Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод керування безпекою мобільних пристроїв в корпоративних мережах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220193.22.01.23 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Федух М.М.
Підпис

Керівник доц., к.т.н, доцент _____ Кльоц Ю.П.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

8 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма КІБЕРБЕЗПЕКА

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Федуху Миколі Миколайовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод керування безпекою мобільних пристроїв в корпоративних мережах

Керівник роботи Кльоц Юрій Павлович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 01.12.2023

3. Вихідні дані до проекту (роботи) Розробити модель безпеки мобільного пристрою та модель системи визначення місця розташування, алгоритм визначення місця знаходження. Реалізувати систему управління безпекою мобільних пристроїв, зокрема визначити вимоги та оцінити ефективність роботи системи.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз наявних моделей безпеки мобільних пристроїв. Постановка задачі. Розробка моделей: безпеки пристрою, визначення місця розташування пристрою. Розробка алгоритму управління безпекою мобільного пристрою. Вимоги до системи управління. Оцінка ефективності роботи системи. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз наявних моделей безпеки та загроз, постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритму визначення місця розташування	16.10.2023	
6	Робота над розділом 4 – розробка системи управління та оцінка ефективності	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ М.М.Федух
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод керування безпекою мобільних пристроїв в корпоративних мережах.

Автор роботи: Федух Микола Миколайович

Керівник роботи: к.т.н., доц. Кльоц Юрій Павлович

Загальний обсяг роботи: 75 сторінок, 25 рисунків, 2 таблиці, 1 додаток, 50 посилань.

Ключові слова: захищеність мобільних пристроїв, модель безпеки, місце розташування мобільного пристрою, система управління безпекою.

Для досягнення мети в роботі були сформульовані та вирішені наступні завдання: розроблено формальну моделі безпеки мобільного пристрою, алгоритм та модель визначення місцезнаходження мобільного пристрою у приміщенні. У роботі розраховано ефективність системи управління безпекою мобільних пристроїв. Надано пропозиції щодо складу, структури та місця системи управління безпекою мобільними пристроями у складі корпоративних мереж з різними рівнями захищеності.

Здобуті результати мають практичне значення в контексті використання мобільних пристроїв у спеціальних приміщеннях. Розроблена система базується на визначенні місця розташування пристрою та зміні налаштувань пристрою у залежності від рівня захисту де перебуває пристрій.

11.12.23

ANNOTATION

Theme of qualification work: Method of managing the security of mobile devices in corporate networks.

Author of the work: Fedukh Mykola Mykolayovych

Mentor: Ph.D., Assoc. Klots Yurii Palovich

Total volume of work: 75 pages, 25 figures, 2 tables, 1 appendix, 50 references.

Keywords: security of mobile devices, security model, mobile device location, security management system.

To achieve the goal, the following tasks were formulated and solved in the work: a formal model of mobile device security, an algorithm, and a model for determining the location of a mobile device in the room were developed. The paper calculates the effectiveness of the security management system of mobile devices. Proposals are provided regarding the composition, structure, and location of the security management system for mobile devices in corporate networks with different levels of security.

The obtained results are of practical importance in the context of the use of mobile devices on special premises. The developed system is based on determining the location of the device and changing the device settings depending on the level of protection where the device is located.

11.12.23

ЗМІСТ

ВСТУП

Розвиток сучасних багатофункціональних мобільних абонентських пристроїв (МП) та інформаційних технологій, пропускної спроможності каналів зв'язку, у тому числі бездротових, призводять до постійного зростання потреби в доступі до інформації, причому незалежно від того, де є користувач. У цьому відношенні не є винятком і корпоративні мережі, у тому числі захищені (ЗКС), що надають доступ до інфокомунікаційних послуг та ресурсів з різними вимогами щодо захищеності. До таких мереж відносяться: інформаційні системи загального користування; інформаційні системи, що опрацьовують персональні дані; геоінформаційні системи.

Віддалений доступ з використанням МП до корпоративних мереж з різними вимогами щодо захищеності передбачає застосування відповідних систем захисту безпеки, що дозволяють забезпечити необхідний рівень забезпечення безпеки інформації незалежно від рівня захищеності сегмента захищеної корпоративної мережі. При цьому принциповою вимогою є використання співробітниками чи користувачами ЗКС єдиного МП для здійснення такого доступу. Відмінність за вимогами захищеності в ЗКС, зазвичай, ділить таку мережу на контури обробки інформації, які, в свою чергу, зазвичай обмежені спеціалізованими приміщеннями з відомим розташуванням на об'єктах організації.

Однак використання сучасних МП, що володіють значними обчислювальними і комунікаційними ресурсами, для обробки конфіденційної інформації обмежено у зв'язку з низкою істотних особливостей, що стосуються їх експлуатації: розмірами, мобільністю користувачів, багатофункціональністю.

Зазначені особливості визначають зовсім інший спектр загроз інформаційній безпеці при роботі з МП порівняно зі стаціонарними засобами обчислювальної техніки (ЗОТ). Постійна зміна розташування користувачів МП, бездротовий віддалений доступ до мереж з різними вимогами щодо захищеності, обмежені обчислювальні можливості з одного боку і високошвидкісні комунікаційні з іншого створюють велику кількість загроз інформаційній безпеці, пов'язаних в першу

чергу з загрозами порушення конфіденційності інформації.

З іншого боку перспективним напрямом вдосконалення сучасних корпоративних мереж є забезпечення надання захищеного доступу абонентам до інформації та послуг з різними вимогами щодо захищеності при використанні єдиного МП. При цьому до послуг, що надаються, у відповідність відносяться:

– телефонний та відеозв'язок з додатковими видами обслуговування;

– захищений електронний поштовий обмін з елементами обліку вхідних та вихідних документів;

– відеоконференцзв'язок;

– доступ до баз та банків даних, мережевих додатків та інформаційних ресурсів.

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

Предмет дослідження: моделі та алгоритми управління безпекою МП.

Мета дослідження: підвищення ймовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами щодо захищеності при використанні єдиного МП.

Завдання дослідження: на основі формальної моделі безпеки МП розробити алгоритм управління безпекою МП, що враховує атрибути доступу користувачів і МП, включаючи його місцезнаходження, вимоги щодо якості послуг, а також науково-технічні пропозиції щодо реалізації системи управління безпекою МП, що дозволяють підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами щодо захищеності при використанні єдиного МП.

1 АНАЛІЗ НАЯВНИХ ДОСЛІДЖЕНЬ І ТЕХНІЧНИХ РІШЕНЬ

1.1. Умови функціонування та вимоги до мобільних пристроїв

В даний час використання сучасних МП у захищених корпоративних мережах суттєво обмежено через відсутність ефективних систем захисту інформації (СЗІ), які б гарантували безпеку інформації [1]. Проте перспективним напрямом удосконалення сучасних корпоративних мереж є забезпечення захищеного доступу абонентам до інформації та послуг із різними вимогами щодо безпеки, використовуючи єдиний МП.

Сучасні корпоративні мережі [2-4], в яких передбачено використання МП, являють собою аналоги структури, представленої на рисунку 1.1.

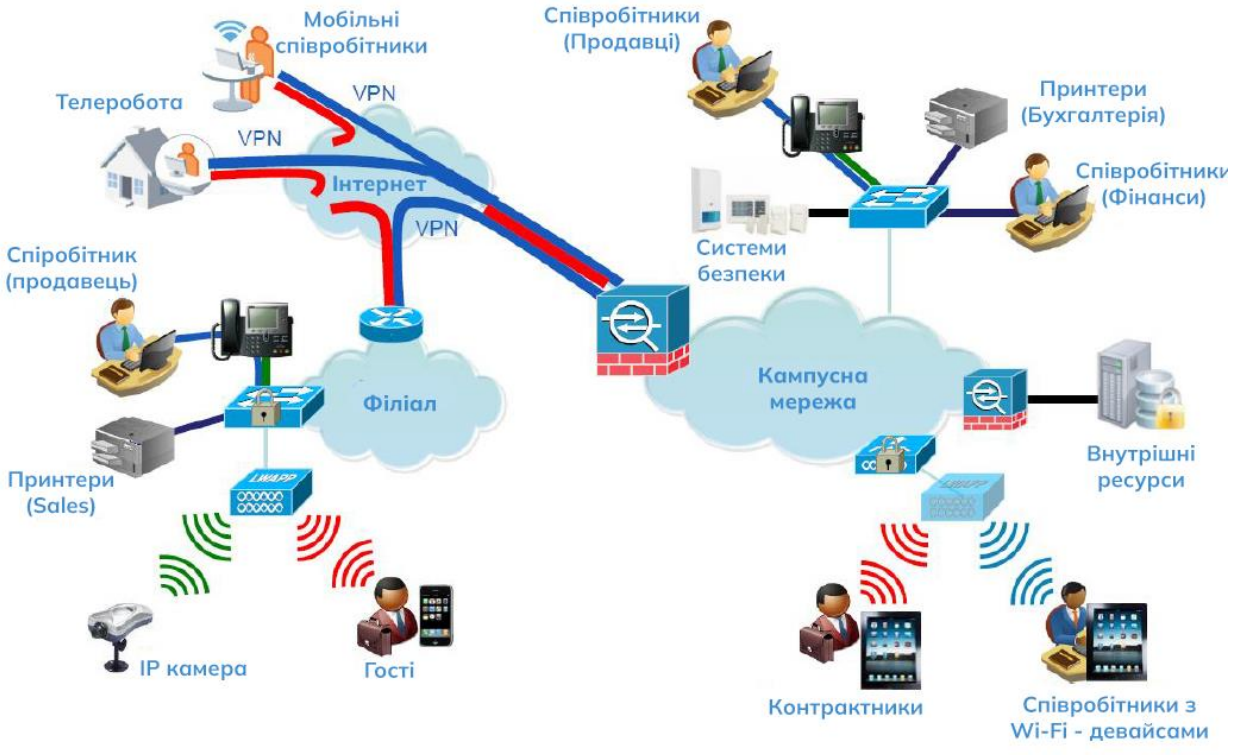

Рисунок 1.1 – Типова структура корпоративних мереж з використанням МП

За наявності інформації, яка потребує більш високого рівня захисту, в

організації створюються різні корпоративні мережі з різними рівнями захисту [5]. Зазвичай для отримання доступу до ресурсів корпоративних мереж із різними вимогами до безпеки використовуються різні МП з відповідними рівнями захисту, що може створювати певні незручності. Для вирішення цієї проблеми та забезпечення безпеки інформації при роботі на єдиному МП зараз використовуються два підходи: встановлення спеціалізованих СЗІ, таких як рішення управління МП (MDM) [6-7], на особистих МП співробітників організації в рамках концепції "BYOD" (Bring Your Own Device); експлуатація корпоративних захищених МП [8].

Проте обидва ці підходи мають недоліки з точки зору захисту інформації з різних причин:

– відсутність обґрунтованих формальних моделей безпеки комп'ютерних систем, які передбачали б експлуатацію МП та враховували б мобільність користувачів;

– системи виявлення місця розташування МП в приміщеннях на території організації, як правило, будуються на основі стандарту 802.11 [9] та володіють низькою точністю виявлення місця розташування порядку 2 метрів, що створює загрозу некоректного застосування встановленої в корпоративній мережі політики безпеки МП;

– існуючі рішення MDM та корпоративні захищені МП не дозволяють апаратної переконфігурації МП, що може призводити до технічних каналів витоку інформації за межами контрольованої зони;

– існуючі методики сертифікації СЗІ не забезпечують гарантії відсутності програмних та апаратних закладок.

Попри наявність сучасних засобів захисту інформації СЗІ, спрямованих на забезпечення безпеки при використанні МП, ключовим питанням залишається довіра до апаратної основи МП [10-11]. Зазвичай ця апаратна основа використовує технологію System-on-Chip (SoC) [12-13]. В більшості сучасних МП використовується архітектура ARM процесорів, які включають в себе технологію "TrustZone".

Аналіз законодавчої бази та вимог до забезпечення інформаційної безпеки (ІБ) при використанні МП у захищених корпоративних мережах [14-15] показав наступне:

– існують спеціальні вимоги до системи ІБ щодо використання МП у захищених корпоративних мережах [16-17];

– використання особистих МП у захищених корпоративних мережах заборонено або обмежено, згідно з концепцією "BYOD", з урахуванням вимог системи ІБ;

– абонентські пристрої, такі як стільникові телефони, смартфони, планшетні комп'ютери тощо, які працюють за стандартом IEEE 802.11, повинні відповідати вимогам корпоративної політики щодо інформаційної безпеки в захищених корпоративних мережах [18-19];

– обладнання для мереж Wi-Fi також повинно відповідати вимогам корпоративної політики щодо інформаційної безпеки.

Очевидно, що використання особистих МП у захищених корпоративних мережах стикається із значними обмеженнями щодо доступності захищених інфокомунікаційних послуг. Відкриті послуги, доступні через особисті МП, можуть бути недоступні або обмежені. Проте сучасні МП здатні надавати доступ до різних видів послуг. Порівняльний аналіз кількості наданих різними МП послуг представлений на рисунку 1.2.

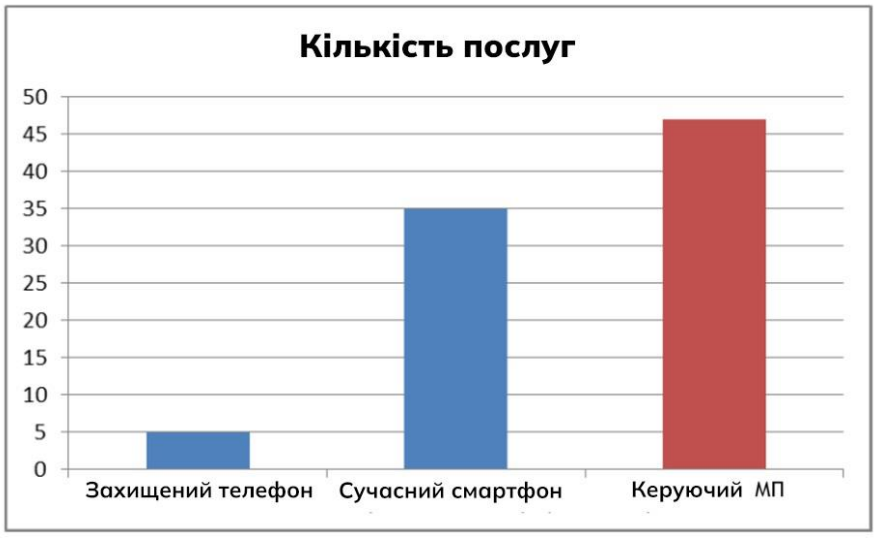

Рисунок 1.2 – Порівняльний аналіз кількості послуг, що надаються МП

З огляду на відсутність ефективних СЗІ, використання МП для доступу до послуг у захищених корпоративних мережах сильно обмежене. Пропонується підвищити рівень захисту інформації шляхом використання керованих МП, які взаємодіють із системою управління безпекою МП. Ця система дозволяє керувати програмно-апаратною конфігурацією МП в залежності від умов їх використання та вимог до безпеки (атрибутів доступу). Структура та топологія системи управління безпекою МП в корпоративній мережі в цьому випадку може виглядати так, як показано на рисунку 1.3.

Рисунок 1.3 – Структура та топологія системи управління безпекою МП у корпоративній мережі

Однак основним недоліком цієї архітектури системи управління безпекою МП є відсутність формальної моделі безпеки МП, яка враховувала б розташування МП у корпоративній мережі, підтверджувала її коректність та надавала ефективні засоби визначення місцезнаходження МП всередині приміщень. Ці фактори підкреслюють актуальність обговорюваної проблеми та необхідність розв'язання

завдання, яке було поставлено під час виконання даної роботи.

1.2 Моделі безпеки комп'ютерних систем з мобільними пристроями

Для формального опису процесу забезпечення інформаційної безпеки в комп'ютерних системах та обґрунтування рівня їх захищеності використовують формальні моделі безпеки [20-22]. Ці моделі служать основою для розробки різних механізмів захисту інформації, включаючи системи контролю доступу. Основною метою системи контролю доступу [23-24] є запобігання будь-якій діяльності, яка може загрожувати безпеці комп'ютерної системи. Це завдання може вирішуватися шляхом запобігання діям або операціям, які можуть виконувати в рамках системи користувачі або запущені від імені користувача процеси, а також шляхом обмеження доступних користувачеві комп'ютерної системи дій.

Більшість сучасних систем контролю доступу будуються на основі моделі Лемпсона [25-26] (рис. 1.4). У цій моделі, монітор звернень виступає посередником при кожній спробі джерела запитувати доступ до ресурсів системи (об'єктів доступу).

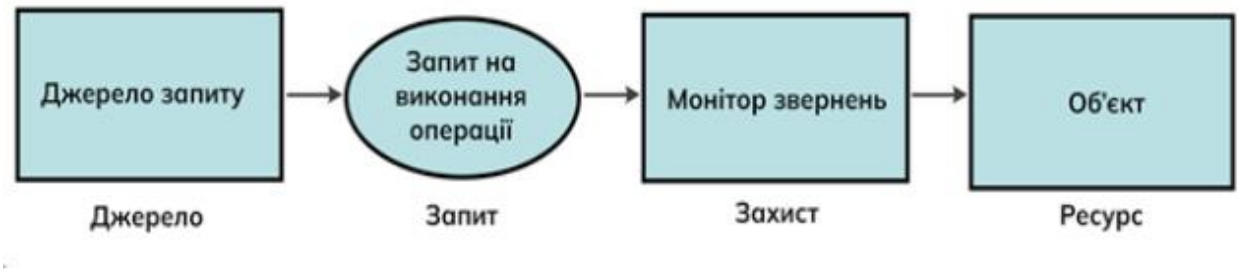

Рисунок 1.4 – Модель системи керування доступом Лемпсона

В існуючій теорії комп'ютерної безпеки для опису елементів комп'ютерної системи використовуються різні терміни, такі як "сутність", "об'єкт", "суб'єкт", "доступ", "контейнер". Суб'єкти здійснюють доступ до сутностей комп'ютерної системи [27], щоб виконувати різні операції, такі як читання, запис, а також активізацію (виконання) суб'єкта на певній сутності.

Система контролю доступу в комп'ютерних системах створюється для

захисту інформації від різних загроз безпеці. При класифікації цих загроз виділяють три основні аспекти: конфіденційність, цілісність та доступність інформації. Ці аспекти визначають три основні класичні загрози для безпеки інформації: порушення конфіденційності, цілісності та доступності інформації, а також ще одну загрозу - розкриття параметрів комп'ютерної системи.

Управління доступом є однією з послуг у сфері захисту інформації і є частиною загальної архітектури захисту, разом з іншими послугами, такими як автентифікація, конфіденційність даних, цілісність даних та безвідмовність. Для надання різних заходів захисту використовують спеціальні механізми, одним із яких є система контролю доступу. У деяких випадках для забезпечення безпеки можуть використовуватися кілька механізмів захисту.

В комп'ютерній системі доступ суб'єкта до об’єкта дозволяється, якщо система контролю доступу визнає, що у суб'єкта є відповідні права доступу до цього об’єкта. Спосіб надання прав доступу суб'єктам до об’єктів системи визначається політикою управління доступом, яка є складовою частиною загальної політики безпеки системи.

Існують різні види політик управління доступом, які регламентують спосіб надання прав доступу суб'єктам до об’єктів [28], такі як дискреційна політика управління доступом, мандатна (повноважна) політика управління доступом, політика рольового управління доступом, політика безпеки інформаційних потоків та політика безпеки ізольованих програмних середовищ (ІПС).

Формальні моделі безпеки [29] для комп'ютерних систем описують, як працює політика управління доступом та використовуються для обґрунтування захищеності сучасних і майбутніх комп'ютерних систем. Слід відзначити, що розвиток технологій в комп'ютерних системах є постійним, і разом з появою нових можливостей з'являються нові фактори, які створюють загрози для безпеки інформації. Ці нові загрози зазвичай не передбачені в існуючих формальних моделях безпеки. Тому кожна нова формальна модель намагається врахувати знову виникаючі фактори, що призводять до нових загроз безпеці інформації. Класифікація та взаємозв'язок низки формальних моделей безпеки КС зображено

на рисунку 1.5.

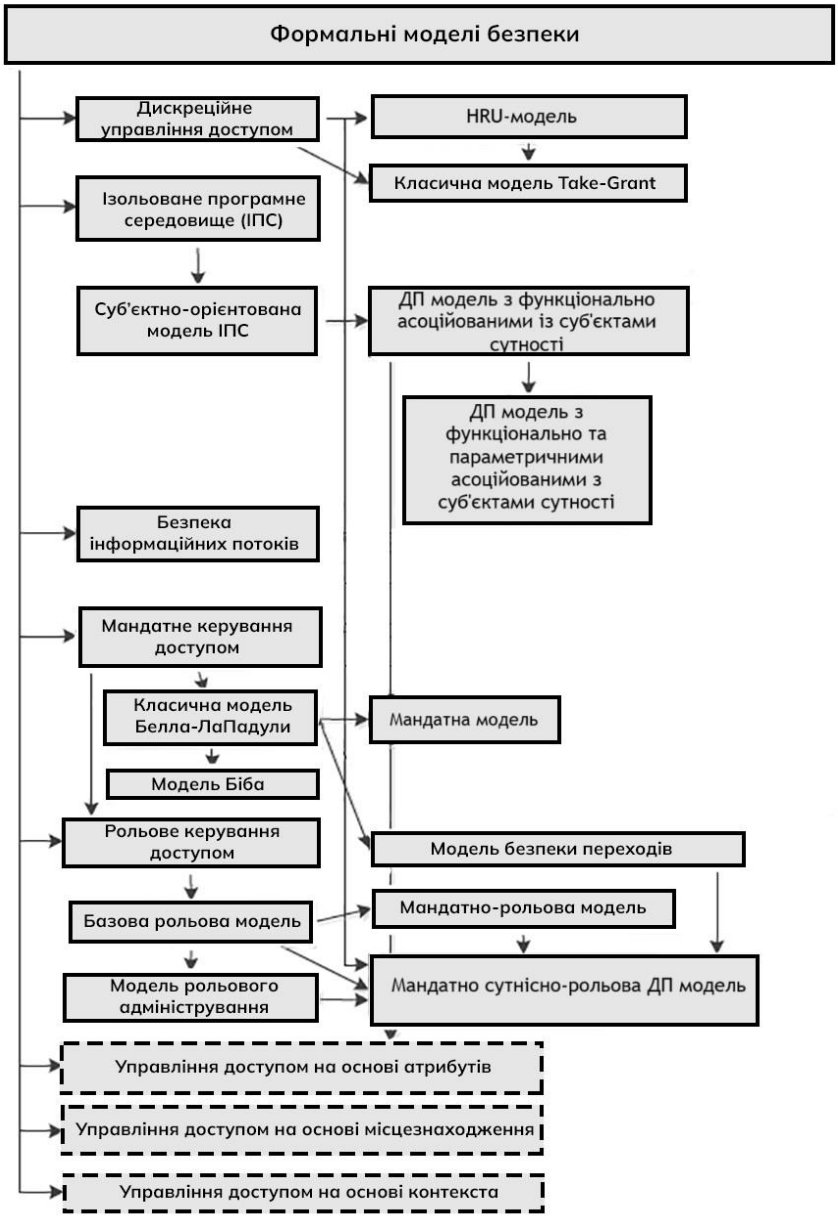

Рисунок 1.5 – Класифікація та взаємозв'язок окремих формальних моделей безпеки КС

На сьогоднішній день існує безліч різних формальних моделей безпеки комп'ютерних систем, які мають дві основні мети. По-перше, вони спрямовані на більш повний перелік всіх можливих факторів, що дозволяє зробити модель безпеки комп'ютерної системи більш гнучкою та адаптивною до реальних умов її функціонування. По-друге, вони використовують більш досконалі механізми управління доступом, що спрощує процедури адміністрування складних

комп'ютерних систем.

Окрім того, важливим чинником є вплив припущень на безпеку комп'ютерної системи під час її розробки, а також неможливість врахувати всі можливі умови її функціонування в реальному середовищі. Це також має серйозний вплив на безпеку комп'ютерної системи і вимагає удосконалення і розробки нових моделей безпеки.

У контексті реалізації формальних моделей безпеки для управління доступом користувачів до МП, стає очевидною необхідність врахування місця розташування як важливого фактора, що впливає на безпеку інформації в комп'ютерних системах. Проаналізувавши уважно цю проблему в контексті існуючих моделей, можна виявити кілька серйозних недоліків, які впливають на адекватність моделей для реальних комп'ютерних систем і загрожують їх безпеці. До цих недоліків можна віднести наступне:

– Питання безпосереднього визначення розташування, як координат користувачів і пристроїв, або приміщень, в яких перебувають користувачі, не розглядаються повністю.

– Не враховується помилка визначення місця розташування пристроїв, яка виникає через недосконаліть сучасних методів визначення місцеположення як на відкритій місцевості, так і всередині будівель.

– Не розглядаються питання оцінки вимог до безпеки для пристроїв в залежності від їх місця розташування і рівня вимог щодо захисту спеціальних приміщень, в яких вони розташовані. Також не враховується рівень конфіденційності інформації і послуг, до яких запитується доступ.

– Можливості інтелектуального блокування МП або окремих їх функціональних блоків, які можуть становити загрозу для інформаційної безпеки в залежності від умов доступу, не використовуються як складова частина системи захисту інформації в комп'ютерних системах.

Ці недоліки свідчать про необхідність подальшого вдосконалення формальних моделей безпеки для управління доступом до МП і покликані привернути увагу до важливості розгляду місця розташування при розробці таких

моделей.

1.3. Моделі загроз та порушника інформаційної безпеки

1.3.1. Характеристика та особливості сучасних мобільних пристроїв

Сучасні МП, що володіють обчислювальними та комунікаційними ресурсами, є багатофункціональними медіа пристроями, в яких функція телефонних переговорів не є першорядно важливою. Для покращення показника економічності основні вузли сучасних МП агреговані у складі мікросхеми класу SoC (System-on-Chip – системі на чіпі) [30], на яку покладається весь перелік завдань збору, обробки, зберігання та обміну користувальницькою та службовою інформацією. Така SoC часто об'єднує на одному кристалі кілька ядер процесора, комунікаційний процесор, графічний співпроцесор та ін. модулів GPS/ГЛОНАСС/Galileo/Beidou, а також набір інтерфейсів для взаємодії з різними типами пристроїв (USB, SD, MMC, UART та ін.) забезпечує конфігурування МП для вирішення різних завдань і вимог користувачів і забезпечує багатофункціональність сучасних МП .

При експлуатації МП існує ряд важливих особливостей, що надають суттєвий вплив на стан захищеності інформаційної взаємодії в рамках роботи в ЗКС. До них відносяться:

– Малий розмір МП. Дана властивість МП призводить до обмеження можливостей інтерфейсу взаємодії з користувачем, впливає на обчислювальні та функціональні можливості, підвищує ризик втрати МП і, відповідно, використання його неавторизованим користувачем.

– Мобільність. Дана властивість МП дозволяє використовувати функціональні можливості МП незалежно від розташування користувача, проте в поєднанні з мініатюрністю дозволяє непомітно здійснити пронос і використання МП всередині приміщень з підвищеними вимогами щодо захищеності.

– Обмеженість обчислювальних ресурсів МП. Даний фактор впливає на виконувані в МП обчислювальні процеси. Оскільки процеси, що відповідають за функції захисту інформації (ЗІ), як правило, повинні виконуватися у фоновому

режимі та постійно задіювати певну частину обчислювальних ресурсів, то в умовах обмеженості цих ресурсів у МП виникають обмеження на функціональність та можливості таких процесів.

– Мультифункціональність МП. До сучасних функцій МП можна віднести використання МП: у вигляді фото- та відеокамери; як навігаційного пристрою; як модему; як переносна точка доступу; як диктофон; як знімний носій інформації.

– Доступ до послуг корпоративної мережі на основі використання принципу одноразового входу SSO (Single Sign-On) [31]. Дана особливість є наслідком мініатюрності МП та складності людино-машинної взаємодії, характерної для МП. У поєднанні з мобільністю та мініатюрністю МП використання режиму SSO призводить до збільшення ризиків використання МП неавторизованим користувачем.

– Доступ до інформаційних ресурсів мереж із різними вимогами щодо захищеності. Використання МП для доступу до мереж з різними вимогами щодо захищеності в даний час обмежене, оскільки не існує ефективних СЗІ, що забезпечують безпеку інформації. Існуючі підходи щодо ЗІ, що використовуються в стаціонарних ЗОТ, не застосовні повною мірою до МП через обмеженість їх обчислювальних ресурсів, а також особливості їх програмно-апаратної архітектури.

Зазначені особливості збільшують ймовірність здійснення загроз під час роботи з МП в умовах ЗКС, тому необхідно враховувати фактори, що впливають на безпеку інформації.

Істотне значення при розробці СЗІ для МП мають питання щодо їх конфігурування з урахуванням показників ресурсоспоживання, що передбачають вибір та розробку СЗІ шляхом комбінування окремих компонентів захисту з урахуванням їх властивостей, обмежень та вимог до них з боку МП.

1.3.2 Фактори, що впливають на безпеку інформації при використанні мобільних пристроїв

Ураховуючи, що використання МП передбачається в різних мережах з

різними вимогами до рівня безпеки і враховуючи зазначені відмінності у характеристиках МП порівняно зі стаціонарними ЗОТ, було виділено актуальні фактори, що впливають на забезпечення безпеки інформації при використанні МП в ЗКС.

Об'єктивні чинники, які впливають на функціонування об'єкта інформатизації, можуть бути розділені на внутрішні та зовнішні фактори. Серед внутрішніх факторів важливо враховувати передачу сигналів, яка відбувається в різних діапазонах, таких як радіохвилі та оптичний діапазон довжин хвиль. Це особливо актуально у випадку передачі інформаційних сигналів за допомогою бездротових каналів зв'язку, таких як Bluetooth, Wi-Fi, GSM, UMTS, LTE тощо [32]. Крім того, об'єкт інформатизації може випромінювати сигнали, включаючи акустичні сигнали, які стосуються вимовної або відтворюваної мови та електромагнітні випромінювання та поля у радіодіапазоні при використанні різних модулів зв'язку. До внутрішніх факторів слід віднести також наявність акустоелектричних перетворювачів в елементах технічних систем, а також дефекти, збої, відмови, аварії технічних засобів та систем. Також важливо враховувати можливі дефекти, збої та відмови програмного забезпечення, оскільки вони можуть суттєво впливати на надійність та функціональність об'єкта інформатизації. Усі ці фактори важливі для забезпечення ефективної та надійної роботи інформаційних систем.

У контексті суб'єктивних чинників, які впливають на безпеку інформації та об'єкта інформатизації, важливо розглянути як внутрішні, так і зовнішні аспекти. Серед внутрішніх факторів можна виділити наступне:

– Розголошення інформації, яка підлягає захисту, може відбуватися через передачу інформації по відкритих лініях зв'язку, обробку інформації на незахищених технічних засобах обробки інформації, копіювання інформації на незареєстровані носії, втрату носія інформації.

– Неправомірні дії осіб, які мають право доступу до інформації, що захищається, можуть включати несанкціоновану зміну інформації або несанкціоноване копіювання інформації.

– Несанкціонований доступ до інформації може бути здійснений через підключення до технічних засобів та систем об'єкта інформатизації, використання закладних засобів, програмного забезпечення технічних засобів об'єкта інформатизації, маскування під зареєстрованого користувача, використання вразливостей програмного забезпечення тощо.

– Помилки обслуговуючого персоналу об'єкта інформатизації під час експлуатації можуть включати помилки при використанні обчислювальної техніки та програмного забезпечення, а також при експлуатації засобів та СЗІ.

Серед зовнішніх суб'єктивних факторів слід виділити:

– Несанкціонований доступ до інформації може відбуватися через підключення до технічних засобів та систем об'єкта інформатизації, використання закладних засобів, програмного забезпечення технічних засобів об'єкта інформатизації, маскування під зареєстрованого користувача, використання вразливостей програмного забезпечення.

– Блокування доступу до інформації може бути досягнуто перевантаженням технічних засобів обробки інформації хибними заявками на її обробку.

– Спотворення, знищення або блокування інформації може бути досягнуто за допомогою різноманітних технічних засобів, включаючи програмне або програмно-апаратне обладнання, при здійсненні комп'ютерних атак або мережевих атак.

Усі ці суб'єктивні чинники можуть суттєво впливати на безпеку інформації та об'єкта інформатизації, тому важливо вживати необхідних заходів для їх управління та захисту.

Аналіз представлених чинників допомагає зробити наступні висновки:

– Велика частина чинників, що впливають на інформаційну безпеку під час роботи з МП, є суб'єктивними, оскільки вони залежать від користувачів. Це включає в себе ризики, пов'язані з неправомірними діями користувачів, які мають доступ до конфіденційної інформації.

– Більша частина виділених об'єктивних внутрішніх факторів, що впливають на безпеку інформації, є результатом наявності в МП функціональних блоків (модулів), які створюють технічні канали для витоку інформації. Це стосується використання таких МП всередині або поблизу спеціальних приміщень з обмеженим доступом, а також при незахищеному доступі до конфіденційної інформації.

Аналіз цих факторів дозволяє сформулювати перелік загроз ІБ, пов'язаних із роботою з МП, а також побудувати модель потенційного порушника під час використання МП в ЗКС. Такий підхід допомагає ліпше розуміти ризики та вживати відповідні заходи для забезпечення безпеки інформації при використанні МП у контрольованих об'єктах.

1.3.3 Моделі загроз та порушника з мобільними пристроями та різними вимогами щодо захищеності

Спільна наявність цих актуальних факторів дозволяє створити модель загроз ІБ в ЗКС при використанні МП. У багатьох випадках доступ до інформації може бути піддатливим до загроз ІБ, які виникають внаслідок використання сторонніх додатків та взаємодії пристроїв з МП під час інформаційної взаємодії всередині ЗКС.

При розробці моделі загроз необхідно враховувати унікальні характеристики МП, які відрізняються від стаціонарних комп'ютерних систем та навіть основні принципи забезпечення ІБ в ЗКС з використанням МП:

– Принцип недовіри до електроніки, зокрема на базі SoC і архітектури ARM, яка широко використовується у таких операційних системах, як Android, а також включає апаратну віртуалізацію та довірену ("Trusted OS"). Для забезпечення безпеки може використовуватися власна довірена операційна система з довіреним початковим завантажувачем, який реалізований за допомогою апаратно-програмного модуля довіреного завантаження для процесорів з архітектурою ARM. Така система контролює наявність апаратних можливостей, що не декларовані виробником, та забезпечує безпеку операцій.

– Принцип недовіри до МП передбачає вимогу наявності СЗІ, які

забезпечують необхідний рівень інформаційної безпеки в корпоративних ЗКС, навіть коли немає довіри до користувачів МП. Можливими засобами захисту є обмеження або заборона використання особистих МП, запуск корпоративних додатків в ізольованих контейнерах, використання МП, які моніторять стан і дії користувачів, а також використання довіреної програмно-апаратної середовища.

– Принцип небезпеки бездротових з'єднань МП передбачає наявність засобів захисту, які гарантують автентичність сторін, що беруть участь у бездротовій мережній взаємодії та забезпечують захищеність передачі даних. Засобами захисту можуть бути застосування шифрування при передачі даних і використання взаємної аутентифікації, яка базується на криптографічних алгоритмах.

– Принцип небезпеки сторонніх додатків передбачає, що будь-які зовнішні програми можуть бути потенційно небезпечними і створювати канали витоку інформації з МП і ЗКС. Для забезпечення захисту вимагається наявність СЗІ, які забезпечують довіреність додатків, які використовуються на МП, і перешкоджають витоку інформації під час запуску цих додатків. Можливими засобами захисту є ізольоване програмне середовище, безпечні ізольовані контейнери для корпоративних додатків, термінальний доступ до додатків на віддаленому корпоративному сервері і довірені гіпервізори для запуску додатків в ізольованому середовищі.

– Принцип небезпеки пристроїв, що взаємодіють з МП передбачає наявність засобів контролю, що підключаються до МП пристроїв, засобів контролю стану та функціональних можливостей окремих МП модулів, а також засобів контролю даних, що передаються в процесі взаємодії МП з іншими пристроями. Такі засоби дозволяють забезпечити необхідний рівень захисту, переконавшись, що всі підключені до МП пристрої є безпечними та довіреними.

Засобами захисту можуть бути: засоби контролю пристроїв, що підключаються до МП; засоби контролю стану та функціональних можливостей окремих модулів МП; засоби контролю даних, що передаються в процесі взаємодії МП з іншими пристроями.

З урахуванням даних принципів, а також на основі досліджень та проведеного аналізу факторів, що впливають на безпеку інформації при експлуатації МП, виокремлено актуальні загрози ІБ. Загрози ІБ при експлуатації МП представлені у вигляді:

<загроза>:=<джерело загрози>,<вразливість>,<спосіб реалізації загрози>, <об'єкт впливу (програма, протокол, дані і т.д.>, <деструктивний вплив>.

Описова модель загроз і порушника ІБ під час експлуатації МП з урахуванням зазначеного уявлення зображено на рисунку 1.6.

Враховуючи зазначені принципи та проведений аналіз факторів, що впливають на безпеку інформації при використанні МП, можна виокремити актуальні загрози ІБ.

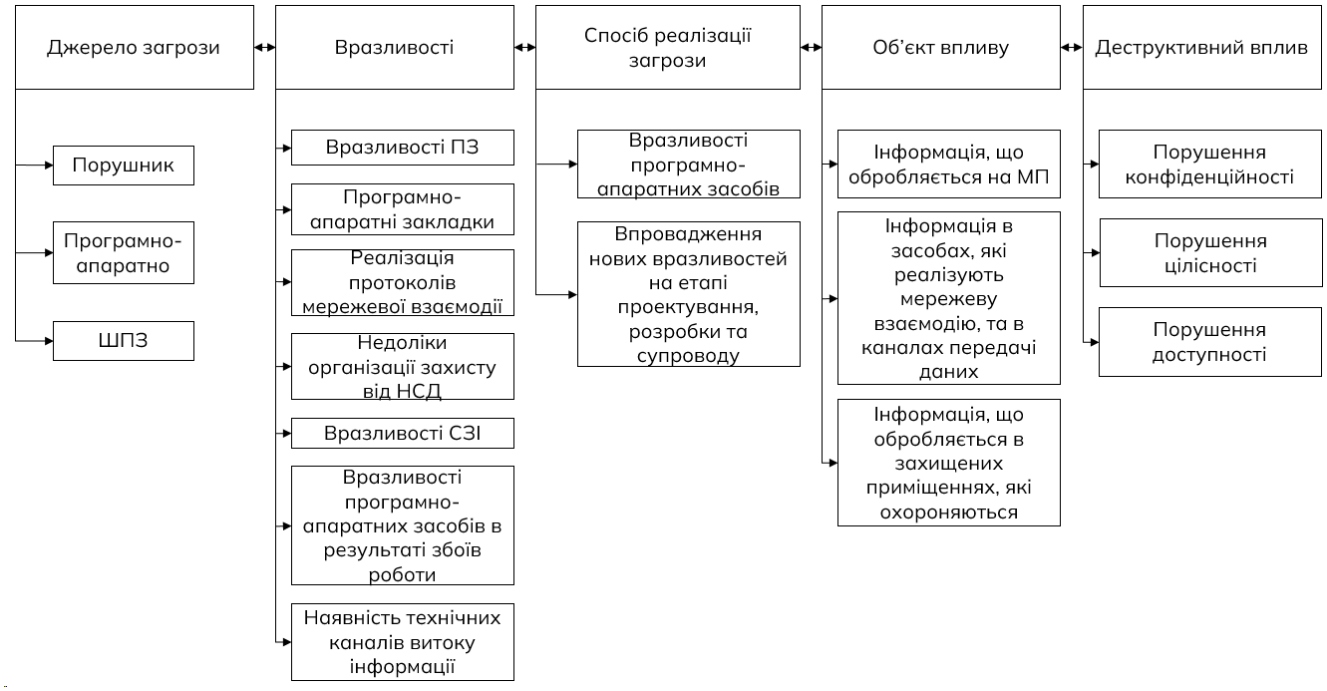

Рисунок 1.6 – Модель загроз та модель порушника при експлуатації МП в ЗКС

Основним джерелом загроз ІБ є внутрішні порушники, оскільки для ефективного захисту від інших загроз існують наявні СЗІ [33]:

– Для захисту від зовнішніх загроз інформаційній безпеці, може бути застосований комплекс організаційно-технічних заходів, спрямованих на виконання вимог інформаційної безпеки в корпоративних захищених мережах.

– Для запобігання загрозам, пов'язаним із програмно-апаратними закладками та шкідливими програмами, можуть бути використані СЗІ, які включають в себе ліцензування та сертифікацію МП, а також застосування ізольованого програмного середовища у складі операційної системи МП та довіреної операційної системи.

Зазначені вразливості включають: недоліки в організації захисту інформації від несанкціонованого доступу (НСД); наявність технічних каналів витоку інформації (ТКВІ) у МП під час експлуатації МП в режимах, які не дозволені [34-35].

У зв'язку з потребою використання єдиного МП для доступу до корпоративних мереж із різними вимогами щодо безпеки, головним завданням є створення умов для такого керування програмно-апаратною конфігурацією МП, яке виключатиме можливість технічних каналів витоку інформації при використанні єдиного МП для доступу до ресурсів корпоративних мереж із різними вимогами щодо безпеки (рисунок 1.7).

Рисунок 1.7 – Схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки

Для запобігання витоку інформації через ТКВІ, може бути використана

система керування програмно-апаратною конфігурацією МП. Ця система дозволяє відключати окремі модулі МП, такі як мікрофони чи радіоінтерфейси, які можуть створювати потенційні джерела сигналів, в залежності від умов доступу та місцезнаходження МП. Наявність такої системи дозволяє контролювати можливість використання МП як засобу зв'язку, враховуючи конкретні умови та обмеження. За відсутності такої системи, внутрішній порушник може мати технічну можливість використовувати МП як засіб зв'язку незалежно від умов доступу та свого місцезнаходження в організації [36-37]. Наприклад, якщо МП несанкціоновано або випадково потрапляє в спеціальне приміщення, де заборонено обробку відкритої інформації та використання МП, цей пристрій може стати джерелом інформаційних сигналів, які містять конфіденційну інформацію. Схему витоку інформації зображено на рисунку 1.8.

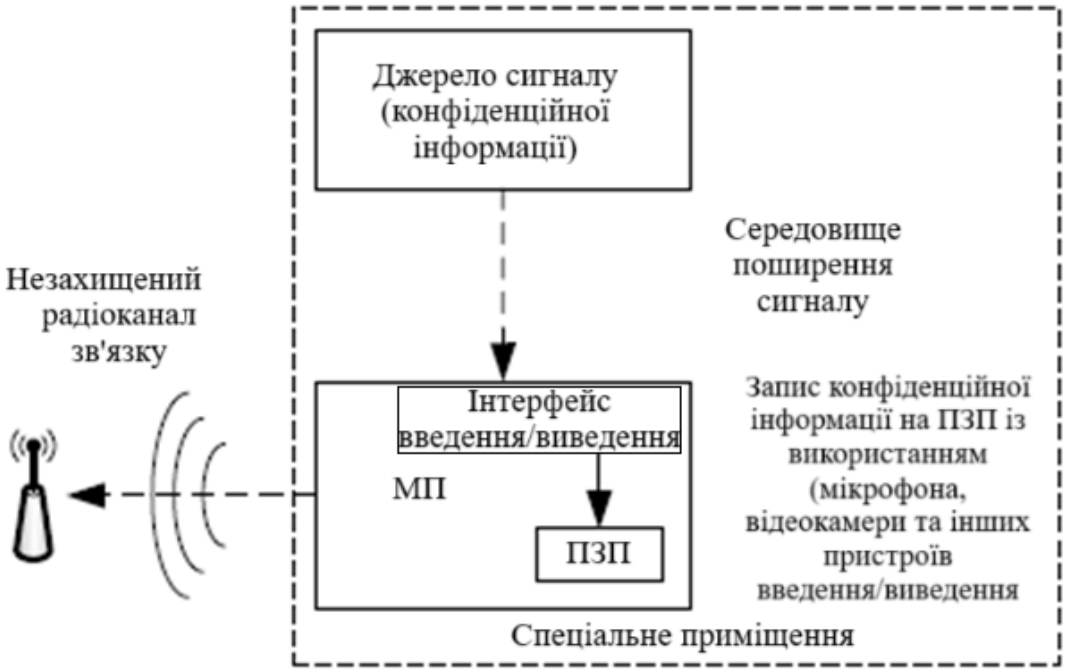

Рисунок 1.8 – Схема витоку інформації при несанкціонованому використанні МП у спеціальному приміщенні

На сьогоднішній день існує кілька СЗІ у вигляді рішень для управління МП, які дозволяють блокувати роботу МП в обмежених режимах. Однак ці рішення мають свої недоліки, оскільки працюють на рівні додатків і не завжди можуть

гарантувати повну безпеку враховуючи принципи недовіри до електроніки, ненадійності МП та відсутності довіри до сторонніх додатків.

З моменту виникнення нових загроз та вразливостей у сфері ІБ, виникає потреба у більш інтегрованих та надійних рішеннях для керування безпекою МП [38]. Новий підхід передбачає створення комплексних систем захисту, які поєднують у собі різноманітні методи та технології, включаючи апаратне забезпечення, алгоритми шифрування, а також засоби для моніторингу та виявлення небажаної активності.

Ці інтегровані рішення створюють основу для ефективного управління безпекою МП в корпоративних мережах, забезпечуючи високий рівень захисту навіть у ситуаціях, де традиційні MDM-системи можуть бути недостатньо надійними. Важливо надавати перевагу розробці та впровадженню таких інтегрованих рішень, які враховують особливості МП та ризики, пов'язані з їх використанням у сфері ІБ.

Контроль за введенням незахищених МП зазвичай здійснюється за допомогою організаційно-технічних заходів. Однак ці заходи можуть бути порушені, якщо немає ефективного контролю за їх виконанням. Таким чином, існує реальна потреба в розробці СЗІ, які можуть автоматично керувати як програмною, так і апаратною конфігурацією МП, блокуючи можливі канали витоку інформації при використанні пристроїв в організаціях, де передбачена обробка конфіденційної інформації, незалежно від їх розташування в організації.

Розроблювана система управління безпекою МП спрямована передусім на захист від загроз, таких як:

- обхід систем захисту інформації;
- деструктивні впливи на системи захисту інформації;
- перехоплення та модифікація переданої інформації;
- розголошення та витік інформації в незахищених місцях доступу;
- використання несанкціонованого програмного забезпечення;
- введення вразливостей за допомогою стандартних засобів.

Основними об'єктами захисту інформації під час впровадження СЗІ є:

– інформація, яку обробляють МП;

– інформація в засобах, що реалізують мережеву взаємодію, а також в каналах передачі даних в мережі;

– інформація, яку обробляють в спеціальних приміщеннях ЗКС.

Вище викладені моделі загроз та потенційних порушників ІБ при використанні МП дозволяють більш докладно сформулювати вимоги до системи управління безпекою МП та реалізованих СЗІ з метою забезпечення безпеки інформації в корпоративних мережах із різними вимогами до захисту.

1.4 Постановка задачі

Для отримання доступу до ресурсів корпоративних мереж із різними вимогами до безпеки використовуються різні МП з відповідними рівнями захисту, а забезпечення безпеки можна реалізувати за допомогою:

– встановлення спеціалізованих СЗІ;

– експлуатації корпоративних захищених МП.

Проте обидва підходи мають ряд недоліків. Аналіз формальних моделей безпеки для управління доступом користувачів до МП вказав на ряд недоліків, які впливають на адекватність моделей для реальних комп'ютерних систем і загрожують їх безпеці. Також виявлено необхідність використання єдиного МП для доступу до корпоративних мереж із різними вимогами щодо безпеки, тому потрібно створити умови для керування програмно-апаратною конфігурацією МП, яка виключатиме можливість технічних каналів витоку інформації при використанні єдиного МП для доступу до ресурсів корпоративних мереж із різними вимогами щодо безпеки.

Мета кваліфікаційної роботи магістра – розробка методу керування безпекою мобільних пристроїв в корпоративних мережах.

Для досягнення поставленої мети слід виконати наступне:

– розробити формальну моделі безпеки мобільного пристрою, яка спрямована на визначення потенційних загроз та вразливостей, що можуть виникнути в контексті використання мобільних пристроїв в корпоративних мережах;

– виконати моделювання місця розташування мобільного пристрою, що дозволить оцінити достовірність місцезнаходження мобільного пристрою у спеціальному приміщенні;

– розробити модель системи виявлення місця розташування мобільного пристрою, що дозволить оцінити ймовірність його місцезнаходження у спеціальному приміщенні з підвищеними вимогами щодо захищеності;

– розробити алгоритм визначення ймовірності місцезнаходження мобільного пристрою у спеціальному приміщенні;

– виконати оцінку властивостей алгоритму керування безпекою мобільного пристрою;

– надати пропозиції щодо складу, структури та місця системи управління безпекою мобільними пристроями у складі корпоративних мереж з різними рівнями захищеності;

– надати пропозиції щодо реалізації захищеного каналу управління між контролером доступу та мобільним пристроєм;

– надати рекомендації щодо оптимального взаємного розташування точок доступу бездротової мережі в системі виявлення місця розташування.

2 МОДЕЛЬ БЕЗПЕКИ МОБІЛЬНОГО ПРИСТРОЮ З РІЗНИМИ ВИМОГАМИ ДО ЗАХИЩЕНОСТІ

2.1. Вимоги до розробки моделі

Відмінною особливістю розробленої моделі є облік атрибутів доступу, включаючи місцезнаходження МП в спеціальних приміщеннях будівлі, в якому розгорнуті корпоративні мережі з різними вимогами щодо захищеності. Запропоновано модель безпеки МП, обґрунтовано її коректність. На основі аналізу технологій виявлення місця розташування МП в приміщеннях всередині будівель запропоновано технологічне рішення, що дозволяє підвищити достовірність виявлення місця розташування МП в приміщеннях з різними вимогами щодо захищеності за рахунок застосування методу статистичних випробувань. Обґрунтовано застосування запропонованого технологічного рішення для оцінювання місцезнаходження МП на території приміщень організації із заданою точністю. Розроблено імітаційну модель, що дозволяє оцінити оптимальні параметри алгоритмів виявлення місця розташування, проведено оцінку його якості.

Система управління безпекою МП, що розглядається як об'єкт дослідження в роботі, в корпоративних мережах з різними вимогами по захищеності може бути віднесена до комп'ютерної системи (КС). Відповідно до [39] при аналізі безпеки КС, які повинні володіти високим рівнем довіри, починаючи з оціночного рівня довіри 5 потрібно, щоб при розробці КС була використана формальна модель політики безпеки .

Для аналізу безпеки запропонованої в роботі системи управління МП та досягнення мети дослідження, що полягає у підвищенні ймовірності забезпечення безпеки інформації при експлуатації МП необхідно розробити модель безпеки МП, яка відрізняється від відомих обліком його місцезнаходження в корпоративних мережах з різними вимогами щодо захищеності. Формальна постановка задачі на розробку моделі: на основі теорій множин, кінцевих автоматів, машинного

навчання, математичної статистики та чисельних методів розробити модель безпеки МП

Запропонована в роботі модель безпеки МП базується на класичній моделі Бела-ЛаПадули [40-42]. Класична модель складається із наступних елементів:

S – множина суб'єктів системи;

MD – множина МП, при цьому $MD \subseteq S$;

O – множина об'єктів системи, включаючи функціональні блоки МП;

$P = \{read, write, append, execute\}$ – множина варіантів доступу і варіантів прав доступу;

$B = \{b \subseteq S * O * P\}$ – множина можливих множин поточного доступу у системі;

$(L, \leq)$ – решітка конфіденційності, де "OI" < "CI";

$M = \{m_{|s|*|O|}\}$ - множина можливих матриць доступу, де $m_{|s|*|O|}$ - матриця доступу, $m[s, o] \subseteq P$ – права доступу суб'єкта s до об'єкта o;

$(f_s, f_o, f_c, f_{loc}) \in F = L^s * L^o * L^s$ – четвірка функцій (f_s, f_o, f_c, f_{loc}), які задають відповідно: $f_s: S \to L$ – рівень доступу суб'єктів; $f_o: O \to L$ – 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;

$V = B * M * F$ – множина станів системи;

Q – множина запитів до системи;

D – множина відповідей на запити;

$W \subseteq Q * D * V^* * V$ – множина дій системи, де $(q, d, v*, v) \subseteq W$ означає що система за запитом q з відповіддю d перейшла із стану v в стан v*;

$N_o = \{0,1,2, \dots\}$ - множина значень часу;

X – множина функцій $x: N_o \to Q$, що задають всі можливі послідовності запитів до системи;

Y – множина функцій $y: N_o \to D$, що задає всі можливі послідовності відповідей системи за запитами;

Z – множина функцій z: $N_o \rightarrow V$, що задає всі можливі послідовності стану системи.

2.2. Розробка формальної моделі безпеки мобільного пристрою

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

Типовий склад сучасного МП представлений на рисунку 2.1. Очевидно, що такий пристрій здатний працювати в режимах, заборонених політикою безпеки ЗКС. Для блокування роботи МП у заборонених режимах необхідний механізм управління програмно-апаратною конфігурацією МП, наприклад, на основі апаратно-програмного модуля довіреного завантаження, що дозволяє забезпечити виконання вимог політики безпеки, встановлених у ЗКС.

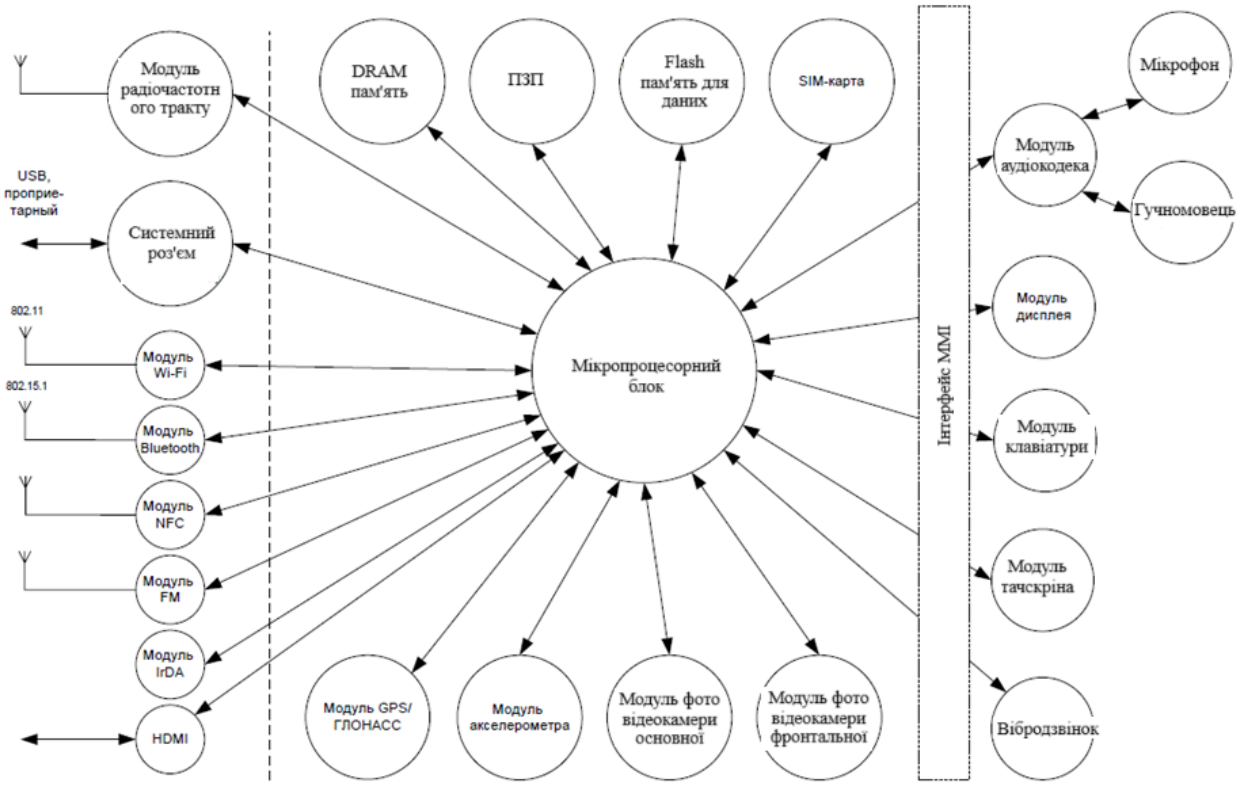

Рисунок 2.1 – Типова будова сучасного МП

У формальній моделі безпеки необхідно визначити стан КС, який визначається, в тому числі, програмно-апаратною конфігурацією МП, що забезпечує безпеку інформації за заданих умов доступу. Для визначення складу та структури допустимих змін МП доцільно розглянути інформаційні тракти проходження сигналів через МП під час роботи їх у різних режимах [43]. На рисунках 2.2 та 2.3 представлений склад задіяних функціональних блоків МП: при інформаційному обміні голосовою інформацією (без аудіозапису розмови на локальну пам'ять); при інформаційний обмін даними.

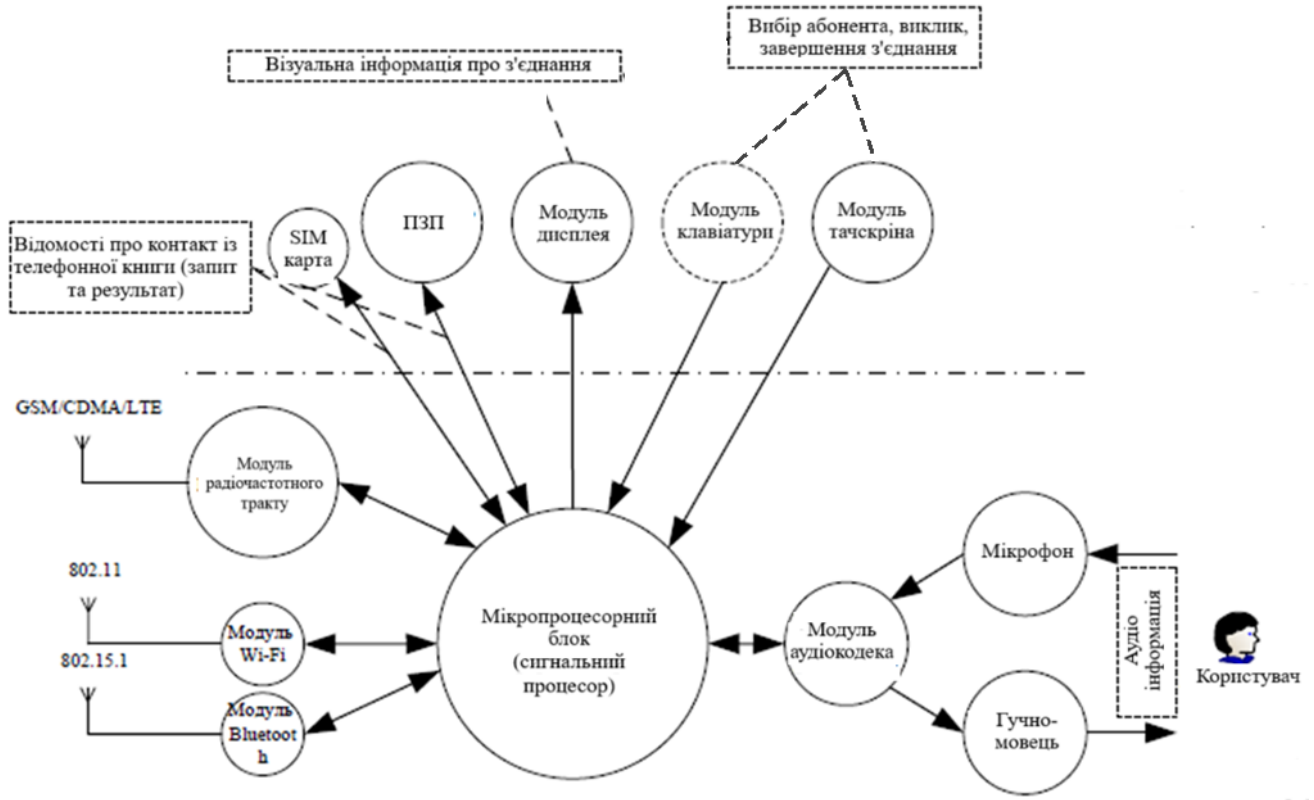

Рисунок 2.2 – Склад задіяних функціональних блоків МП при інформаційному обміні голосовою інформацією (без аудіозапису розмови на локальну пам'ять

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

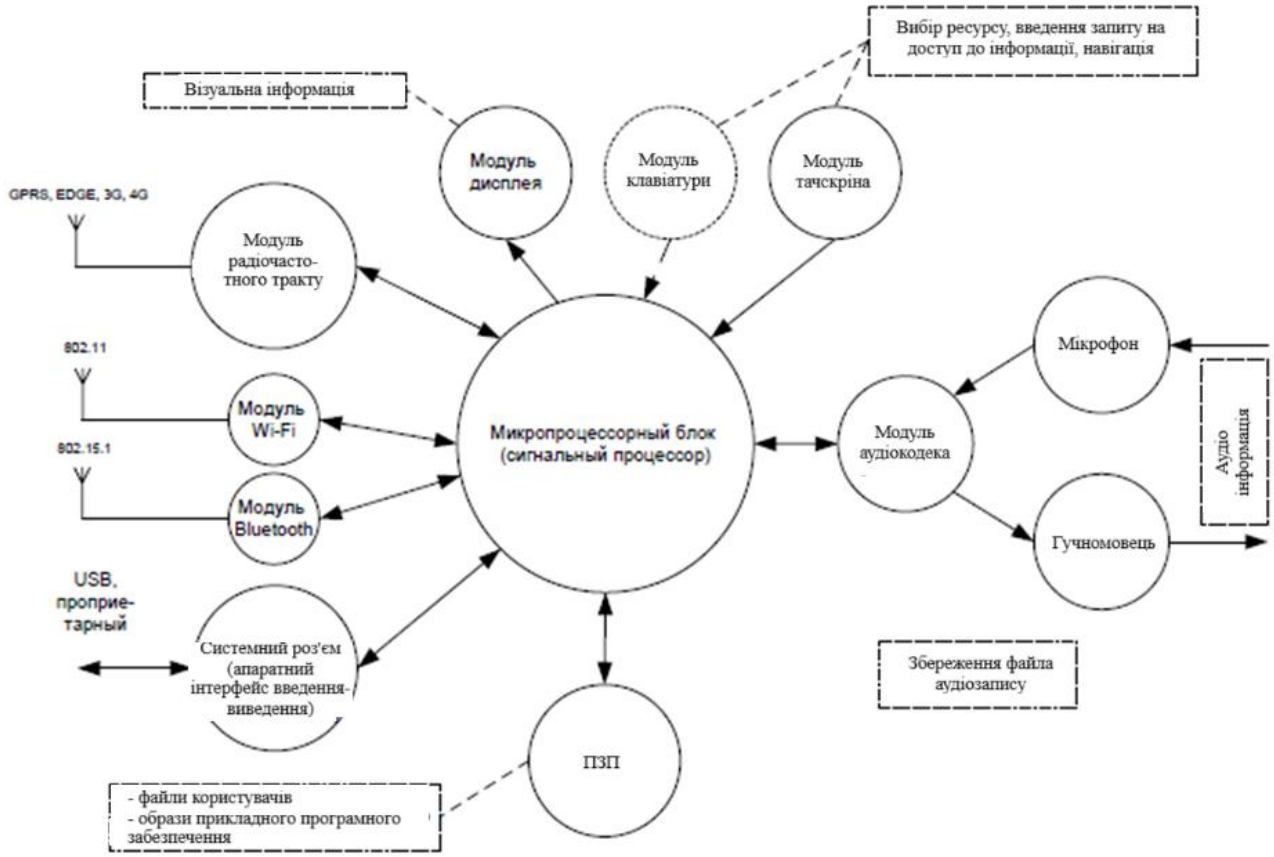

Рисунок 2.3 – Склад задіяних функціональних блоків МП під час обміну даних

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

– ідентифікаційні дані про користувача, МП, операційну систему (ОС) та додатках МП;

– мережна адресна інформація;

– рівень конфіденційності та ідентифікатор запитуваної послуги;

– час запиту на доступ.

Принципово важливим атрибутом доступу є розташування. Вимоги безпеки до технічних засобів, включаючи ЗОТ та МП в рамках нормативних документів, визначаються, як правило, приміщеннями, в яких дані пристрої знаходяться, в яких може бути передбачено обробку інформації з обмеженим доступом. Враховуючи, що місце розташування МП є випадковою величиною, а також недостатньо високу

точність виявлення місця розташування при використанні технологій стандарту 802.11, дану характеристику стану МП можна представити у вигляді вектора:

$$\overrightarrow{P_{L_R}} = \{P(\widetilde{L_R} = "OI"), P(\widetilde{L_R} = "CI")\}, \quad (2.1)$$

де $P(\widetilde{L_R} = "OI")$ – ймовірність того, що МП знаходиться в приміщенні з рівнем вимог щодо захищеності для відкритої інформації ("OI"); $P(\widetilde{L_R} = "CI")$ – ймовірність того, що МП знаходиться в приміщенні з рівнем вимог щодо захищеності для конфіденційної інформації ("CI").

Таким чином, для керування доступом у комп'ютерній системі з МП необхідно:

– множину об'єктів доступу *AO* доповнити множиною функціональних блоків МП: ПЗУ, ОЗУ, ЦП, АПМДЗ, модулі Bluetooth, дисплея, Wi-Fi, клавіатури, GSM, USB, тачскріна, фото- та відеокамери та інші;

– множину суб'єктів доступу *AS* доповнити множиною МП *MD*, таким що $MD \subseteq AS$;

– множину ролей U доповнити множиною можливих конфігурацій МП, так щоб $CONF \subseteq U$, при цьому кожна конфігурація (роль) визначається набором тих чи інших прав та видів прав доступу на об'єкти доступу, що включають у собі, зокрема, функціональні блоки МП;

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

– визначити властивості системи захисту, які враховують рівні конфіденційності розташування та особливості програмно-апаратних конфігурацій МП з урахуванням мандатного розмежування доступу та особливостей функціонування системи виявлення місця розташування МП.

2.3. Моделювання місця розташування мобільного пристрою

Необхідно зазначити, що за рамками формальної моделі безпеки МП та поданих доказів залишилася проблема точності виявлення місця розташування МП і, зокрема, точність виявлення місця розташування МП у приміщеннях усередині будівлі. На відміну від розташування на відкритій місцевості всередині будівель немає можливості використовувати супутникову навігацію через слабкий сигнал, при цьому СЗІ вимагають точності, сумірної з точністю, що досягається у супутникових системах навігації.

До базових принципів, на яких ґрунтуються всі способи виявлення місця розташування, відносяться:

– тріангуляція та трилатерація – оцінювання розташування на основі геометричних властивостей кутів до об'єкта (тріангуляція) або відстаней від трьох і більше об'єктів з відомим місцезнаходженням (трилатерація);

– аналіз карти вимірювань – оцінка місця розташування на основі карти точок вимірювань параметрів сигналу (карти сигнального простору);

– аналіз близькості – визначення місця розташування по близькості до приймача сигналу щодо інших;

– аналіз динаміки руху.

Порівняльний аналіз технологій виявлення місця розташування за точністю та призначенням наведено на рисунку 2.4.

Аналізуючи рисунок, можна зробити висновок, що технологій, які використовуються для визначення розташування, відносно небагато. До них відносяться GSM/CDMA/3G, RFID/Bluetooth/Wi-Fi, а також технології, що використовують лазерні далекоміри та датчики, що вимірюють орієнтацію у просторі – альтиметри, гіроскопи та 3Д-акселерометри. Сучасний технологічний рівень не дозволяє використовувати інерційні датчики в якості основи для системи виявлення місця розташування в приміщеннях внаслідок ефекту накопичення помилки за короткостроковий період. Дані недоліки були частково усунені в

подальших технологіях що використовує як додаткову розмірність, що характеризує місце розташування МП всередині будівлі, графічний потік, що отримується з вбудованої в МП камери, і відповідну йому базу даних координат у вигляді 3Д-моделі будівлі. Очевидно, що дана технологія не застосовується в ЗКС через вимог ІБ.

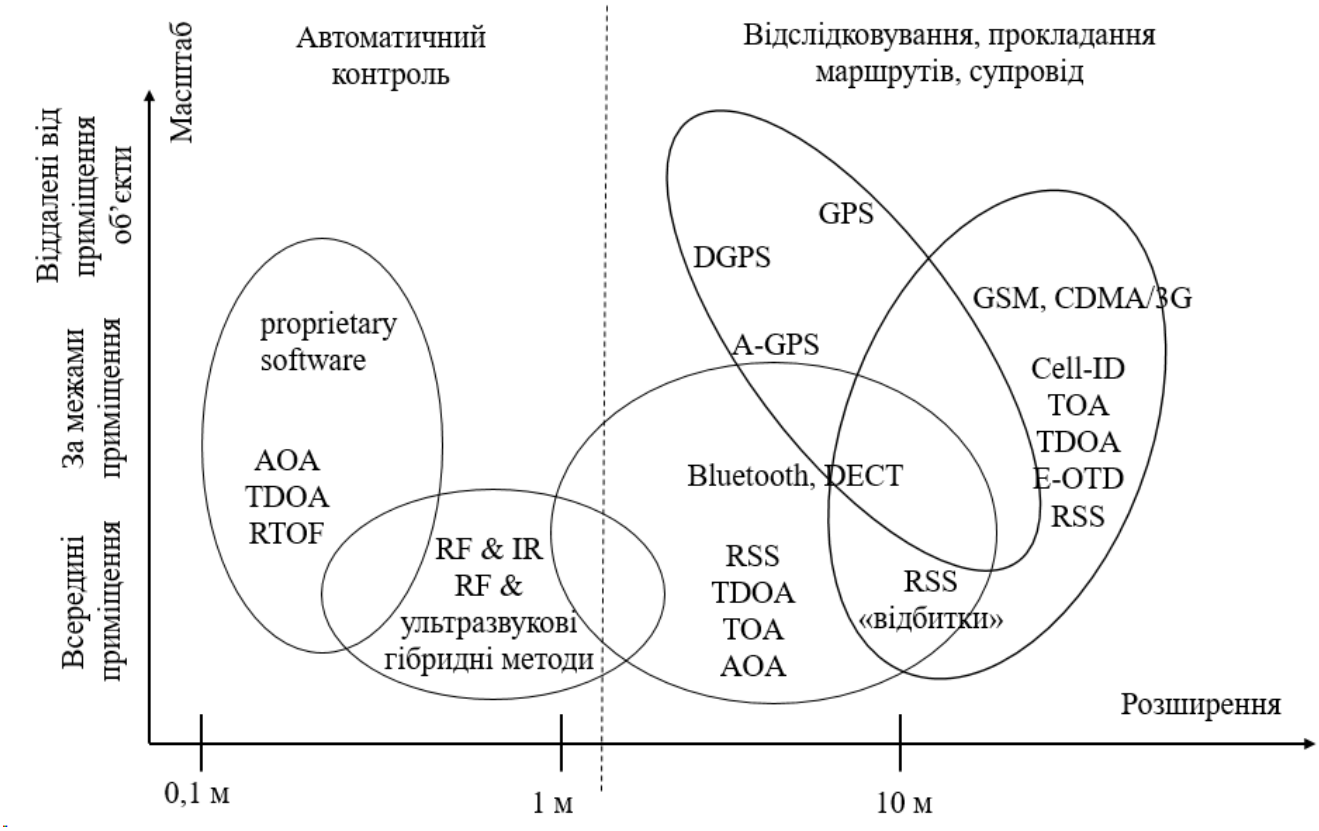

Рисунок 2.4 – Порівняння технологій виявлення місця розташування

Технології супутникової навігації не застосовуються всередині приміщень через значне згасання сигналу від супутників [44]. Технології на базі сигналів GSM/CDMA/3G/LTE мають низьку точність для вирішення задачі визначення місця розташування МП. Ультразвукові методи, методи радіочастотної ідентифікації (RFID) не дозволяють організувати захищений канал управління МП, а деякі з них не забезпечують, у тому числі, ідентифікацію МП.

До системи виявлення місця розташування МП висувається ряд вимог, виконання яких впливає на забезпечення конфіденційності інформації:

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

– повинна забезпечуватися ідентифікація користувача МП у системі виявлення місця розташування.

Виходячи з аналізу рисунка 2.4, а також відомих особливостей технічних реалізацій зазначених технологій, прийнятну точність визначення розташування всередині будівлі, а також ідентифікацію користувача МП, дозволяють забезпечувати методи, засновані на застосуванні радіочастотної ідентифікації, а також методи, засновані на застосуванні безпровідної мережі передачі даних. На основі [45-46] було проведено порівняльний аналіз даних технологій. Результати аналізу представлені у таблиці 2.1.

Таблиця 2.1 – Порівняльний аналіз ефективності датчиків радіочастотної ідентифікації і Wi-Fi для вирішення завдання виявлення місця розташування МП

Показник	Технологія	
	RFID	Wi-Fi
Точність	менше 1м	1-7м
Складність реалізації	середня	Низька/середня (для систем з навчанням)
Масштабованість	низька	хороша
Стійкість до перешкод	низька	хороша
Стійкість до атак типу «людина посередині»	низька	висока
Можливість створення каналу управління МП	відсутня	є

На відміну від RFID-технології, способи визначення місця розташування на основі безпровідної мережі передачі даних позбавлені даних недоліків, але при

цьому мають більш високу вартість і меншу точність визначення місця розташування МП. У ряді наукових публікацій пропонується використовувати комбіновані технічні рішення, що дозволяють компенсувати недоліки обох.

Завдання визначення місцезнаходження і завдання захищеної інформаційної взаємодії може вирішуватися з використанням єдиного модуля бездротового зв'язку стандарту 802.11, або може бути розділена на технологічно незалежні бездротові модулі. Для сигналів стандарту 802.11 рішення задачі виявлення місця розташування може бути здійснено з використанням методів тріангуляції (трилатерації) та аналізу карти сигнального простору. Слід зазначити, що метод трилатерації не вимагає проведення попередніх вимірювань рівня сигналів мережі на відміну від методів аналізу картки вимірів, що суттєво спрощує її розробку, експлуатацію та супровід. Однак у той же час підсистеми виявлення місця розташування, засновані на методі трилатерації, мають набагато нижчу точність порівняно з системами на основі аналізу карти сигнального простору.

При визначенні місця розташування суттєве значення має не стільки координати знаходження МП, скільки приміщення, в якому воно знаходиться. Причина цього полягає в тому, що вимоги безпеки визначаються саме приміщенням, в якому знаходиться МП. Очевидно, що приміщення – це значно грубший об'єкт для розпізнавання порівняно з координатами МП. Кожна з розглянутих технологій виявлення місця розташування на базі безпровідної мережі передачі даних і стандарту 802.11 призначена саме для обчислення координат точки розташування МП 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 МП, а про коло, в межах якого може знаходитися пристрій, при цьому радіус даного кола дорівнює максимальній похибці визначення місцезнаходження для заданої технології. В межах даного кола можуть знаходитися різні приміщення з різними вимогами щодо захищеності. Для підвищення достовірності визначення місцезнаходження МП в спеціальних приміщеннях, до яких пред'являються підвищені вимоги щодо захищеності,

необхідно обчислити площу приміщень кожного рівня захищеності, що знаходяться всередині кола, що визначає ймовірне місцезнаходження МП. Відношення отриманої площі приміщень до загальної площі даного кола дозволить визначити ймовірність знаходження МП у спеціальному приміщенні.

Як базові технології, що використовують безпровідні мережі передачі даних для визначення місця розташування, а також для обґрунтування алгоритмічної розв'язності пропонованого підходу з обчислення ймовірності знаходження МП у спеціальному приміщенні незалежно від вибраного методу, пропонується використовувати технології, засновані на застосуванні:

– методу трилатерації (тріангуляції) сигналу МП, що приймається декількома точками доступу безпровідної мережі передачі даних [47];

– методу k-найближчих сусідів [48];

– методу, заснованого на використання байєсовського підходу [49].

Вибір даних методів обумовлений:

– різною обчислювальною складністю;

– різними вимогами щодо обслуговування та обчислювальної потужності;

– різною похибкою виявлення місця розташування.

Розв'язання задачі обчислення площі приміщень кожного рівня захисту, що знаходяться всередині кола і визначає ймовірне місце знаходження МП, необхідно вирішувати, виходячи з наступних умов:

– конфігурація та розташування приміщень заздалегідь відома;

– координати точки розташування МП та розташування кола, в межах якої може бути МП, щоразу обчислюється відомими методами;

– конфігурація та розташування приміщень усередині даного кола є геометричні об'єкти довільної форми;

– максимальний радіус кола, в межах якого може знаходитися МП, залежить від використовуваної технології виявлення місця розташування і

дорівнює максимальному значенню помилки виявлення місця розташування для заданої технології, що отримується емпіричним шляхом.

За вказаних умов використання класичного геометричного підходу для обчислення площі фігури є неприйнятним, в першу чергу, у зв'язку із необхідністю обчислення площі фігур довільної конфігурації в кожний момент часу та необхідністю обліку великої кількості можливих варіантів. Найбільш підходящим способом визначення площ довільних фігур є метод статистичних випробувань - метод Монте-Карло [50]. Даний метод дозволяє визначити площу довільної фігури всередині кола, що визначає ймовірне місцезнаходження МП, проте може знадобитися попереднє навчання.

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

Застосування методу Монте-Карло для обчислення ймовірності знаходження МП у спеціальному приміщенні при використанні спільно з технологіями визначення місцезнаходження на базі безпровідної мережі передачі даних дозволить знизити вплив нестійкості радіосигналів безпровідної мережі передачі даних на помилку визначення місця розташування МП та підвищити достовірність обчислення ймовірності перебування МП в спеціальному приміщенні ЗКС.

2.4 Модель системи визначення місця розташування мобільного пристрою

Ключове значення для визначення вимог безпеки, що висуваються до МП, мають не так координати його місцезнаходження, скільки інформація про приміщення, в якому він знаходиться. Тому для вирішення задачі визначення ймовірності місцезнаходження МП в спеціальному приміщенні необхідні відомості про склад та параметри приміщень ЗКС. Дані відомості характеризують описову модель будівлі та можуть бути подані у вигляді:

$$R = \left\{\left((x_{i1}, y_{i1}), \dots, (x_{in}, y_{in}), L_{R_i}\right)\right\}, i = \overline{1, N_R}\,, \tag{2.2}$$

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

В результаті визначення місця розташування у відповідності з представленими моделями виявлення місця розташування МП можуть бути отримані координати МП – $(\tilde{x}, \tilde{y})$. Помилка визначення місця розташування в цьому випадку з урахуванням того, що реальне положення МАУ – (x, y), обчислюється за допомогою виразу:

$$e_L = \sqrt{(x - \tilde{x})^2 + (y - \tilde{y})^2}. \tag{2.3}$$

Реальне місце розташування користувача МП знаходиться в межах кола з центром із координатами $(\tilde{x}, \tilde{y})$ і радіусом, рівним максимальному значенню похибки вимірювання розташування $U_e = max[e_L]$. Враховуючи, що величина U_e порівнювана з розмірами приміщень, то реальне місце розташування користувача МП може значно відрізнятися від обчисленого, тому рішення задачі визначення ймовірності місцезнаходження МП в спеціальному приміщенні є нетривіальним і вимагає врахування додаткових факторів. Графічна ілюстрація даної задачі представлена на рисунку 2.5.

Аналізуючи рисунок 2.5 видно, що реальне місце розташування МП (x, y) може знаходитися в приміщеннях будь-якого рівня вимог щодо захищеності, оскільки в радіусі максимальної помилки вимірювання розташування U_e 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, що впливають випадковим чином, а також обраної технології виявлення місця розташування. Враховуючи, що карта розташування приміщень відома, а також може бути отримана емпіричним шляхом (на етапі навчання системи) статистичні параметри похибки виміру розташування можна оцінити ймовірність того, що

користувач знаходиться в приміщенні із заданим рівнем вимог захищеності.

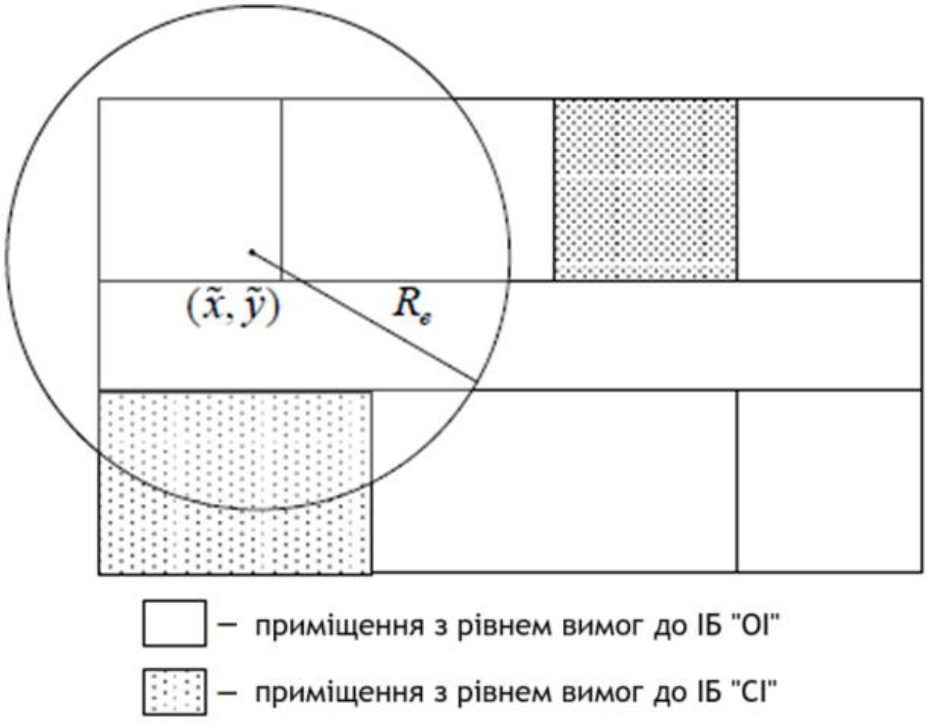

Рисунок 2.5 – Завдання визначення ймовірності місцезнаходження МП у спеціальному приміщенні

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

$$P\left(\widetilde{L_R} = L_R\right) = \frac{F_{AS_q}(L_R, (\tilde{x}, \tilde{y}), U_e)}{\pi * U_e^2}, \quad (2.4)$$

де L_R – заданий рівень вимог щодо захищеності, для якого здійснюється оцінювання; U_e - радіус кола, що характеризує максимальну похибку визначення

розташування; $(\tilde{x}, \tilde{y})$ – координати визначеного місцезнаходження; $F_{AS_q}(L_R, (\tilde{x}, \tilde{y}), U_e)$ – функція, що обчислює площу приміщень з рівнем L_R, що знаходяться всередині кола з центром у точці $(\tilde{x}, \tilde{y})$, радіусом U_e та площею $\pi * U_e^2$.

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

$$P_{L_R} = \left\{P\left(\widetilde{L_R} = \text{"OI"}\right), P(\widetilde{L_R} = \text{"CI"})\right\}. \quad (2.5)$$

Функція визначення $F_{AS_q}(L_R, (\tilde{x}, \tilde{y}), U_e)$ для довільної конфігурації розташування приміщень, а також довільних значень $(\tilde{x}, \tilde{y})$ і U_e є важкою задачею для геометричних методів, проте вона легко може бути вирішена чисельним методом на основі методу статистичних випробувань (методу Монте-Карло). Даний метод заснований на отриманні великої кількості реалізації стохастичного (випадкового) процесу, що формується таким чином, щоб його ймовірнісні характеристики збігалися з аналогічними величинами розв'язуваної задачі.

Реалізація методу Монте-Карло з метою вирішення задачі обчислення функції $F_{AS_q}(L_R, (\tilde{x}, \tilde{y}), U_e)$ полягає в наступному:

– за допомогою генератора випадкових чисел із заданим законом розподілу ймовірностей формуються координати випадкової точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ таким чином, щоб вони лежали всередині кола з центром у точці $(\tilde{x}, \tilde{y})$ і радіусом U_e, де N_{MC} – кількість експериментів;

– визначається приміщення, в якому знаходиться поточна точка (x_i', y_i') та відповідний йому рівень вимог щодо ІБ – $\widetilde{L_R} = F_{L_R}\left((x_i', y_i'), R\right)$, де $R = \left\{r_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \dots (x_{in}, y_{in}), L_R\right)\right\}$ – розташування та рівні вимог щодо захищеності приміщень, $i = \overline{1, N_R}, (x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \dots (x_{in}, y_{in})$ – координати n кутів приміщень N_R – кількість приміщень.

– лічильник входів в приміщення з $L_{R_i} = \widetilde{L_R}$ збільшується на одиницю -

$N(L_{R_i}) \coloneqq N(L_{R_i}) + 1.$

Закон розподілу ймовірностей для випадкових величин – координат точки $(x_i', y_i'), i = \overline{1, N_{MC}}$ залежить від використовуваної технології виявлення місця розташування. Величина (x_i', y_i') характеризує обчислене місце розташування МП і формується на основі статистики вимірів помилок визначення місця розташування. Збір цієї статистики складає етапі розгортання Wi-Fi.

Оскільки конфігурація приміщень у різних будинках відмінна одна від іншої, матеріали стін, міжкімнатних перекритів та дверей вносять спотворення в поширення радіосигналу і сам сигнал Wi-Fi досить нестабільний, то доцільно статистику вимірювань помилок виявлення місця розташування подати у вигляді гістограми частот (ряду розподілу):

$$\lambda_{e_L} = \left\{R_e, P\{a \le a_L < b\} = \sum_{a \le e_L < b} p(e_L) \,\middle|\, \sum_{0 \le e_L < R_e} p(e_L) = 1\right\}, \qquad (2.6)$$

де R_e – максимальне значення похибки виявлення місця розташування; $P\{a \le a_L < b\}$ – ймовірність того, що похибка виявлення місця розташування знаходиться на відрізку *(a,b)*, де *a* – нижня межа, *b* – верхня межа; $\sum_{a \le e_L < b} p(e_L)$ – сума ймовірностей виникнення помилки визначення місця розташування, що рівна величині $e_{L.}$

В результаті застосування методу Монте-Карло значення функції $F_{S_q}(L_R, (\tilde{x}, \tilde{y}), R_e)$ розраховується як:

$$F_{S_q}(L_R, (\tilde{x}, \tilde{y}), R_e) = \frac{N(L_R)}{N_{MC}}, \qquad (2.7)$$

а оцінка ймовірності того, що користувач знаходиться в приміщенні того чи іншого рівня захисту:

$$P_{L_R} = \left\{ \frac{N(\widetilde{L_R} = \text{"OI"})}{N_{MC}}, \frac{N(\widetilde{L_R} = \text{"CI"})}{N_{MC}} \right\} \tag{2.8}$$

Точність даного методу суттєво залежить від кількості випробувань – N_{MC} та параметрів генератора випадкових чисел, що використовується для формування координат випадкової точки $(x_i', y_i'), i = \overline{1, N_{MC}}$. Похибку можна розрахувати як $\varepsilon = \frac{1}{\sqrt{N_{MC}}}$. Таким чином при точності $\varepsilon_{\text{потрібне}}$ необхідна кількість дослідів становитиме $N_{MC} \approx \frac{1}{\varepsilon^2_{\text{потрібне}}}$.

Критерій прийняття рішення про рівень захищеності приміщення можна представити наступним співвідношенням:

$$\widetilde{L_R} = \begin{cases} \text{"OI"}, \text{при } \dfrac{N(\widetilde{L_R} = \text{"OI"})}{N_{MC}} \geq L_K^{\text{потрібне}} \\ \text{"CI"}, \text{при } \dfrac{N(\widetilde{L_R} = \text{"CI"})}{N_{MC}} < L_K^{\text{потрібне}} \end{cases} \tag{2.9}$$

де граничне значення для критерія $L_K^{\text{потрібне}}$ визначається таким чином, щоб виконувалася вимога щодо кількості помилок 2-го роду:

$$P_\beta\left(\widetilde{L_R} > L_R\right) \leq P_\beta^{\text{дод}} \tag{2.10}$$

Важливим завданням системи управління безпекою МП є забезпечення конфіденційності інформації. Базуючись на цьому, граничне значення $L_K^{\text{потрібне}}$ повинне обиратися таким чином, щоб конфіденційність інформації була забезпечена. Критичним показником достовірності визначення місця розташування МП у спеціальних приміщеннях є величина похибки 2-го роду. Таким чином, значення критерія прийняття рішення про рівень захищеності приміщення та вимога щодо кількості помилок 2-го роду дозволяють регулювати рівні похибок 1-

го та 2-го роду під час прийняття рішення про місцезнаходження МП.

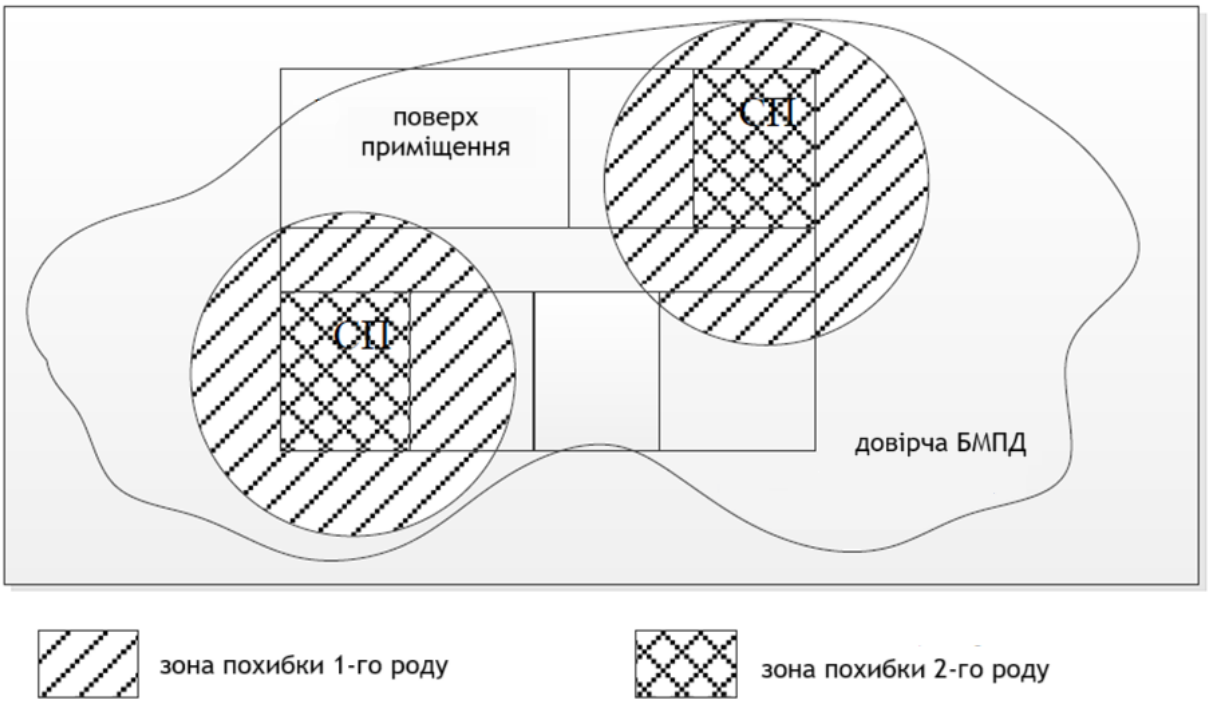

Рисунок 2.6 – Графічне подання похибок 1-го та 2-го роду щодо місцезнаходження МП у спеціальних приміщеннях

Графічно зони похибок 1-го та 2-го роду представлені на рисунку 2.6 Похибки 2-го роду є критичними, оскільки порушують конфіденційність інформації, тоді як похибки 1-го роду спричиняють лише порушення доступності деяких послуг, що надаються користувачеві МП.

2.5 Висновки до розділу

У параграфі 2.1 зроблено опис елементів моделі безпеки МП, яка базуватиметься на класичній моделі Бела-ЛаПадули. Дана модель відрізняється від відомих моделей наявністю обліку місцезнаходження МП в корпоративних мережах з різними вимогами щодо захищеності.

У параграфі 2.2 описано типову будову МП та використання різних функціональних блоків при різних способах передачі даних, зокрема при

інформаційному обміні голосовою інформацією (без аудіозапису) та під час обміну даних повідомленнями. Здійснено опис атрибутів доступу, які можуть бути пов'язані з користувачем МП, станом програмно-апаратного середовища МП, адресною інформацією та іншими параметрами при яких повинні блокуватися заборонені режими роботи МП.

У параграфі 2.3 описано базові принципи за допомогою яких можна визначити місце розташування об’єкта. Проведено порівняння технологій виявлення місця розташування на основі яких зроблено висновки, що для визначення локації можна використовувати GSM, CDMA, 3G, RFID, Bluetooth, Wi-Fi технології. Обґрунтовано використання Wi-Fi, що дозволяє одночасно здійснювати як вимірювання рівня сигналу МП точками доступу, так і захищену інформаційну взаємодію між МП і ЗКС, знижуючи тим самим витрати при проектуванні і супроводі в порівнянні з системами визначення місцезнаходження на основі датчиків та інших технологій.

Модель системи виявлення місця розташування МП, що дозволяє оцінити ймовірність його місцезнаходження у спеціальному приміщенні з підвищеними вимогами щодо захищеності висвітлено у параграфі 2.4.

3. АЛГОРИТМ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНОГО ПРИСТРОЮ

3.1. Алгоритм визначення ймовірності місцезнаходження мобільного пристрою у спеціальному приміщенні

На основі обчисленого розташування МП можна визначити приміщення, в якому імовірно знаходиться даний пристрій. Рівень захищеності приміщення, атрибути доступу та встановлена в ЗКС політика безпеки в сукупності визначають вимоги безпеки до МП, які можуть бути представлені у вигляді пакета, профілю захисту або завдання безпеки. На рисунку 3.1 представлено алгоритм визначення ймовірності місцезнаходження МП у спеціальному приміщенні на основі методу Монте-Карло.

У блоці 1 алгоритму здійснюється введення вихідних даних:

– отримані емпіричним шляхом дані про вибіркове середнє значення похибки вимірювання розташування для використовуваного алгоритму визначення місцезнаходження та вибірково середньоквадратичне відхилення похибки визначення місця розташування;

– параметр, що визначає число "сигма", що враховується при обчисленні радіусу зони похибки виявлення місця розташування;

– кількість випробувань для реалізації методу Монте-Карло;

– обчислене розташування користувача МП;

– гістограма частот щільності ймовірності розподілу помилки визначення місця розташування;

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

У блоці 2 здійснюється ініціалізація початкових значень для:

– радіуса зони, що визначає ймовірне місце розташування користувача МП;

– початкові значення вектору ймовірностей, що визначає ймовірність

віднесення до того чи іншого рівня захищеності обчислене місце розташування МП.

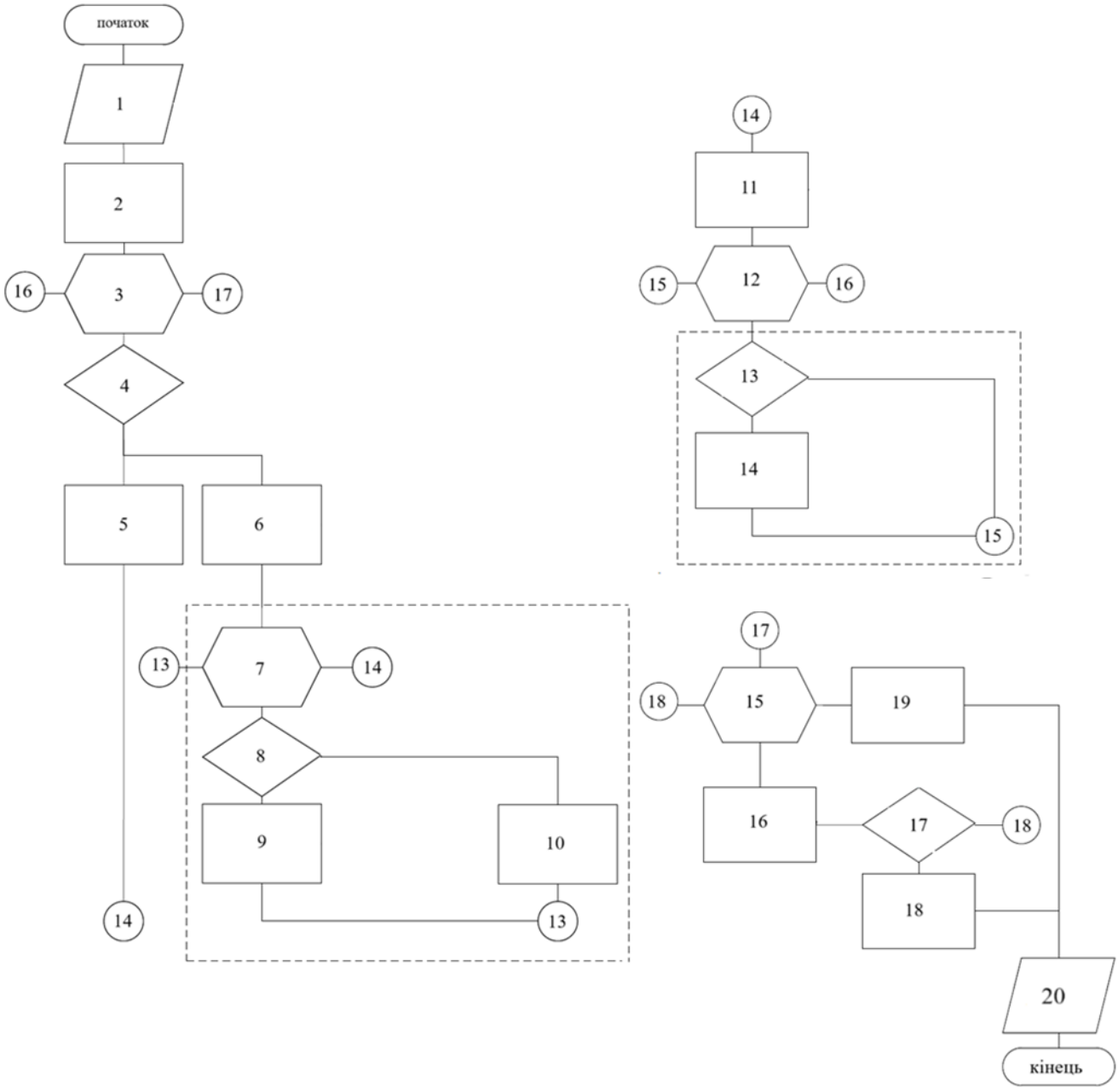

Рисунок 3.1 - Блок-схема алгоритму визначення ймовірності знаходження МП у спеціальному приміщенні та прийняття рішення про вимоги щодо рівня його захищеності

У блоці 3 реалізований ітератор циклу обчислень випробувань у відповідність до методу Монте-Карло.

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

У блоці 5 задається значення радіуса зони, що визначає ймовірне місце розташування МП, для рівномірного закону розподілу ймовірностей випадкової величини процесу, що використовується в методі Монте-Карло.

У блоках 6-10 реалізовано моделювання випадкового процесу відповідно до закону розподілу ймовірностей похибки обчислення місцезнаходження, що визначається гістограмою частот і емпіричними даними. У процесі моделювання обчислюється значення радіуса зони, що визначає можливе місце розташування МП, для емпіричного закону розподілу ймовірностей випадкової величини процесу, що використовується 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.

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

У блоках 15-19 здійснюється розрахунок ймовірності знаходження МП в приміщеннях з різними рівнями захищеності, що виконується на основі методу Монте-Карло і заданого порога прийняття рішення.

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

Математичні вирази для розрахунку ймовірності знаходження МП у спеціальному приміщенні та прийняття рішення про рівень захищеності приміщення, в якому імовірно знаходиться МП представлені формулами 2.2-2.9.

3.2. Властивості розробленого алгоритму керування безпекою мобільного пристрою

Для розробленого алгоритму управління безпекою МП було проведено оцінку наступних основних властивостей:

- результативність;
- елементарність;
- коректність;
- обчислювальна складність;
- складність алгоритму пам'яті;
- точність;
- співпадіння.

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

Даний алгоритм є елементарним, оскільки містить блоки, що виконують прості операції: присвоєння, обчислення математичних виразів та порівняння. Для блоків, що не є елементарними, призначених для перетворення вихідних даних, елементарність досягається докладним описом операцій, що здійснюються над даними в цих блоках. Не елементарними блоками розробленому алгоритмі є лише блоки вимірювання рівня сигналу, прийнятого точками доступу. У цьому блоці реалізується операція виведення даних із драйвера модуля бездротового зв'язку, що містять інформацію про рівень потужності сигналу, що приймається від МП.

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

Загальна часова складність алгоритму визначається часом ініціалізації $T_{ін}$ і часом, що витрачається на процедури виявлення місця розташування T_{LOC}, формуванням вимог безпеки T_{POLICY} і формування конфігурації МП T_{CONF}. Таким чином складність алгоритму становить:

$$S_t = T_{\text{ін}} + T_{LOC} + T_{POLICY} + T_{CONF}, \quad (3.1)$$

де $T_{LOC} = \{t_{\text{трилат}}, t_{kNN}, t_{\text{НММ}}\}$, $t_{\text{трилат}}$ – складність алгоритму трилатерації, t_{kNN} – складність алгоритму виявлення місця розташування на основі методу k-найближчих сусідів, t_{HMM} – складність алгоритму виявлення місця розташування на основі байєсівського підходу.

Найбільш трудомісткими процедурами є процедури виявлення місця розташування методами k-найближчих сусідів, методом на основі байєсівського підходу та процедура формування вимог безпеки $T_{POLICY.}$

Складність алгоритму визначення місця розташування методом k-найближчих сусідів складає:

$$t_{kNN} \sim k * N_{kNN}, \quad (3.2)$$

де k – число «сусідів», N_{kNN} – число точок сигнального простору.

Складність алгоритму визначення місця розташування методом на основі байєсівського підходу складає:

$$t_{\text{НММ}} \sim N_{AP} * N_{Int} + k * N_{\text{НММ}}, \quad (3.3)$$

де N_{AP} - кількість точок доступу безпровідної мережі; k – число найбільш вірогідних станів; N_{Int} – кількість інтервалів гістограми частоти для функції щільності розподілення ймовірностей похибки визначення місця розташування; N_{HMM} – кількість точок сигнального простору.

Складність алгоритму формування вимог безпеки залежить від кількості приміщень та заданої кількості випробувань методу Монте-Карло. Таким чином

$$T_{POLICY} \sim N_{MC} N_{Int} N_R, \tag{3.4}$$

де N_{MC} – задана кількість випробувань для методу Монте-Карло; N_{Int} – кількість інтервалів гістограми частоти для щільності розподілення ймовірності похибки визначення місця розташування; N_R – кількість приміщень. Таким чином складність алгоритму за часом буде складати:

$$S_t = C_1(N_{AP} * N_{Int} + k * N_{\text{НММ}}) + C_2 * N_{MC} * N_{Int} * N_R, \tag{3.5}$$

де C_1, C_2 – константи.

В якості вихідних технічних характеристик задано наступні параметри МП: потужність передавача 0,08Вт; частота передавача 2,4ГГц; розташування, рівні захисту та інші параметри приміщення визначаються схемою приміщення, яку представлено на рисунку 88 при розмірі приміщення 16,8м х 38,0м. Точки доступу безпровідної мережі в системі координат досліджуваного приміщення розташовані наступним чином: AP_1=(3,6м;19,2м), AP_2=(3,6м;5,2м); AP_3=(20,0м;12,0м); AP_4=37,6м;5,2м); AP_5=(37,6м; 19,2м).

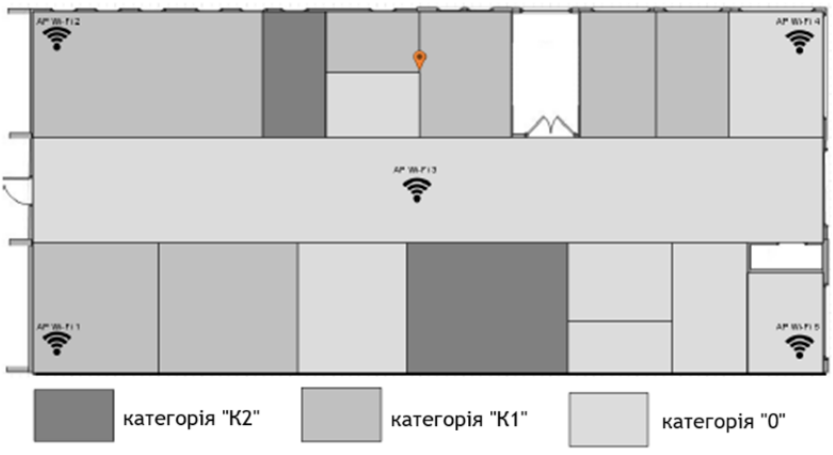

Рисунок 3.1 – Схема приміщень для проведення дослідження

Нормативи інформаційної швидкості для послуг, що надаються користувачу МП, вказано у таблиці 3.1.

Таблиця 3.1 - Нормативи інформаційної швидкості для послуг, що надаються користувачу МП

Послуга	КБ/с
Відеоконференція	384
Електронний поштовий обмін	64
Робота в режимі VoIP-клієнта	128
Надсилання мультимедійних повідомлень через мережу стільникового зв'язку	128
Прийом та передача захищених SMS повідомлень	64
Захищений відеоконференцзв'язок	512
Захищена IP-телефонія	256
Захищений електричний поштовий обмін	64
Захищений доступ до передачі даних бездротовими каналами зв'язку Wi-Fi (802.11n)	10000

Складність алгоритму пам'яті дорівнює $S_v = N_{AP} * N_{Int} * N_{\text{НММ}} + N_R$. Така оцінка складності поліноміальна. У процесі визначення місцезнаходження методом на основі байєсівського підходу необхідно зберігати дані про всі приміщення, а також статистику умовних ймовірностей спостереження рівнів потужності сигналу МП в N_{HMM} точках сигнального простору.

Точність розробленого алгоритму визначається похибкою обчислень, яка складається із $\delta_н$ – непереборні похибки вихідних даних, $\delta_м$ – похибки методу; $\delta_в$ – похибка обчислення.

$$\delta = \delta_{\text{н}} + \delta_{\text{м}} + \delta_{\text{в}}. \quad (3.6)$$

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

$$\delta_{\text{н}} = 10^{-N+1}, \tag{3.7}$$

де N – довжина мантиси.

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

Для оцінки похибки методу керуватимемося наступними правилами:

- при сумуванні чисел одного знаку точність суми дорівнює найменшій точності будь-якого доданку:

$$\delta_{\text{м}}^{+} = \sup(\delta_1, \delta_2, \dots, \delta_n). \tag{3.8}$$

- при відніманні чисел відбувається збільшення найбільшої відносної похибки одного з компонентів виразу в v раз, де

$$v = \frac{|a+b|}{|a-b|}, \tag{3.9}$$

тоді

$$\delta_{\text{м}}^{-} = \sup(\delta_1, \delta_2, \dots, \delta_n) * v, \tag{3.10}$$

де a і b – величини, що входять до операції віднімання.

- добуток і частка двох величин мають похибку, приблизно рівну сумі відносних похибок компонентів виразів:

$$\delta_{\text{м}}^{\text{х}} \approx \sum_{i=1}^{n} \delta_i \tag{3.11}$$

$$\delta_{\text{м}}^{\div} \approx \sum_{i=1}^{n} \delta_i \tag{3.12}$$

- для оцінки похибки функцій використовуються такі співвідношення:

$$\delta_{\text{м}}^{y} \approx v * \delta_{\text{н}}(x), \tag{3.13}$$

де

$$v = \frac{|x| * |f'(x)|}{f(x)}, \tag{3.14}$$

де $y=f(x)$ – досліджувана функція; x – аргумент досліджуваної функції; y – обчислене значення функції. Таким чином, розрахункова точність алгоритму складає 10^{-4}.

3.3 Висновок до розділу

Розроблено алгоритм управління безпекою МП, що дозволяє забезпечити зміну програмно-апаратної конфігурації МП в залежності від умов (атрибутів) доступу, що включають, в тому числі, місце розташування МП, та критеріїв якості послуг. Характерними рисами даного алгоритму є: реалізація формальної моделі безпеки МП, яка передбачає врахування умов (атрибутів) доступу, включаючи місце розташування МП, вимоги мандатної рольової політики управління доступом; застосування методу Монте-Карло для підвищення достовірності виявлення місця розташування МП у спеціальному приміщенні на підставі обчисленого місцезнаходження методами трилатерації, k-найближчих сусідів та методу, заснованого на байєсівському підході; використання алгоритму оцінки інформаційної швидкості в каналі Wi-Fi, що враховує перешкоди, для вибору оптимальної, з точки зору вимог щодо якості послуг, програмно-апаратної конфігурації МП; формування оптимальної програмно-апаратної конфігурації МП з точки зору виконання вимог політики безпеки в ЗКС та якості послуг, що реалізується у формі багатокритеріальної оптимізації цілочисельного динамічного програмування.

4. СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ

4.1. Вимоги до системи управління безпекою мобільними пристроями у складі корпоративних мереж з різними рівнями захищеності

Розроблена система управління безпекою МП в корпоративних мережах з різними вимогами щодо захищеності передбачає наявність наступних компонентів:

– центр управління інформаційною безпекою (ЦУІБ);

– контролер доступу МП;

– довірена бездротова мережа передачі даних;

– підсистема виявлення місця розташування;

– довірені багатофункціональні МП, до складу яких входить агентний модуль, здатний приймати сигнали управління та керувати програмно-апаратною конфігурацією пристрою.

В рамках управління інформаційною безпекою можуть бути реалізовані механізми віддаленого моніторингу, засновані на використання особливостей реалізації мережевих протоколів. Зокрема спосіб віддаленого моніторингу та управління інформаційною безпекою мережевої взаємодії на основі використання системи доменних імен та програмне забезпечення, що дозволяє реалізувати цей спосіб. Для захисту ЗКС від комп'ютерних атак, а також запобігання перевантаженням у мережі та помилкам функціонування необхідно використовувати механізми міжмережевого екранування. Реалізація таких механізмів захисту описує спосіб аналізу інформаційного потоку та визначення стану захищеності мережі на основі адаптивного прогнозування та пристрій для його здійснення, а також варіанти побудови систем дистанційного керування та моніторингу перспективних міжмережевих екранів.

Для вирішення завдання безпечного доступу мобільного користувача до послуг мереж із різними вимогами щодо захищеності має забезпечуватися виконання таких умов:

– Існує бездротова мережа довірених точок доступу з відомим розташуванням точок доступу.

– Канал управління між довіреними точками доступу та МП захищений криптографічними засобами захисту інформації.

– МП має можливість функціонувати у різних програмно-апаратних конфігураціях.

– На МП функціонує апаратно-програмний модуль довіреного завантаження.

– На МП працює довірена операційна система (ДОС).

– У ДОС МП функціонує ізольоване програмне середовище.

– Користувач МП успішно автентифікований у системі управління доступом корпоративної мережі.

На рисунку 4.1 представлено загальну структуру основних компонентів ЗКС, що забезпечують функціонування розробленої системи.

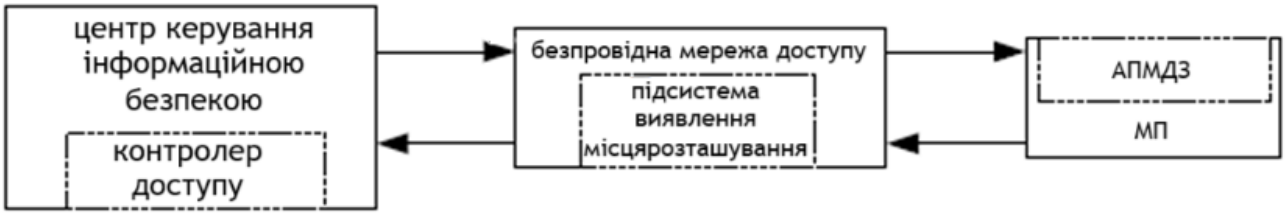

Рисунок 4.1 – Узагальнена структура основних компонентів ЗКС

Для забезпечення наявності керованої конфігурації, а також можливості незалежної обробки інформації в МП даний пристрій може включати до свого складу дубльовані компоненти, що відповідають за обробку даних. Дублювання компонентів має забезпечувати оптоелектронну чи іншу розв'язку трактів проходження сигналів з різними вимогами щодо захищеності (різними рівнями конфіденційності оброблюваної інформації). Приклад такого компонування у складі МП представлений на рисунку 4.2.

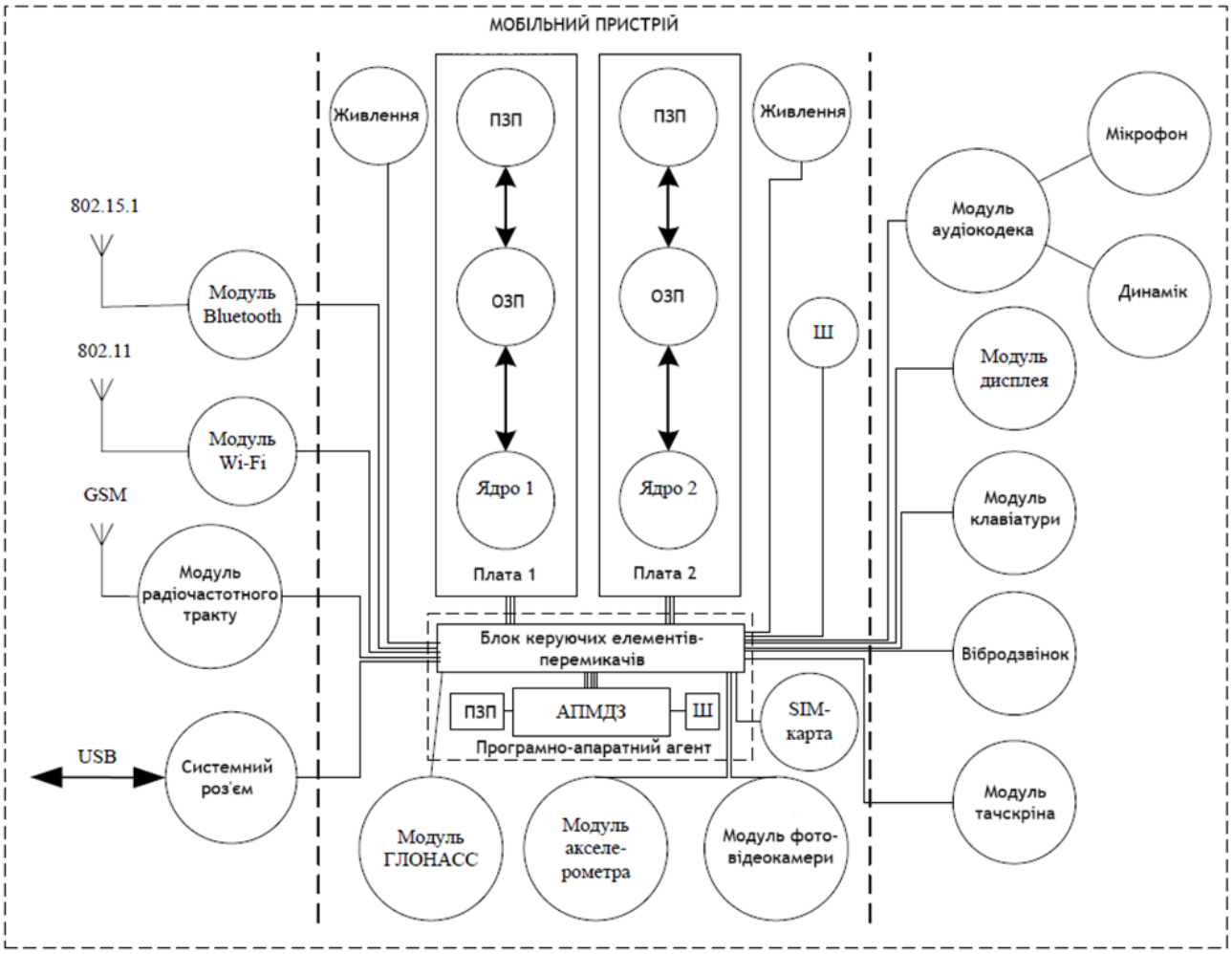

Рисунок 4.2 - Склад та структура мобільного пристрою з дублюванням функціональних блоків, які відповідають за обробку інформації в мережах з різними вимогами щодо захищеності

Керована програмно-апаратна конфігурація МП визначає його стан. Конфігурація МП в залежності від його розташування та інших атрибутів доступу визначає можливості користувача та МП щодо доступу до послуг корпоративних мереж з різними вимогами щодо захищеності та, відповідно, обмеження на використання тих чи інших послуг та функціональних можливостей МП. Таким чином, система управління безпекою МП дозволяє узгоджувати стан МП з вимогами політики безпеки корпоративних мереж з різними рівнями захищеності, а також вимогами щодо якості послуг, що надаються.

4.2. Пропозиції щодо реалізації захищеного каналу управління між контролером доступу та мобільним пристроєм

Відомо, що управління має мати властивості стійкості, безперервності, оперативності і прихованості. Для забезпечення даних властивостей канал управління повинен мати додаткові механізми захисту. Оскільки між контролером доступу та МП можливий канал управління лише через безпровідні мережі передачі даних, то можливі такі варіанти: VPN-з'єднання, наприклад, на базі протоколу HTTPS; захищені SMS-повідомлення; VPN-з'єднання у складі інкапсульованих даних протоколів низьких рівнів (канального, мережного, транспортного).

Варіант побудови захищеного каналу керування між контролером доступу МП з прикладу протоколу HTTPS представлений на рисунку 4.3.

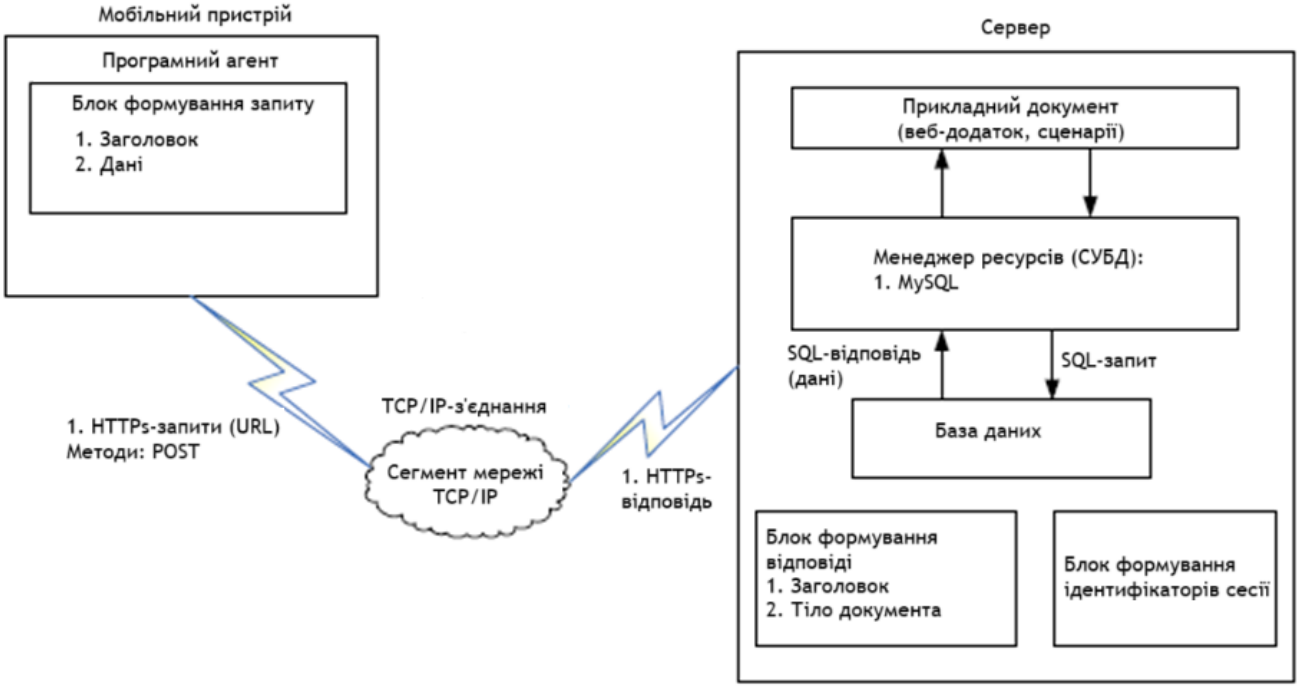

Рисунок 4.3 - Варіант побудови захищеного каналу керування на базі протоколу HTTPS

Розширена схема взаємодії МП та контролера доступу представлена на прикладі протоколу HTTPS. Доцільно канал управління між МП та віддаленим

сервером доступу реалізувати захищеним із встановленням VPN-каналу. У разі, якщо розголошення розташування користувача МП критично, можуть бути використані протоколи, що реалізують конфіденційні розподілені обчислення.

Слід зазначити, що реалізація захищеного каналу управління з урахуванням протоколу прикладного рівня HTTPS має істотні недоліки щодо стійкості, оперативності, прихованості, надійності і захисту від розвідування. Одним із варіантів вирішення цієї проблеми може бути використання можливостей протоколів низького рівня для реалізації такого захищеного каналу управління.

На рисунку 4.4. представлено варіант реалізації захищеного каналу управління у складі MAC-підрівня канального рівня стека протоколів.

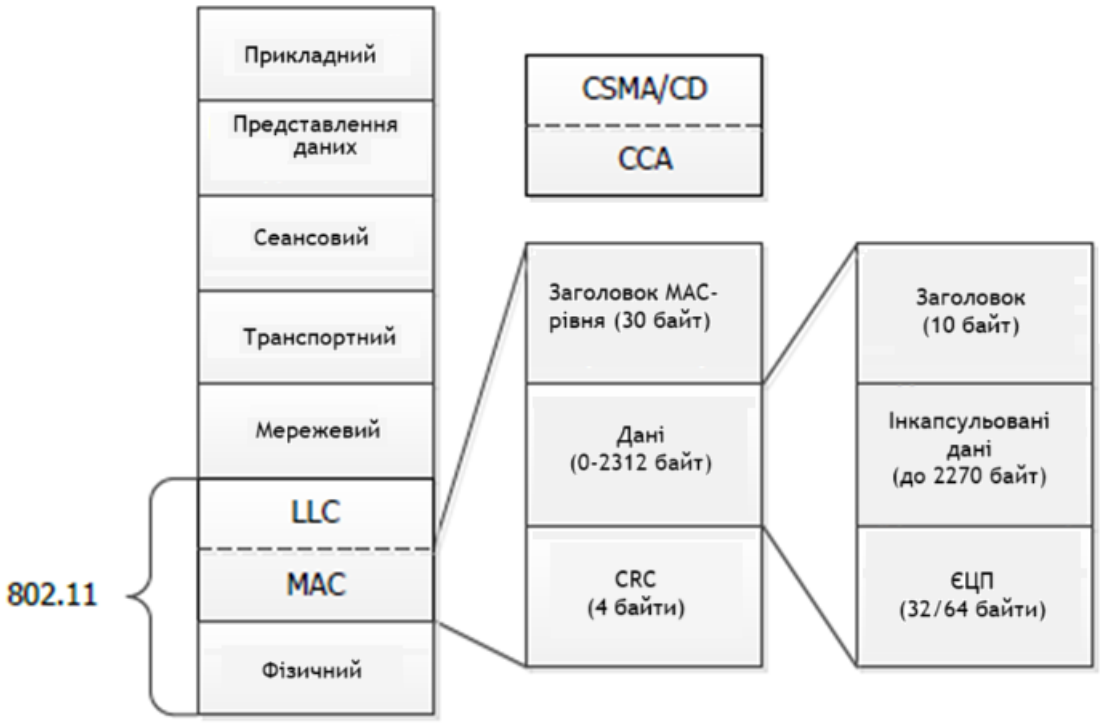

Рисунок 4.4 – Захищений канал управління МП у складі інкапсульованих даних MAC-підрівня канального рівня 802.11

За рахунок використання інкапсульованих даних у складі пакета можуть передаватися зашифровані сигнали керування. Варіант побудови структури даних у складі пакета інкапсульованих даних представлений на рисунку 4.5.

Обробка сигналів управління повинна бути покладена на програмно-

апаратний модуль у складі АПМДЗ МП або на елементи програмного коду драйверів інтерфейсів бездротової передачі даних.

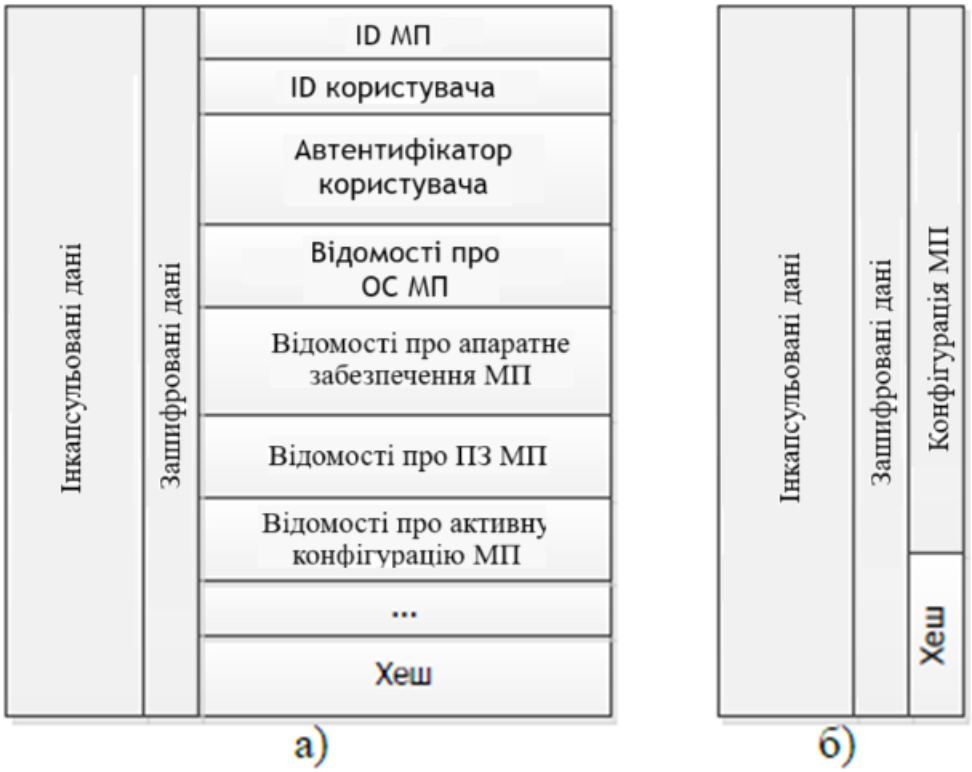

Рисунок 4.5 – Варіанти реалізації структури даних: а) під час передачі атрибутів доступу контролеру МП; б) під час передачі МП управляючого впливу як зміни

4.3 Рекомендації щодо розташування точок доступу бездротової мережі в системі виявлення місця розташування

Для методу трилатерації було досліджено вплив кількості точок доступу, що використовуються, та їх розташування на точність визначення місцезнаходження. Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to max, \\ var\ AP_j = (x_j, y_j), j = \overline{1, N_{AP}}, \\ var\ N_{AP} = 3..5, \end{cases} \tag{4.1}$$

де e_L – похибка виявлення місця розташування, що обчислюється у відповідності до виразу (2.3), у якому $(\widetilde{x_{tr}}, \widetilde{y_{tr}})$ – обчислені методом трилатерації координати розташування MG, а $(\tilde{x}, \tilde{y})$ – реальні координати розташування МП; N_{AP} точок доступу із заданими координатами $(x_j, y_j), j = \overline{1, N_{AP}}$.

Для трьох точок доступу найкраща точність визначення місцезнаходження досягається при розташуванні точок доступу так, як показано на рисунку 4.6.

Рисунок 4.6 – Схема оптимального розташування трьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування

Для чотирьох точок доступу найкраща точність визначення місцезнаходження досягається при взаємному розташуванні точок доступу так, як показано на рисунку 4.7.

Рисунок 4.7 – Схема оптимального розташування чотирьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування

Для п’яти точок доступу найкраща точність визначення місцезнаходження досягається при взаємному розташуванні точок доступу так, як показано на

рисунку 4.8.

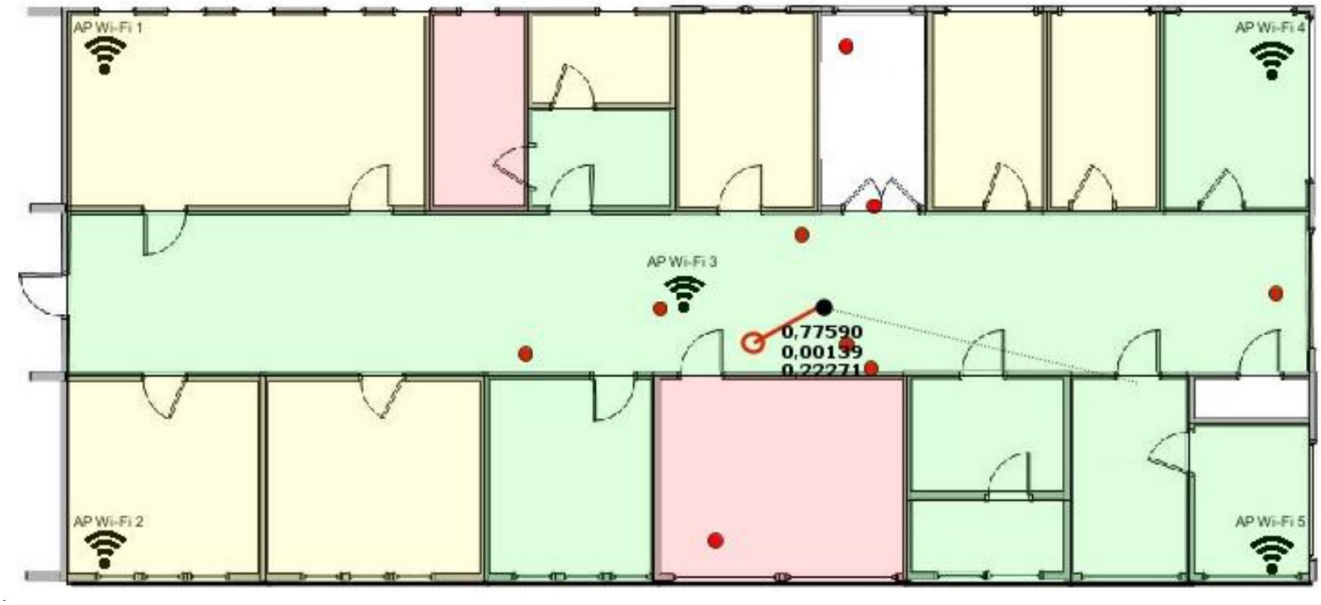

Рисунок 4.8 – Схема оптимального розташування п’яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування

4.4 Оцінка ефективності системи управління безпекою мобільних пристроїв у корпоративних мережах

4.4.1. Розрахунок часу необхідного для зміни конфігурації мобільного пристрою

У процесі руху користувача з МП неминуче виникають ситуації, коли змінюються атрибути доступу і в тому числі рівень захищеності приміщень, де знаходиться мобільний користувач. Атрибути доступу та політика безпеки визначають вимоги до конфігурації МП за поточних умов доступу. Для мобільних користувачів час зміни конфігурації МП у деяких ситуаціях є важливим показником якості.

Процес зміни конфігурації МП здійснюється у кілька етапів:

– Вимірювання рівня сигналу МП на точках доступу бездротової мережі передачі даних (T_{RSS}).

– Визначення розташування МП (T_{LOC}).

– Надсилання атрибутів доступу (запиту на доступ до послуг) з МП (T_{REQ}).

– Обробка запиту з урахуванням параметрів політики безпеки (T_{POLICY}).

– Формування та відправка керуючої команди на зміну конфігурації МП (T_{RESP}).

– Прийом та обробка керуючої команди на стороні МП, застосування нової конфігурації (T_{CONF}).

Таким чином, оцінка загального часу, необхідного для зміни конфігурації МП, може бути подана у вигляді

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \quad (4.2)$$

Розрахунок часу, необхідного на кожному етапі, буде виконано для найпоширенішого стандарту бездротової передачі – IEEE 802.11 при наступних обмеженнях та припущеннях:

– доступ до бездротової мережі передачі даних встановлений, МП пройшов аутентифікацію та знаходиться в зоні дії довіреної бездротової мережі передачі даних;

– розрахунок часових параметрів виконується на найгірший випадок.

Відповідно до стандарту IEEE 802.11 передача пакета даних на канальному рівні, що володіє ідентифікаційною інформацією про передавача здійснюється у 4 етапи. Дані етапи представлені рисунку 4.9.

У стандарті IEEE 802.11 використовується метод колективного доступу з виявленням несучої та уникнення колізій (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA). Перед початком передачі здійснюється вибір вільного каналу з урахуванням алгоритму оцінки чистоти каналу (Channel Clearance Algorithm, CCA). В основі даного алгоритму лежить вимірювання енергії сигналу на антені та потужності прийнятого сигналу (Received Signal Strength Indicator,

RSSI). Якщо потужність прийнятого сигналу нижче заданого порога, то канал оголошується вільним і MAC-рівень отримує статус CTS (Clear To Send).

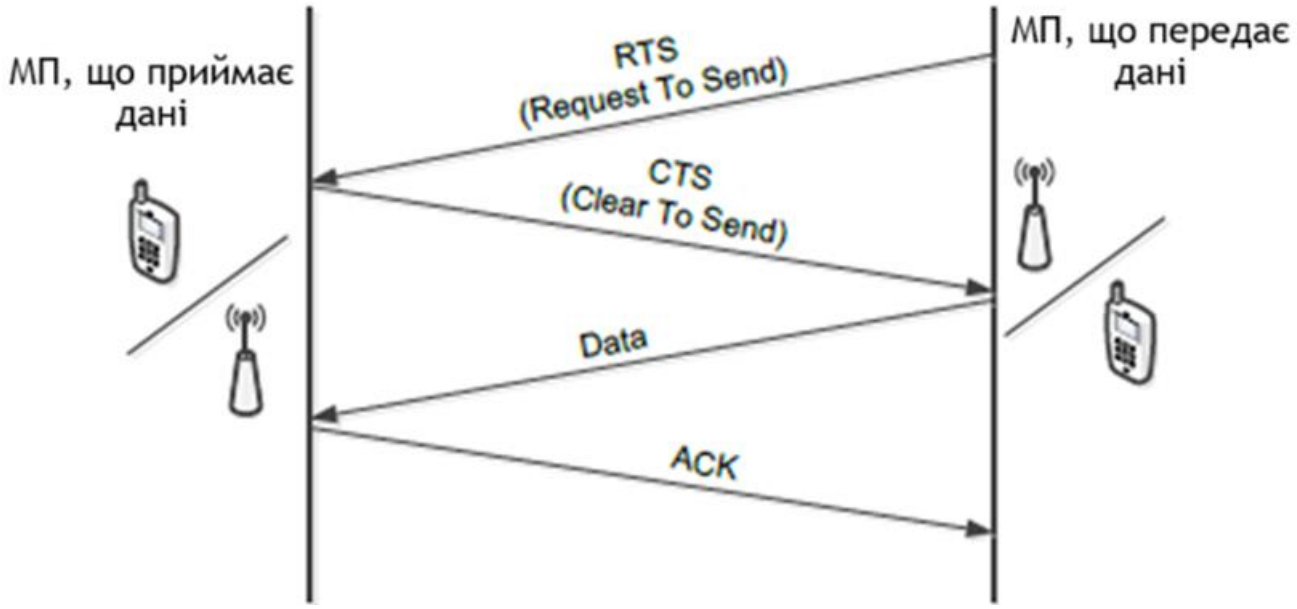

Рисунок 4.9 – Чотирьох етапний протокол передачі даних, що реалізує метод колективного доступу до середовища з мінімізацією ймовірності виникнення зіткнень

Перед початком передачі даних, МП відправляє повідомлення RTS (Ready To Send), що містить інформацію про готовність відправлення даних, адресата і тривалість передачі. Якщо приймальна станція (точка доступу) відповідає посилкою сигналу CTS, МП починає передачу даних. Після завершення передачі даних точка доступу повертає кадр ACK, що підтверджує безпомилковий прийом.

Максимальна дальність дії бездротової мережі визначається безліччю параметрів і насамперед потужністю передавача, чутливістю приймача та наявністю перешкод. Розрахунок часу передачі сигналу від передавача до джерела в умовах будівлі зробимо для дальності в l=100 м. Тоді чотирьох етапна передача даних здійснюватиметься за час, що дорівнює

$$t_{data} \approx \frac{4 * l}{c} = \frac{4 * 100}{299792458} = 1{,}334256 * 10^{-6} c. \quad (4.3)$$

Відповідно, передача пакета даних з ідентифікуючою МП інформацією буде здійснюватися за час $T_{RSS}=t_{data}$.

З тих самих міркувань, здійснюється розрахунок значень T_{REQ} і T_{RESP}. При цьому необхідно врахувати, що максимальний розмір блоку даних передбачений специфікацією пакетування даних передбачає блок даних до 2048 байт, рекомендуючи при цьому використовувати пакети довжиною 1500 і 2048 байт. Оскільки в запиті на доступ містяться відомості про атрибути доступу та запитуваної послуги, а у відповіді на запит – інформація про конфігурацію, що призначається, то розмір переданих даних може перевищувати максимальний розмір пакета, тому для значень T_{REQ} і T_{RESP} передбачимо 10-кратне перевищення максимального розміру пакет. Тоді з урахуванням (4.5) буде:

$$T_{REQ} \approx T_{RESQ} \approx 10 * t_{data} = 1.334256 * 10^{-5} c. \quad (4.4)$$

Значення T_{LOC} визначається часом, необхідним для отримання даних про рівень сигналу МП точками доступу, в зоні дії яких знаходиться даний пристрій, а також часом роботи алгоритму виявлення місця розташування МП і рівня захищеності приміщення, в якому воно знаходиться.

Значення T_{LOC}, T_{POLICY}, T_{CONF} визначаються швидкодією програмно-апаратної складової системи управління МАУ.

У процесі імітаційного моделювання та функціонування розроблених програм для ПК було отримано наступні результати:

Виходячи з отриманих оцінок часу виконання процедур та виразу (4.4) отримаємо оцінку значення часу, необхідного для зміни конфігурації МП:

$$\begin{aligned} T_{RECONF} &= T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \\ &\approx 0{,}001334256 * 10^{-3} + 2{,}92 * 10^{-3} + 0{,}01334256 * 10^{-3} \\ &+ 0{,}71 * 10^{-3} + 0{,}01334256 * 10^{-3} + 1{,}12 * 10^{-3} \\ &\approx 4{,}778019376 * 10^{-3} \approx 4{,}778 \text{ мс} \end{aligned} \quad (4.5)$$

Отримана оцінка часу, необхідного для зміни конфігурації МП в 4,778 мс дозволяє зробити висновок, що при даних обмеженнях і припущеннях час переконфігурації МП не перевищує заданий поріг і знижує рівень захищеності під час руху МП.

Дані розрахунки не враховують частоту опитування довірених точок доступу, що знаходяться в радіусі зони дії МП, і відповідно не враховують частоту отримання оцінок рівня потужності сигналу МП. Значення вимірювань рівня сигналу МП є критичними, оскільки є вихідними даними для підсистеми виявлення місця розташування МП. Тому при розробці програмного забезпечення та драйверів для точок доступу та бездротового адаптера МП необхідно враховувати дані міркування та використовувати частоту опитування доступних МП порівняно з отриманою оцінкою часу конфігурації.

Для оцінювання залежності часу переконфіграції МП від кількості випробувань у методі Монте-Карло було проведено експеримент. З аналізу даних експерименту видно, що з поточних умов при числі випробувань у чисельному методі Монте-Карло M<5000 час переконфігурації МП знаходиться в межах допустимих значень. Також з аналізу графіка видно, що залежність має експоненційне зростання складності. Даний факт пред'являє підвищені вимоги до продуктивності обладнання системи керування доступом та умови її експлуатації.

На підставі отриманих значень може бути отримана оцінка ймовірності збереження конфіденційності інформації при доступі до послуг мереж з різними вимогами щодо захищеності згідно з прийнятою системою показників ефективності. Імовірність збереження конфіденційності інформації запропоновано оцінювати за допомогою виразу:

$$P_{\text{СК}}(T_{RECONF}) = \\ = P\left[(T_{RECONF} \le T_{RECONF}^{\text{доп}})/(CONF \subset CONF^{\text{доп}})\right] * \left(1 - P_{\text{ПрЗ}}\right) \quad (4.6)$$

Показник $P_{Пр3}$ може бути розраховано як:

$$P_{\text{ПрЗ}} = 1 - \prod_{m=1}^{k} P_{\text{НСД}_m}, \tag{4.7}$$

де k – кількість перешкод, яку потрібно подолати порушнику для того щоб отримати доступ до інформаційних та програмних ресурсів; $P_{\text{НСД}_m}$ – ймовірність подолання порушником m-тої перешкоди (засобу захисту).

При цьому прийнято, що ймовірність подолання системи захисту $P_{ПЗ} \rightarrow 0$. Таким чином, за умови $\text{CONF} \subset \text{CONF}^{\text{доп}}$, прийнятих обмежень і допущень ($P_{ПЗ} \rightarrow 0$), а також отриманої оцінки часу переконфігурації $T_{RECONF}=4.778*10^{-3}$ с, що знаходиться в межах заданих замовником значень $T_{RECONF}^{\text{доп}} = 10^{-2}$с, можна зробити висновок про те, що $P_{\text{СК}}(T_{\text{RECONF}}) \rightarrow 1$.

4.4.2 Розрахунок своєчасності доступу до послуг та інформації з використанням мобільних пристроїв

Ймовірність надання інформації чи послуг $P_{\text{ДІ}}(T_{\text{ДІ}})$ за заданий час $T_{\text{ДІ}}^{\text{зад}}$ буде визначатися за допомогою табульованої неповної гамма-функції:

$$P_{\text{ДІ}}^{\text{У}}(T_{\text{ДІ}}) = \int_0^{\theta} \exp(-\tau) * \frac{\tau^{\gamma} d\tau}{\Gamma(\gamma)}, \tag{4.8}$$

де $\Gamma(\gamma) = \int_0^{\theta} \exp(-\tau) * \tau^{\gamma} d\tau$ – гамма-функція; $\gamma = \frac{T_{\text{заг}}}{\sqrt{T_2 - T_{\text{заг}}}}$; $\theta = T_{\text{ДІ}}^{\text{зад}} * \frac{\gamma^2}{T_{\text{заг}}}$; $T_{заг}$ і T_2 - розраховані відповідно до середнього часу та 2-го моменту реакції системи при обробці запитів системи (повного часу перебування в обробці з урахуванням очікування в черзі), $T_{\text{ДІ}}^{\text{заг}}$ - заданий час (гранично допустимий) для обробки запиту на доступ до інформації (послуг).

Відповідно до виразу (4.4) розраховане часом, потрібне для переконфігурації МП становить $T_{RECONF} = 4{,}78 * 10^{-3}$с. Відповідне йому значення ймовірності своєчасності обробки запиту, отримане за допомогою табульованої неповної гамма-функції рівне

$$\mathrm{Р}_{\text{ДІ}}^{\text{У}}(\mathrm{Т}_{\text{ДІ}}) = \Gamma(\gamma) = \Gamma\left(\frac{T_{RECONF}}{\sqrt{D[T_{RECONF}] + T_{RECONF}^2}}\right) = \Gamma(1{,}034) = 0{,}9983 \qquad (4.9)$$

Таким чином, за однакових умов отримання доступу до послуг для системи, що розробляється, і її прототипу в умовах, МП в системі, що розробляється, необхідно здійснити реконфігурацію, додатково витративши на цей час, що дорівнює $T_{RECONF} = 4{,}78 * 10^{-3}$ с.

4.5 Висновки до розділу

В параграфі 4.1 описано компоненти системи управління безпекою МП з різними вимогами щодо захищеності. Визначено механізми моніторингу та управління інформаційною безпекою мережевої взаємодії на основі використання системи доменних імен та відповідного програмного забезпечення. У параграфі представлено структуру МП задля забезпечення наявності керованої конфігурації та можливості незалежної обробки інформації.

У параграфі 4.2 надано пропозиції щодо реалізації захищеного каналу управління між контролером доступу та МП, зокрема представлено варіант побудови захищеного каналу керування між контролером доступу МП з прикладу протоколу HTTPS. Також представлено варіант побудови структури даних у складі пакета інкапсульованих даних, оскільки так можуть передаватися зашифровані сигнали керування.

В параграфі 4.3 продемонстровано рекомендації щодо розташування точок доступу бездротової мережі в системі виявлення місця розташування МП задля найкращої точності визначення локації МП.

В параграфі 4.4 проведено розрахунок часу, необхідного для зміни конфігурації МП, та своєчасності доступу до послуг та інформації з використанням МП.

ВИСНОВКИ

Мета кваліфікаційної роботи магістра – розробка методу керування безпекою мобільних пристроїв в корпоративних мережах. Для досягнення поставленої мети було виконано наступне: розроблено формальну моделі безпеки МП, виконано моделювання місця розташування МП, розроблено модель системи виявлення місця розташування МП, розроблено алгоритм визначення ймовірності місцезнаходження МП у спеціальному приміщенні, виконано оцінку властивостей алгоритму керування безпекою МП, надано пропозиції щодо системи управління безпекою МП у складі корпоративних мереж з різними рівнями захищеності, надано пропозиції щодо реалізації захищеного каналу управління між контролером доступу та МП, надано рекомендації щодо оптимального взаємного розташування точок доступу бездротової мережі в системі виявлення місця розташування.

У другому розділі викладено опис елементів моделі безпеки МП. Ця модель відрізняється від вже існуючих моделей тим, що враховує місцезнаходження МП в корпоративних мережах з різними типами захисту. Описано типову структуру МП та використання різних функціональних блоків при різних методах передачі даних, зокрема при обміні голосовою інформацією та обміні повідомленнями. Представлено опис атрибутів доступу, пов'язаних з користувачем МП, станом його програмно-апаратного середовища, адресною інформацією та іншими параметрами, які впливають на блокування заборонених режимів роботи. Зазначено основні принципи визначення місцезнаходження об'єкта. Виконано порівняння технологій визначення місцезнаходження, на підставі чого зроблено висновок, що для цього можна використовувати технології GSM, CDMA, 3G, RFID, Bluetooth, Wi-Fi. Обгрунтовано використання технології Wi-Fi, яка дозволяє одночасно вимірювати рівень сигналу мобільного пристрою точками доступу та забезпечувати захищену інформаційну взаємодію між мобільним пристроєм і зонами контрольованої сегрегації, тим самим зменшуючи витрати при проектуванні і обслуговуванні в порівнянні з системами визначення місцезнаходження на основі датчиків та інших технологій. Модель системи

визначення місця розташування МП, яка дозволяє оцінити ймовірність його місцезнаходження у спеціальному приміщенні з підвищеними вимогами до захисту, розглянуто у параграфі 2.4.

У третьому розділі розроблено алгоритм управління безпекою мобільного пристрою, який дозволяє динамічно змінювати програмно-апаратну конфігурацію пристрою відповідно до атрибутів доступу. Цей алгоритм вирізняється такими особливостями, як впровадження формальної моделі безпеки мобільного пристрою, яка враховує атрибути доступу, включаючи місце розташування пристрою, вимоги мандатної рольової політики управління доступом; використання методу Монте-Карло для підвищення достовірності визначення місця розташування пристрою в спеціальному приміщенні; формування оптимальної програмно-апаратної конфігурації мобільного пристрою з урахуванням виконання вимог політики безпеки в зоні контрольованої сегрегації та якості послуг. Це досягається за допомогою багатокритеріальної оптимізації цілочисельного динамічного програмування.

У розділі 4 описано складові системи управління безпекою МП з різними вимогами до захисту. Визначені механізми моніторингу та управління інформаційною безпекою мережевої взаємодії, базуючись на використанні системи доменних імен та відповідного програмного забезпечення. Представлено структуру МП для забезпечення наявності керованої конфігурації та можливості незалежної обробки інформації. Запропоновано варіанти реалізації захищеного каналу управління між контролером доступу та мобільним пристроєм, зокрема, розглянуто побудову захищеного каналу керування за допомогою протоколу HTTPS. Також представлено варіант побудови структури даних у складі пакета інкапсульованих даних для передачі зашифрованих сигналів керування. Наведено рекомендації щодо розташування точок доступу бездротової мережі в системі виявлення місця розташування МП для досягнення найкращої точності визначення його місцезнаходження. Проведено розрахунок часу, необхідного для зміни конфігурації МП, та своєчасності доступу до послуг і інформації за допомогою МП.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Weichbroth Paweł, Łysik Łukasz. Mobile Security: Threats and Best Practices. *Mobile Information Systems.* 2020. DOI: 10.1155/2020/8828078.

2. Corporate Network Example. URL: https://creately.com/diagram/example/ifibp55o1/corporate-network-example-classic (дата звернення 08.09.2023).

3. Enterprise Network Diagram. URL: https://www.smartdraw.com/network-diagram/examples/enterprise-network/ (дата звернення 09.09.2023).

4. Luis Castro Silva, Samyr Vale. A Methodology for Network Security Infrastructure according to the New Brazilian General Law for Personal Data Protection. *International Journal of Computer Applications*. 2021. Vol 183. DOI: 10.5120/ijca2021921520

5. Метод паралельного моніторингу параметрів корпоративних мереж. URL: https://cutt.ly/4wPQU91P (дата звернення 12.09.2023).

6. The Top 10 MDM Solutions for Business. URL: https://www.stanfieldit.com/mdm-solution/ (дата звернення 14.09.2023).

7. H. Ahn, S. Choi, M. Mueck and V. Ivanov. Data Plane Framework for Software-Defined Radio Access Network Based on ETSI-Standard Mobile Device Architecture. I*EEE Access*. 2019. Vol. 7. PP. 163421-163436. DOI: 10.1109/ACCESS.2019.2952619.

8. The ultimate guide to mobile device security in the workplace. URL: https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace (дата звернення 15.09.2023).

9. IEEE 802.11. The Working Group Setting the Standards for WIRELESS LOCAL AREA NETWORKS. URL: https://www.ieee802.org/11/ (дата звернення 20.09.2023).

10. Ali Balapour, Hamid Reza Nikkhah, Rajiv Sabherwal. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management.* 2020. Vol. 52. DOI:

https://doi.org/10.1016/j.ijinfomgt.2019.102063

11. France Belanger, Robert E. Crossle. Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*. 2018. Vol 28, No 1. PP. 34-49. DOI: https://doi.org/10.1016/j.jsis.2018.11.002

12. System on a Chip: How Smaller, Faster Devices are Made. URL: https://www.ansys.com/blog/what-is-system-on-a-chip (дата звернення 24.09.2023).

13. Advantages System on a Chip Technology. URL:https://www.waferworld.com/post/system-on-a-chip-technology-and-the-advantages-of-using-it (дата звернення 24.09.2023).

14. С. Я. Кавин. До питання поняття «інформаційної безпеки» в національному та міжнародному праві. *Juris Europensis Scientia*. 2022. Vol 4. PP. 95-101. DOI: https://doi.org/10.32782/chern.v4.2022.19

15. Бондар Г. Л. Інформаційна політика та інформаційна безпека. *Публічне управління та митне адміністрування*. 2019. Вип. 4. С. 42 – 49

16. Жилін А. В., Шаповал О. М., Успенський О. А.. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

17. Гребенюк А.М., Рибальченко Л.В.. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

18. Information Security Policy and Practices. URL: https://wingify.com/information-security-policy/ (дата звернення 02.10.2023).

19. T Security Policy. URL: https://www.hud.ac.uk/media/policydocuments/IT-Security-Policy.pdf (дата звернення 02.10.2023).

20. Лаптєв О. А., Степаненко В. І., Тихонов Ю. О.. Формальні математичні моделі для забезпечення безпеки інформації. *Сучасний захист інформації*. 2019, Вип. 1. DOI: 10.31673/2409-7292.2019.015963

21. Потенко О.С., Корченко А.О.. Порівняльний аналіз моделей безпеки в інформаційних системах. *Збірник тез наукових доповідей. Стан та удосконалення*

безпеки інформаційно-телекомунікаційних систем (SITS' 2021). Миколаїв – Коблево, 2021. - с.31-34.

22. Толюпа С., Пархоменко І., Штаненко С.. Модель системи протидії вторгненням в інформаційних системах. *Інфокомунікаційні технології та електронна інженерія*. Вип 1, 2021. - с. 39-50.

23. Системи контролю і управління доступом від А до Я. URL: https://deps.ua/ua/knowegable-base/reference-information/7824.html (дата звернення 04.10.2023).

24. Christos K. Verginis, Dimos V. Dimarogonas. Control of cooperative manipulator-endowed systems under high-level tasks and uncertain dynamics. *Annual Reviews in Control*. 2022. Vol. 54. PP. 219-240. DOI: https://doi.org/10.1016/j.arcontrol.2022.09.004.

25. Kashmar, N., Adda, M., Atieh, M.. From Access Control Models to Access Control Metamodels: A Survey. Advances in Information and Communication. *FICC 2019. Lecture Notes in Networks and Systems*. 2020. Vol. 70. DOI: https://doi.org/10.1007/978-3-030-12385-7_61

26. Allae Erraissi, Abdessamad Belangour. A Big Data Security Layer Meta-Model Proposition. *Advances in Science, Technology and Engineering Systems Journal*. 2019. Vol. 4, No. 5. PP. 409-418. DOI: 10.25046/aj040553

27. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ 1999.

28. Master Access Control Models for Enhanced Cybersecurity. URL: https://resources.infosecinstitute.com/certifications/cissp/access-control-models-and-methods/ (дата звернення 07.10.2023).

29. Владімірова В. Б. Принципи побудови політики безпеки інформації. Зб. тез доп. 80-ї наук. конф. викл. акад.. Одеса, 2020 р. – С. 245–247.

30. Класифікація інтегральних схем. URL: http://ni.biz.ua/13/13_13/13_131869_klassifikatsiya-integralnih-shem.html (дата звернення 13.10.2023).

31. X. Bao, X. Zhang, J. Lin, D. Chu, Q. Wang and F. L. Towards the Trust-Enhancements of Single Sign-On Services. *2019 IEEE Conference on Dependable and Secure Computing (DSC)*. 2019. PP. 1-8. DOI: 10.1109/DSC47296.2019.8937676.

32. Mohaiminul Islam, Shangzhu Jin. An Overview Research on Wireless Communication Network. *Advances in Wireless Communications and Networks*. 2019. Vol. 5, No. 1. PP. 19-28. DOI: 10.11648/j.awcn.20190501.13

33. B. C. Mallikarjun, K. J. Kiranmayi, N. Lavanya, K. H. Prateeksha and J. Sushmitha. Intruder Detection System - A LoRa Based Approach. *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. 2020. PP. 255-258. DOI: 10.1109/ICCES48766.2020.9137923.

34. Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu. User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*. 2020. Vol 170. DOI: https://doi.org/10.1016/j.comnet.2020.107118

35. A. Ly, Y.-D. Yao. A Review of Deep Learning in 5G Research: Channel Coding, Massive MIMO, Multiple Access, Resource Allocation, and Network Security. *IEEE Open Journal of the Communications Society*. 2021. Vol. 2. PP. 396-408. DOI: 10.1109/OJCOMS.2021.3058353.

36. Thomas C. G., Jayanthila Devi. A Study and Overview of the Mobile App Development Industry. *International Journal of Applied Engineering and Management Letters (IJAEML)*. 2020. Vol. 5, No 1. PP. 115–130.

37. D. Cerdeira, N. Santos, P. Fonseca, S. Pinto. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems. *2020 IEEE Symposium on Security and Privacy (SP)*. 2020. PP. 1416-1432. DOI: 10.1109/SP40000.2020.00061.

38. Identifying emerging cyber security threats and challenges for 2030. URL: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 (дата звернення 17.10.2023).

39. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої

встановлена законом та не становить державної таємниці. Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ 2021.

40. Cristiá, M., Rossi, G. Automated Proof of Bell–LaPadula Security Properties. *J Autom Reasoning*. 2021. Vol. 65. PP. 463–478. DOI: https://doi.org/10.1007/s10817-020-09577-6

41. X. TIAN, H. SONG. A zero trust method based on BLP and BIBA model. *2021 14th International Symposium on Computational Intelligence and Design (ISCID)*. 2021. PP. 96-100. DOI: 10.1109/ISCID52796.2021.00031.

42. J. Yao, V. Zimmer. Security Model. In: Building Secure Firmware. *Apress*. 2020. DOI: https://doi.org/10.1007/978-1-4842-6106-4_12

43. Z. Yuan, F. Liu, W. Yuan, Q. Guo, Z. Wang and J. Yuan. Iterative Detection for Orthogonal Time Frequency Space Modulation With Unitary Approximate Message Passing. *IEEE Transactions on Wireless Communications*. 2022. Vol. 21, No 2. PP. 714-725. DOI: 10.1109/TWC.2021.3097173.

44. GPS.gov. Technical Documentation. URL: https://www.gps.gov/technical/ (дата звернення 23.10.2023).

45. RFID Tag Specifications. URL: https://www.wristbands.com/pages/rfid-tag-specs (дата звернення 25.10.2023).

46. Specifications. Wi-Fi Alliance. URL: https://www.wi-fi.org/discover-wi-fi/specifications (дата звернення 25.10.2023).

47. Rosli Nurmi, Sophian Ali, Ashraf Arselan. Localisation of Inspection Probes in A Storage Tank. *Journal of Integrated and Advanced Engineering (JIAE).* 2021. Vol 1. DOI: 10.51662/jiae.v1i2.21

48. K-Nearest Neighbor (KNN) Algorithm. URL: https://www.geeksforgeeks.org/k-nearest-neighbours/ (дата звернення 28.10.2023).

49. Britannica, The Editors of Encyclopaedia. "Bayesian analysis". URL: https://www.britannica.com/science/Bayesian-analysis (дата звернення 29.10.2023).

50. Stephanie Glen. Monte Carlo Simulation/Method. URL: https://www.statisticshowto.com/monte-carlo-simulation/ (дата звернення 02.11.2023).

ДОДАТОК Б Перелік наукових праць

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

УДК 004.4

Тези доповідей

**VII Міжнародної науково-практичної конференції
до 30-ти річчя кафедри кібербезпеки та програмного забезпечення**

"Інформаційна безпека та комп'ютерні технології"

1 листопада 2023 року

Кропивницький 2023

УДК 004.4

Матеріали VII Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 004.056

М.М.Федух[1], Ю.П.Кльоц[1], Н.С.Петляк[1]
mfedukh@khmnu.edu.ua, klots@khmnu.edu.ua, npetlyak@khmnu.edu.ua
[1]Хмельницький національний університет, м. Хмельницький

ПІДХОДИ ДО КЕРУВАННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ В ЗАХИЩЕНИХ ПРИМІЩЕННЯХ

Використання сучасних мобільних пристроїв для обробки конфіденційної інформації обмежено через ряд суттєвих особливостей їх функціонування, таких як розміри, мобільність користувачів і багатофункціональність.

Ці характеристики визначають великий спектр потенційних загроз інформаційній безпеці, які відрізняються від тих, які існують при використанні стаціонарних обчислювальних засобів. Постійна зміна місцезнаходження користувачів мобільних пристроїв (МП), бездротовий дистанційний доступ до мереж з різними вимогами до захищеності, обмежені обчислювальні можливості з одного боку та високошвидкісні комунікаційні можливості з іншого створюють велику кількість загроз інформаційній безпеці, зокрема загрози порушення конфіденційності інформації.

Необхідно розробити універсальну систему захисту інформації, що забезпечуватиме конфіденційність при використанні МП. Основною метою цієї системи буде забезпечення безпеки інформації, коли користувачі отримують доступ до різних мереж з різними вимогами до захищеності за допомогою МП. Це досягатиметься за допомогою адаптивного управління безпекою МП через зміну його програмно-апаратної конфігурації, що дозволить адаптувати стан МП до параметрів доступу, вимог щодо безпеки корпоративної мережі та вимог до якості послуг, які надаються.

До основних принципів, які лежать в основі всіх методів визначення розташування, включаються:

– тріангуляція та трилатерація - методи оцінювання місцезнаходження на основі геометричних характеристик кутів, що вказують на об'єкт (тріангуляція), або відстаней від трьох або більше об'єктів з відомим місцезнаходженням (трилатерація);

– аналіз карти вимірів - метод базується на оцінці розташування, виходячи з карти точок вимірювань параметрів сигналу, що називається "картою сигнального простору";

– аналіз близькості здійснює визначення місця розташування на підставі того, наскільки близько об'єкт знаходиться до приймача сигналу в порівнянні з іншими об'єктами;

– аналіз динаміки руху: цей метод залежить від вивчення і врахування динаміки руху об'єкта, що допомагає визначити його розташування на основі змін в часі.

Ці принципи визначення розташування використовуються для різноманітних завдань і додатків, де точність і надійність визначення місцезнаходження є критичними факторами.

На рисунку 1 представлено порівняльний огляд технологій визначення розташування з урахуванням їх точності та застосування.

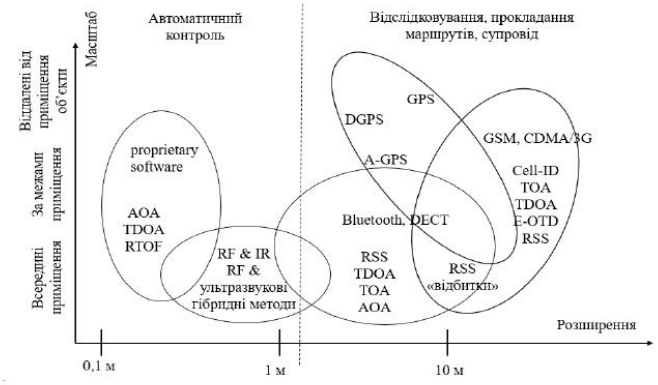

Рис. 1. Порівняння технологій визначення розташування

Технології супутникової навігації не можна використовувати всередині приміщень через значне пригнічення сигналу від супутників. Методи, що базуються на сигналах GSM/CDMA/3G/LTE, мають обмежену точність для вирішення завдань визначення місця розташування мобільних пристроїв (МП). Ультразвукові методи, радіочастотна ідентифікація (RFID), технології на основі волоконно-оптичних ліній зв'язку не дозволяють створити захищений канал управління для МП і, крім того, деякі з них не надають можливість ідентифікувати МП.

Для системи визначення розташування мобільних пристроїв встановлюються ряд вимог, виконання яких впливає на збереження конфіденційності інформації:

– точність визначення місця розташування повинна бути настільки високою, щоб можна було ідентифікувати конкретне приміщення, в якому перебуває користувач мобільного пристрою, і при цьому з мінімальною похибкою 2-го роду;

– ідентифікація користувача мобільного пристрою в системі визначення розташування повинна забезпечити можливість однозначно встановити особу, яка використовує мобільний пристрій, в контексті системи визначення розташування.

Завдання визначення місцезнаходження та завдання захищеної інформаційної взаємодії можуть бути вирішені за допомогою одного бездротового модуля стандарту 802.11, або можуть бути розділені на технологічно незалежні бездротові модулі. Для сигналів стандарту 802.11, розв'язання задачі визначення розташування може бути досягнуто за допомогою методів тріангуляції (трилатерації) та аналізу карти сигнального простору. Слід зауважити, що метод трилатерації не потребує попередніх вимірювань рівня сигналів мережі, що різко спрощує розробку, експлуатацію та підтримку системи. Проте, в той же час підсистеми розташування, побудовані на основі методу трилатерації, мають помітно меншу точність порівняно з системами, що використовують аналіз карти сигнального простору.

Як основні технології, які використовують бездротові мережі передачі даних для визначення місця розташування та для обґрунтування алгоритмічної складності запропонованого підходу до розрахунку ймовірності знаходження мобільного пристрою (МП) у спеціальному приміщенні, незалежно від обраного методу, запропоновано використовувати наступні технології:

– метод трилатерації сигналу МП: цей метод передбачає використання кількох точок доступу бездротових мереж для визначення місця розташування МП;

– метод k-найближчих сусідів: цей метод базується на аналізі найближчих сусідів для визначення місця розташування МП;

– метод, що використовує байєсівський підхід: цей метод використовує байєсівську ймовірність для визначення місця розташування МП;

– розв'язання задачі обчислення площі приміщень кожного рівня захищеності: це вимагає врахування наступних умов: конфігурація та розташування приміщень відомі заздалегідь; координати місця розташування МП та розташування кола, в межах якого може знаходитися МП, обчислюються відомими методами; конфігурація та розташування приміщень усередині даного кола мають геометричну форму довільної природи; максимальний радіус кола, в межах якого може знаходитися МП, залежить від використовуваної технології розташування і визначається максимальною помилкою розташування для даної технології, яку отримано емпірично.

У вищезазначених умовах застосування традиційного геометричного підходу для розрахунку площі фігур не є прийнятним. Це пояснюється, передусім, необхідністю визначення площі фігур довільної конфігурації в будь-який момент часу та урахуванням великої кількості можливих варіантів. Найбільш відповідним методом для визначення площі довільних фігур є статистичний метод, відомий як метод Монте-Карло. Цей метод дозволяє визначити площу довільної фігури, яка знаходиться всередині кола, що визначає ймовірне місцезнаходження мобільного пристрою, хоча може вимагати попереднього навчання. Попереднє навчання означає процес збору статистики помилок визначення місця розташування для конкретної технології. Ця статистика представляє собою розподіл значень помилок розташування і становить основу для проведення статистичних експериментів. Важливою частиною цього процесу є врахування помилки розташування як випадкової величини.

Застосування методу Монте-Карло для розрахунку ймовірності знаходження мобільного пристрою (МП) в спеціальному приміщенні у поєднанні з технологіями визначення розташування на базі бездротових мереж передачі даних дозволяє зменшити вплив нестійкості радіосигналів у бездротових мережах на похибку визначення місця розташування МП і підвищити надійність розрахунків ймовірності в спеціальному приміщенні в межах захищеної корпоративної мережі.

Тому обґрунтовано алгоритмічну реалізованість запропонованого підходу до обчислення ймовірності розташування мобільного пристрою (МП) в спеціальному приміщенні. Досліджено, що для підвищення точності визначення розташування МП цілком доцільно використовувати емпіричні дані щодо статистики помилок вимірювання місця розташування. При цьому межове значення критерію прийняття рішення про рівень захищеності приміщення, в якому знаходиться МП, повинно визначатися на основі вимог замовника і припустимих значень помилки другого роду. Для апробації моделі системи розташування було проведено імітаційне моделювання. Проведена комплексна оцінка якості цієї моделі, яка включала перевірку її адекватності, чутливості та стійкості. Також були отримані оцінки параметрів приватних моделей, що впливають на точність визначення розташування МП.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Федуха Миколи Миколайовича
ПІБ здобувача вищої освіти
студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

5.12.2023
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 4%**

	Документ		Сумарний збіг по Базі Даних	
ID: 121899 Назва: Метод керування безпекою мобільних пристроїв в корпоративних мережах Додано в БД: 2023-12-06 Автора: Федух М.М. Керівники: Кльоц Ю.П. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	87143	585	438 (1%)	6 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015975343

Дата перевірки:
06.12.2023 10:42:18 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 10:42:52 EET

ID користувача:
100008300

Назва документа: **Федух_плагіат**

Кількість сторінок: 72 **Кількість слів:** 12396 **Кількість символів:** 99706 **Розмір файлу:** 3.42 MB **ID файлу:** 1015654796

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.23%
Схожість

Найбільша схожість: 0.55% з джерелом з Бібліотеки (ID файлу: 1015654798)

1.87% Джерела з Інтернету	159	Сторінка 74
0.69% Джерела з Бібліотеки	47	Сторінка 75

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	96
Підозріле форматування	13 сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод керування безпекою мобільних пристроїв в корпоративних мережах

Автор: Федух Микола Миколайович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Кльоц Юрій Павлович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 2,23%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 0%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені системою Unichek модифікації стосуються математичних формул і не є порушенням академічної доброчесності.

Керівник роботи _____ Ю.П. Кльоц

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Федух Микола Миколайович

Тема Метод керування безпекою мобільних пристроїв в корпоративних мережах

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 75

1. Короткий зміст роботи та прийнятих В рамках роботи проведено дослідження проблем захисту інформації при використанні мобільних пристроїв у приміщеннях із різними рівнями захисту та розроблено метод керування безпекою мобільних пристроїв. В роботі поставлено та вирішено наступні задачі: розробити формальну модель безпеки мобільного пристрою, виконати моделювання місця розташування мобільного пристрою, розробити модель системи виявлення місця розташування пристрою, розробити алгоритм визначення ймовірності місця розташування мобільного пристрою у спеціальному приміщенні, розробити систему управління мобільними пристроями у складі корпоративних мереж з різними рівнями захищеності, надати рекомендації щодо оптимального розташування точок доступу бездротової мережі в системі виявлення місця розташування.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми дослідження та сформульовано мету та основні завдання дослідження. У першому розділі було досліджено особливості використання мобільних пристроїв у корпоративних мережах із різними рівнями захисту, наявні моделі систем керування доступом, моделі загроз та порушників. У другому розділі описано модель визначення місця знаходження пристрою у приміщенні в основі якої використано модель Бела-ЛаПадули, розроблено модель безпеки мобільного пристрою та визначено технологію передачі даних за допомогою якої буде здійснюватися визначення місця розташування. У третьому розділі розроблено алгоритм та метод визначення приналежності пристрою до того чи іншого рівня захисту у поточний момент часу. У четвертому розділі представлено розроблену систему управління безпекою мобільних пристроїв, описано вимоги до блоків пристроїв, що відповідають за обробку та передачу даних.

4. Позитивні сторони роботи полягають можливості модифікації налаштувань мобільних пристроїв у залежності від місця перебування пристрою (в залежності від рівня захисту приміщення) задля забезпечення безпеки інформації.

5. Негативні сторони роботи У роботі недостатньо описано метод. Проте модель, алгоритм та реалізована система, які передують розробці методу чи відображають подальше впровадження, описані в повній мірі.

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор Мартинюк Валерій Володимирович.

« 8 » грудня 2023 року _____ (підпис)