	
						комбіноване		загальне	Природного	Суміщеного
						всього	у т. ч. від загального			
Середньої точності	0,5-1	IV	г	великий	середній	300	150	150	1,5	0,9

Таблиця 3.5 – Допустимі рівні шуму і еквівалентні рівні звуку

Рівні звукового тиску в дБ в октавних полосах із середньо-геометричними частотами, Гц									Рівні звуку та еквівалентні рівні звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

Таблиця 3.6 – Допустимі рівні вібрації [73]

Гранично допустимі рівні віброприскорення, дБ, в октавних полосах із середньо-геометричними частотами, Гц								Коректовані рівні віброприскорення, дБА
8	16	31,5	63	125	250	500	1000	
73	73	79	85	91	97	103	109	76

Таблиця 3.7 – Мінімальні межі вогнестійкості приміщення [78]

Ступінь вогнестійкості будівлі	Стіни				Колони	Східчасті майданчики	Плити та інші несійні конструкції	Елементи покриття	
	Несійні та східчасті клітки	Самоносійні	Зовнішні несійні	Перегородки				Плити, прогони	Балки, ферми
2	REI 120 М0	REI 60 М0	Е 15 М0	EI 15 М0	R 120 М0	R 60 М0	REI 45 М0	REI 15 М0	R 30 М0

Примітка. R – втрати несійної здатності; Е – втрати цілісності; І – втрати теплоізолювальної спроможності; М – показник здатності будівельної конструкції поширювати вогонь (межа поширення вогню); М0 – межа поширення вогню дорівнює 0 см; М1 – М ≤ 25 см – для горизонтальних конструкцій; М ≤ 40 см – для вертикальних і похилих конструкцій; М2 – М > 25 см – для горизонтальних конструкцій; М > 40 см – для вертикальних і похилих конструкцій, нн – не нормується.

Таблиця 3.8 – Протипожежні норми проектування будівель і споруд [80]

Об’єм приміщення, тис. м^3	Категорія пожежної небезпеки	Ступінь вогнестійкості	Відстань, м, для щільності людського потоку в загальному проході, осіб/м^2			Кількість людей на 1 м ширини евакуаційного виходу	Протипожежні розриви, м, для ступеня їх вогнестійкості			Найбільша кількість поверхів	Максимально допустима площа поверху, м^2, для числа поверхів		
			до 1	2-3	4-5		I,II	III	IV, V		1	2	3 і більше
до 15	Б	2	40	25	15	45	9	9	12	6	н.о.	–	–

Примітки: н.о. – не обмежується, н.н. – не нормується.

Додаток А

(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ ВНТУ,

канд. техн. наук, професор

Г.Г.Бортник

. “__” _____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

КЕРУВАННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ В КОРПОРАТИВНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

08-34.МКР.008.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Городецька О. С.

Виконавець: ст. гр. ТКС-18м

Палагнюк Д. М.

Вінниця-2019

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 09.12.2019 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є дослідження і розробка підвищення ймовірності забезпечення безпеки потрібної для доступу до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами по захищеності при використанні єдиного МАП.

Задачами магістерської кваліфікаційної роботи є:

- розробка технічного завдання;
- аналіз додатків і перспектив для підвищення результативності захисту інформації при роботі з МАП;
- розробка моделі безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності, і обґрунтована її коректність;
- розробка алгоритму управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог щодо безпечності та якості послуг, проведена оцінка його властивостей, доведена його ефективність;
- розробка системи управління безпекою МАП, що відрізняється можливістю віддаленого управління програмно-апаратної залежності від умов доступу, вимог політик безпеки і якості послуг, що надаються для забезпечення захищеного доступу до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності.

Об’єкт дослідження є система управління безпекою МАП в корпоративних інфокомунікаційних мережах.

Предмет дослідження є система управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності.

Основними завданнями роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;

- модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності;

- алгоритм управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог безпеки і якості послуг;

- система управління безпекою мобільних абонентських пристроїв;

- аналіз економічної ефективності проведеної розробки;

- дослідження питань безпеки життєдіяльності.

Створення підвищення ймовірності забезпечення безпеки потрібної для доступу до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами по захищеності при використанні єдиного МАП.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах звіту з переддипломної практики “Керування безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах”, який виконувався у ВНТУ 2019/2020 н.р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цього звіту.

Список використаних джерел розробки:

3.1 Вишнякова, О. А. Математическая модель обнаружения точки беспроводного доступа по измерениям можности излучения разнесенными наблюдателями / О. А. Вишнякова, Д. Н. Лавров, С. Ю. Лаврова // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. – Омск : Изд-во ОмГУ. – 2013. – No 2(28). – С.49–59.

3.2 Ворошилин, Е. П. Моделирование процессов и явлений в системах святи : методическое пособие для самостоятельной работы магистров направления 210700.68 "Инфокоммуникационные технологии и системы связи" / Е. П. Ворошили // ТУСУР, 2012.

3.3 Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978-5-9912-0328-9.

3.4 Маркин, Д. О. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 9. – С. 39–50.

3.5 Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – No 4 (22). – С. 21–31.

3.6 Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978- 5-9912-0328-9.

3.7 Положення про кваліфікаційну роботу у Вінницькому національному технічному університеті / Уклад. О. Н. Романюк, Р. Р. Обертюх, Т. О. Савчук, Л. П. Громова – Вінниця : ВНТУ, 2015 – 27 с.

3.8 Кухарчук В.В., Ігнатенко О.Г., Обертюх Р.Р. Методичні вказівки до оформлення дипломних проектів (робіт) для студентів всіх спеціальностей.- В.: ВДТУ, 2002.

3.9 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

3.10 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.11 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.12 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання.- Вінниця:ВНТУ, 2018.- 50 с.

3.13 Палагнюк Д. М. Принципи забезпечення інформаційної безпеки / Д. М. Палагнюк, О. В. Березюк, Д. С. Тищук, // Матеріали науково-практичної конференції "Якість і безпека. Сучасні реалії", 14-15 березня 2018 р. – Вінниця : ВНТУ, 2018. – С. 19-22.

3.14 Бєлов В. С. Самоорганізація безпровідної сенсорної Mesh-мережі / В. С. Бєлов, Д. М. Палагнюк // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2018/paper/view/4505

3.15 Палагнюк Д. М. Інфокомунікаційні мережі на основі SHDSL технології / Д. М. Палагнюк, М. В. Васильківський // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2831.

3.16 Палагнюк Д. М. Еволюція стандартів IEEE802.11x / Д. М. Палагнюк, В. С. Бєлов // Конференції ВНТУ електронні наукові видання, XLVI Науково-технічна конференція факультету інфокомунікацій, радіоелектроніки та наносистем (2017). Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2017/paper/view/2569.

3.17 Палагнюк Д. М. Система дистанційного моніторингу / Д. М. Палагнюк, С. Т. Барась // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-frtzp/all-frtzp-2018/paper/view/5405

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТКС-18м Палагнюк Д. М.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження створення підвищення ймовірності забезпечення безпеки потрібної для доступу до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами по захищеності при використанні єдиного МАП.

Технічні вимоги, яким повинна відповідати розробка, наступні:

- рівень значущості α – 0,1;
- СКВ вимірювання рівня сигналу – 2 дБм;
- довірчий інтервал ε – 10^{-2};
- частота передавача – 2,4 ГГц;
- потужність передавача +0,09 Вт;
- розрахунок місця розташування МАП методами трилатерації;
- параметри, що характеризують сигнально-перешкодну обстановку k_{λ} – 0,6, Г – 14.

Запропоновано в роботі на основі формальної моделі безпеки розробити алгоритм управління безпекою МАП, що враховує атрибути доступу користувачів і МАП, включаючи його місце розташування, вимоги за якістю послуг, що надаються, а також науково-технічні пропозиції щодо реалізації

системи управління безпекою МАП, що дозволяють підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційним послугам та інформації корпоративних мереж з різними вимогами захищеності при використанні єдиного МАП.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документ-тація
		початок	закінчення		
1.	Розробка технічного завдання (ТЗ)	02.09.2019р.	06.09.2019р.	Розроблене ТЗ	Додаток А
2.	Аналіз стану наукових досліджень та технічних рішень в області захисту інформації під час використання мобільних абонентських пристроїв	09.09.2019р.	13.09.2019р.	Проведений аналіз	Вступ. Розділ 1.
3.	Модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності	16.09.2019р.	04.10.2019р.	Проведений аналіз	Розділ 2
4.	Алгоритм управління безпекою мобільного абонентського пристрою, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог безпеки і якості послуг	07.10.2019р	25.10.2019р.	Характе-ристики і параметри	Розділ 3

5.	Система управління безпекою мобільних абонентських пристроїв	28.10.2019р.	08.11.2019р.	Характе-ристики і параметри	Розділ 4
6.	Аналіз економічної ефективності розробки	11.11.2019р.	15.11.2019р.	Економічна частина МКР	Розділ 5
7.	Охорона праці та безпека в надзвичайних ситуаціях	18.11.2019р.	22.11.2019р.	Частина ОТ та БНС	Розділ 6
8.	Оформлення пояснювальної записки та графічної частини	25.11.2019р.	29.11.2019р.	Оформлена документа-ція	ПЗ та графічна частина
9.	Нормоконтроль МКР	02.12. 2019р.	06.12.2019р.	Позитивні відзиви	Відзив. рецензія
10.	Захист МКР ЕК		09.12. 2019р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- Типовий склад сучасного МАП;
- Узагальнена блок-схема алгоритму управління безпекою МАП;
- Блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП;
- Схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу;
- Схема управління конфігурацією МАП;
- Схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення;
- Допустимі значення виробничих факторів;
- економічна частина МКР;
- розділ ОП та БНС;

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується отримати оптимальні рішення при керуванні безпекою мобільних абонентських пристроїв в корпоративних інфокомунікаційних мережах.

8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

Документація, що розробляється в процесі виконання досліджень повинна містити:

- техніко-економічне обґрунтування розробки;
- типовий склад сучасного МАП;
- узагальнена блок-схема алгоритму управління безпекою МАП;
- блок-схема алгоритму управління програмно-апаратною оптимальною конфігурацією МАП;
- схема розташування приміщень з точками доступу і вимірюванням коливань рівня сигналу;
- схема управління конфігурацією МАП;
- схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення;
- економічну частину та розділ БНС і ЦЗ;

11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.