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

# Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ МОБІЛЬНОГО АБОНЕНТСЬКОГО ТЕРМІНАЛУ В КОРПОРАТИВНИХ МЕРЕЖАХ ДОСТУПУ
08-34.МКР.009.00.000 ПЗ

Виконав: студент 2-го курсу,
групи АРЗ-18м
спеціальності 172 – Телекомунікації та радіотехніка

_____ Стець Д.С.

Керівник: к.т.н., доцент каф. ТКСТБ

_____ Стальченко О.В.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф. БМІ

_____ Коваль Л.Г.

«____» _____ 2019 р.



Вінниця ВНТУ - 2019 рік

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

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

"___" _____2019 року

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

Стецю Дмитру Сергійовичу.
(прізвище, ім'я, по батькові)

1. Тема роботи Підвищення інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу
керівник роботи Стальченко Олександр Володимирович, канд. техн. наук, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "02" 10 2019 року № 254
2. Строк подання студентом роботи 02 грудня 2019 року
3. Вихідні дані до роботи 1. Кількість точок доступу для методу трилатерації – 5; 2. Кількість найближих «сусідів» для методу k-ближніх сусідів –9; 3. Крок сітки карти сигнального простору - h=1,5x1,5; 4. Кількість вимірювань в кожній точці сигнального простору з відомими координатами – 30; 5. Тривалість пере конфігурації мобільного абонентського пристрою - $4{,}778019376 \cdot 10^{-3}$ с; 6. Значення ймовірності своєчасного оброблення запиту на обслуговування – 0,9983.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Аналіз стану наукових досліджень та технічних рішень в області захисту інформації під час використання мобільних абонентських пристроїв; 2. Система управління безпекою мобільних абонентських пристрої, що забезпечують підвищення імовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг і інформації корпоративних мереж з різними вимогами по захищеності під час використання єдиного МАП.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1. Типова структура корпоративних мереж з МАП; 2. Структура і топологія системи управління безпекою МАП в корпоративній мережі; 3. Схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки; 4. Схема витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні; 5. Схема доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП; 6. Схема доступу до інформації з використанням різних конфігурацій МАП; 7. Багатоагентна система позиціонування МАП; 8. Схема підсистеми управління конфігурацією МАП; 9. Склад і структура мобільного абонентського пристрою з дублюванням функціональних блоків, що відповідають за обробку інформації в мережах з різними вимогами по захищеності; 10. Будова захищеного каналу управління на базі

протоколу HTTPS; 11. Структурна схема, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв.

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Спеціальна частина | Стальченко О.В., доцент кафедри ТКСТБ | | |
| Економічна частина | Лесько О.Й., к.е.н., професор | | |
| Охорона праці та безпека в надзвичайних ситуаціях | Березюк О.В. к.т.н., доцент | | |

7. Дата видачі завдання 02 вересня 2019 року

**КАЛЕНДАРНИЙ ПЛАН**

| № з/п | Назва етапів магістерської кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Розробка технічного завдання | 06.09.2019р. | |
| 2. | Техніко-економічне обґрунтування розробки | 13.09.2019р. | |
| 3. | Аналіз стану наукових досліджень та технічних рішень в області захисту інформації під час використання мобільних абонентських пристроїв | 04.10.2019р. | |
| 4. | Система управління безпекою мобільних абонентських пристроїв | 25.10.2019р. | |
| 5. | Підвищення імовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг і інформації корпоративних мереж з різними вимогами по захищеності під час використання єдиного МАП | 08.11.2019р. | |
| 6. | Аналіз економічної ефективності розробки | 15.11.2019р. | |
| 7. | Охорона праці та безпека в надзвичайних ситуаціях | 22.11.2019р. | |
| 8. | Оформлення пояснювальної записки та графічної частини | 29.11.2019р. | |
| 9. | Нормоконтроль МКР | 02.12.2019р. | |
| 10. | Попередній захист МКР, рецензування МКР | 06.12. 2019р. | |
| 11. | Захист МКР ЕК | 09.12. 2019р. | |

Студент _____ Стець Д.С.
( підпис )

Керівник роботи _____ Стальченко О.В.
( підпис )

# РЕФЕРАТ

УДК 621.391

Стець Дмитро Сергійович. Підвищення інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу. Магістерська кваліфікаційна робота зі спеціальності «Телекомунікації та радіотехніка» – Вінниця: ВНТУ, 2019. – 116 с. Українською мовою.

Рисунків 44, таблиць 12, бібліографія 65.

Здійснено аналіз сучасних технічних рішень для захисту інформації в МАП. Досліджено модель безпеки мобільного абонентського пристрою в корпоративних мережах з різними вимогами по захищеності. Показано, що основним параметром, який є невизначеним фактором для визначення умов надання доступу до МАП, є його місце розташування.

Представлено опис алгоритму управління безпекою МАП, що дозволяє визначити оптимальну програмно-апаратну конфігурацію пристрою з урахуванням атрибутів доступу і вимог по захищеності і якості послуг.

Наведено науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП у корпоративних мережах, що забезпечує підвищення ймовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП.

# ABSTRACT

UDC 621.391

Dmytro Stets. Improvement of information security of the mobile subscriber terminal in corporate access networks. Master's qualification work in the specialty "Telecommunications and Radio Engineering" - Vinnitsa: VNTU, 2019. - 116 p. In Ukrainian language.

Figures 44, Tables 12, Bibliography 65.

The analysis of modern technical solutions for the protection of information in the MAD. The model of security of mobile subscriber device in corporate networks with different security requirements is investigated. It is shown that the main parameter that is an undetermined factor in determining the conditions for granting access to the MAD is its location.

The description of the MAD security management algorithm is presented, which allows to determine the optimal hardware and software configuration of the device taking into account the access attributes and requirements for security and quality of services.

The scientific and technical proposals on the practical implementation of the MAD security management system in corporate networks are provided, which increases the likelihood of ensuring information security when accessing information communications services and information of corporate networks with different security requirements when using a single MAD.

ЗМІСТ

# ВСТУП

*Актуальність теми.* Розвиток сучасних багатофункціональних мобільних абонентських пристроїв (МАП) та інформаційних технологій, пропускну здатність каналів зв'язку, в тому числі бездротових, призводять до постійного зростання потреби в доступі до інформації [1], причому незалежно від того, де знаходиться користувач. В цьому відношенні не є винятком і корпоративні мережі, в тому числі, захищені (ЗКМ), що надають доступ до інфокомунікаційних послуг і ресурсів з різними вимогами по захищеності. До таких мереж відносяться, в тому числі, інформаційні системи загального користування, інформаційні системи, які обробляють персональні дані, а також геоінформаційні системи [2].

Віддалений доступ з використанням МАП до корпоративних мереж з різними вимогами по захищеності передбачає застосування відповідним 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 (користувачами) ЗКМ єдиного мобільного пристрою для здійснення такого доступу. Різниця за вимогами захищеності в ЗКМ, як правило, здійснює розподіл такої мережу на контури обробки інформації, які, в свою чергу, зазвичай обмежені спеціалізованими приміщеннями з відомим розташуванням на об'єктах організації.

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

Зазначені особливості визначають зовсім інший спектр загроз інформаційної безпеки при роботі з МАП в порівнянні зі стаціонарними засобами обчислювальної техніки (ЗОТ). Постійна зміна місця розташування користувачів МАП, бездротовий віддалений доступ до мереж з різними вимогами по захищеності, обмежені обчислювальні можливості з одного боку і високошвидкісні комунікаційні з іншого створюють велику кількість загроз інформаційній безпеці, пов'язаних в першу чергу з погрозами порушення конфіденційності інформації [3].

З іншого боку перспективним напрямком удосконалення сучасних корпоративних мереж є забезпечення надання захищеного доступу абонентам до інформації та послуг з різними вимогами по захисту при використанні єдиного МАП [4]. При цьому до наданих послуг у

відповідність ставляться:

- телефонний і відео зв'язок з додатковими видами обслуговування;
- захищений електронний поштовий обмін з елементами обліку вхідних і вихідних документів;
- відеоконференційний зв'язок;
- доступ до баз і банків даних, мережевим додаткам інформаційних ресурсів.

Необхідність надання зазначеного переліку послуг з використанням одного універсального абонентського пристрою користувачам, враховуючи, що послуги можуть надаватися мережами з різними вимогами по захищеності, дозволяє говорити про те, що існує об'єктивна потреба в розробці універсального МАП і системи захисту інформації (СЗІ), що дозволяє забезпечити конфіденційність інформації [4] при своєчасному [18] наданні доступу до зазначеного переліку послуг з використанням одного МАП. Задачею СЗІ буде забезпечення безпеки інформації при доступі до послуг мереж з різними вимогами по захищеності з використанням МАП, шляхом управління безпекою МАП за допомогою адаптивного зміни його програмно-апаратної конфігурації, що дозволяє погоджувати стан МАП з умовами (атрибутами) доступу, вимогам безпеки корпоративної мережі, а також вимогами щодо якості послуг, що надаються.

*Аналіз останніх досліджень.* Огляд технічних і програмно-апаратних рішень, а також нормативно-правової бази в галузі захисту інформації при роботі з МАП показав, що в даний час:

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

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

В даному напрямку досліджень суттєві результати в галузі вивчення моделей безпеки управління доступом в вітчизняних та зарубіжних наукових працях отримані під керівництвом Девянин П.Н., Зегжди Д.П., Гайдамакин Н.А., Бочкова М. В., Герасименко В. А ., Бородакій Ю.В., Макліна Дж., Самарате П., сандхі Р. Дослідження проблем захисту інформації, в тому числі і проблем аналізу захищеності інформації проводилися під керівництвом Ломако А.Г., Молдовяна А.А., Стародубцева Ю. І., кайдани І. Н., Остапенко А.Г., Шелупанова А.А., Котенко І. В. В області питань мобільного радіозв'язку і радіодоступу, засобів широкосмугового доступу, безпеки бездротових мереж доступу відомі роботи Челишева В. Д., Кловського Д. Д., Коржика В. І., Вишневського В. М., Шахновича І.В., Баскакова С.І., Зюко А. Г. та інших. В області захисту інформації при експлуатації МАП відомі роботи Гузаірова М. В., Машкін І. В., Бабікова А. Ю., Десницкого В. А. і Карпеева Д. О. [5-10]. Однак питання управління безпекою МАП для забезпечення доступу до послуг корпоративних мереж з різними вимогами по захищеності розглянуті недостатньо повно.

На основі аналізу тенденцій і перспектив розвитку сучасних корпоративних мереж виявлено протиріччя між вимогами, що пред'являються до безпеки інформації [5] при доступі до захищеної служби і інформації з використанням універсальних МАП, і технічними можливостями СЗІ, що дозволяють забезпечити безпеку інформації при здійсненні такого доступу в корпоративних мережах з різними вимогами по захищеності.

На підставі цього висунута гіпотеза дослідження, яка полягає в тому, що для підвищення ймовірності забезпечення безпеки інформації при експлуатації МАП і забезпеченні безпечного доступу до послуг корпоративних мереж з різними вимогами по захищеності необхідно розробити модель безпеки МАП і алгоритм, що дозволяє управляти безпекою (програмно-апаратною конфігурацією) МАП, погоджуючи його з вимогами по ІБ і якості послуг, що надаються, в залежності від умов надання доступу до послуг та ресурсам, в яких знаходиться МАП, а також науково-технічні пропозиції по реалізації системи управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності.

Перераховані фактори обумовлюють актуальність теми дослідження МКР: "Управління безпекою мобільних абонентських пристроїв в корпоративних мережах".

*Мета та постановка задачі*. Метою даної кваліфікаційної роботи є підвищення ймовірності забезпечення безпеки інформації при доступі до

інфокомунікаційних послуг та інформації корпоративних мережах з різними вимогами по захищеності при використанні єдиного МАП.

Задачами магістерської кваліфікаційної роботи є:

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

Приватні наукові завдання дослідження:

- провести аналіз існуючих наукових досліджень і технічних рішень щодо захисту інформації в МАП, а також способів побудови систем захисту інформації при доступі до мереж з різними вимогами по захищеності з використанням єдиного пристрою; розробити систему показників якості, що дозволяє оцінити ефективність процесу захисту інформації при експлуатації системи управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності;

- розробити формальну модель безпеки МАП, що відрізняється від відомих урахуванням місцезнаходження МАП в спеціальних приміщеннях, до яких пред'являються підвищені вимоги по ІБ, обгрунтувати її коректність;

- розробити алгоритм управління безпекою МАП, що враховує атрибути доступу користувачів МАП, що включають в себе, в тому числі, ймовірність знаходження МАП в спеціальному приміщенні, а також вимоги щодо якості послуг, що надаються; розробити моделюючий алгоритм і здійснити імітаційне моделювання функціонування системи управління безпекою МАП для отримання оцінки ефективності запропонованих технічних рішень;

- сформувати науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, а також рекомендації щодо вибору параметрів алгоритмів визначення місця розташування МАП в приміщеннях корпоративної мережі і алгоритму обчислення ймовірності знаходження МАП в спеціальному приміщенні.

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

*Предмет дослідження:* моделі та алгоритми управління безпекою МАП.

*Методи досліджень* базуються на використанні теорії машинного навчання, теорії ймовірності та математичної статистики, апарату прихованих марківських моделей, теорії алгоритмів, теорії управління, теорії множин, теорії оптимізації, чисельних методів і методів математичного та імітаційного моделювання.

*Наукова новизна одержаних результатів полягає:*

- в розробці і обґрунтуванні коректності нової формальної моделі безпеки МАП, що відрізняється від відомих урахуванням оцінки його місцезнаходження в спеціальному приміщенні, інших атрибутів доступу, а також реалізацією вимог мандатної і рольової політик безпеки в корпоративних мережах з різними вимогами щодо єдиного МАП;

- в розробці нового алгоритму управління безпекою МАП, що відрізняється від відомих визначенням оптимальної, з точки зору забезпечення конфіденційності інформації та якості послуг, що користувачеві послуги, програмно-апаратну конфігурацію МАП, з урахуванням ймовірності його наявності в спеціальних приміщеннях та інших атрибутах доступу;

– у розробці системи управління безпекою мобільних абонентських пристроїв, яка здатна віддалено керувати програмними та апаратними конфігураціями МАП, в залежності від умов доступу, безпеки та політики якості служби для забезпечення безпечного доступу до інформації та інформації з мереж з різними вимогами безпеки.

*Практичне значення МКР полягає*:

– розробити науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, що підвищує ймовірність скомпрометований інформації при приєднані інформації послуги та ресурси в мережах з різними вимогами безпеки при використанні єдиного МАП;

– в розробці рекомендацій щодо формування оптимальних параметрів

системи визначення місця розташування МАП, що дозволяють підвищити достовірність обчислення його місцезнаходження в спеціальних приміщеннях.

Теоретичне значення проведене в МКР, полягає в розробці офіційного приладу для моделювання безпеки МАП в корпоративних мережах з урахуванням його розташування в спеціальних приміщеннях, а також розробці алгоритму для програмної та апаратної оптимізації конфігурації (безпеки) МАП, що дозволяє підвищити ймовірність забезпечення безпеки інформації в доступі до інформації та інформації про корпоративні мережі з

різними вимогами до безпеки при використанні єдиної карти з урахуванням вимог до ІБ та якості послуг, що надаються в корпоративній мережі.

*Практична значимість роботи полягає*:

1) у дослідженні ефективності відомих методів і систем для визначення розташування МАП, коли вони використовуються всередині будівлі в налаштуваннях і обгрунтовуючи оптимальні параметри алгоритмів для визначення місцезнаходження МАП, що дозволяє збільшити надійність визначення місцезнаходження МАП в спеціальних приміщеннях;

2) впровадити запропоновані алгоритми у вигляді набору програм для ЕОМ і для перевірки працездатності їх використання в корпоративній мережі;

3) у розробці науково-технічних пропозицій з практичної реалізації системи управління безпекою МАП, підвищення ймовірності підвищення безпеки інформації в доступі до інформації та інформації з корпоративних мереж різні вимоги до безпеки при використанні єдиного МАП.

*Апробація роботи* та її основні результати роботи проводилися на Всеукраїнській науково-практичній інтернет-конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2020) у 2019 році.

# 1 АНАЛІЗ СТАНУ НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНІЧНИХ РІШЕНЬ В ОБЛАСТІ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ

В даному розділі проведено аналіз умов функціонування і вимог, що пред'являються до МАП в корпоративних мережах, недоліків існуючих засобів захисту інформації та проблем, пов'язаних із забезпеченням безпеки інформації при роботі з МАП. Дана характеристика існуючим формальним моделям безпеки комп'ютерних систем і систем контролю доступу, побудованим на їх основі. Виділено недоліки існуючих формальних моделей при використанні їх в відношенні сучасних МАП. Досліджено критичні з точки зору забезпечення безпеки інформації особливості сучасних МАП. На основі аналізу нормативно-правових документів виділений перелік актуальних чинників, що впливають на безпеку інформації при експлуатації МАП, а також запропоновані моделі загроз і порушника, що відображають склад загроз безпеки інформації та можливості порушників безпеки при використанні МАП в корпоративних мережах з різними вимогами по захищеності . Проведено аналіз існуючих захищених МАП, програмних і програмно-апаратних мобільних технічних рішень, а так-же технічних рішень, що дозволяють здійснювати доступ до мереж з різними вимогами по захищеності з використанням одного абонентського пристрою. Описано особливості експлуатації МАП в захищених корпоративних мережах. Обґрунтовано необхідність врахування місця розташування МАП в корпоративної мережі для забезпечення ефективної роботи СЗІ. Проведено аналіз способів і технічних рішень з визначення місця розташування МАП в приміщеннях всередині будівлі, представлена їх класифікація, виділені їхні переваги і недоліки. Обґрунтовано використання БМПД для вирішення завдання обчислення ймовірності знаходження МАП в спеціальних приміщеннях. Сформульовано наукове завдання дослідження.

## 1.1 Умови функціонування та вимоги, що пред'являються до мобільних абонентських пристроїв

В даний час використання сучасних МАП в захищених корпоративної мережах суттєво обмежено у зв'язку з відсутністю ефективних СЗІ, які гарантують забезпечення безпеки інформації. Разом з тим перспективні напрямком удосконалення сучасних корпоративних мереж є забезпечення захищеного доступу абонентам до інформації та послуг з різними вимогами

по захищеності при використанні єдиного МАП [10].

Сучасні корпоративні мережі, в яких передбачено використання є МАП, є аналогами структури, представленої на рис. 1.1.

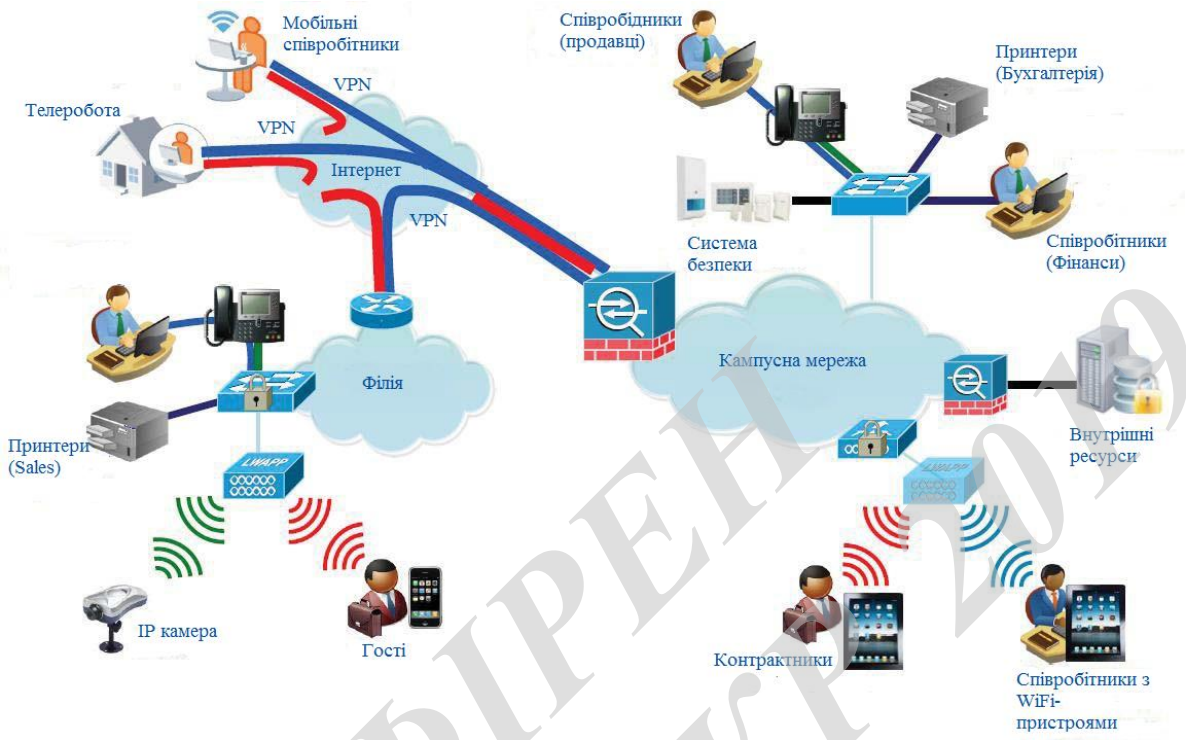



Рисунок 1.1 - Типова структура корпоративних мереж з МАП

При наявності в організації інформації, що вимагає більш високого рівня захисту, всередині неї створюються кілька корпоративних мереж з різними потребам по захищеності. Як правило, для отримання доступу до ресурсів корпоративних мереж з різними вимогами по захищеності використовуються різні МАП з необхідними рівнями захищеності, що створюється виділені незручності. Для вирішення даної проблеми і забезпечення безпеки інформації при роботі на єдиному МАП в даний час використовується два підходи:

– монтаж спеціалізованих СЗІ (MDM- рішення) [3] особистим співробітникам МАП організації в рамках концепції BYOD (Bring Your Own Device);

– експлуатація корпоративних захищених МАП [12].

Однак ці рішення не володіють достатньою ефективністю з точки зору захисту інформації з різних причин [3]:

– відсутні обґрунтовані формальні моделі безпеки комп'ютерних систем, в яких передбачена експлуатація МАП і враховується мобільність користувачів;

– системи визначення місця розташування МАП в приміщеннях на

території організації, як правило, будуються на основі БМПД стандарту 802.11 [14] і мають низьку точністю з помилкою визначення місця розташування близько 2 метрів, що створюється загрозу некоректного застосування встановленої в корпоративного мережі політики безпеки МАП;

– існуючі MDM-рішення [11] і корпоративні захищені ні МАП [2] не передбачають апаратної переконфігурації МАП, що є причиною наявності технічних каналів витоку інформації всередині пристрою за межі контрольованої зони;

– більшість сучасних МАП побудовані на базі імпортної електроніки, яка не є довіреною [13], а існуючі методики сертифікації СЗІ не дозволяють гарантувати відсутність програмних і апаратних закладок.

Незважаючи на наявність сучасних СЗІ, спрямованих на забезпечення безпеки інформації при роботі з МАП, принциповою проблемою є питання довіри до апаратних платформ МАП, які реалізуються, як правило, на базі імпортної електроніки і технології SoC (System-on-Chip) . Згідно дослідженням компанії "Алладін Р. Д." [13] в більшості сучасним них МАП використовується архітектура ARM процесорів, в яких впроваджена технології "TrustZone", розроблена англійською компанією ARM. Зроблено це для апаратної ізоляції (віртуалізації) двох паралельних процесів – довіреного (безпечного) в рамках роботи, так званої ОС "Secure OS" і звичайного (де працюють програми під управлінням звичних операційних систем - Android, iOS, Linux, Tizen, Sailfish ) - "RichOS" (гостьова ОС) [13]. Довірені процеси в "TrustZone" володіють повним контролем над звичайною ОС, включаючи поліцейські функції і функції розвідки. За допомогою програми "TrustZone" управляються довіреною операційною системою "Secure OS", яка впроваджується в мікросхему на етапі її виробництва. При цьому звичайна ОС "RichOS", наприклад, Android не має функціональних можливостей щодо визначення наявності ОС "Secure OS". Дане дослідження [13] також показало, що в понад 95% сучасних процесорах з ARM-архітектурою впроваджено технологію "TrustZone", включно із захищеними смартфони типу "Коперник С1", Samsung Z3, YotaPhone, YotaPhone 2, а також сертифіковані ОС "Android 6.0 Marshmallow ", ядро Astra Linux Special Edition 1.4 (реліз" Новоросійськ "для ARM), ядро Linux 4.5.

Аналіз нормативно-правової бази та вимог щодо забезпечення ІБ при використанні в захищених корпоративних мережах [10] показав, що:

– існують особливі вимоги системи ІБ щодо експлуатації МАП в захищених корпоративних мережах;

– використання особистих МАП в ЗКМ заборонено або істотно обмежено в рамках принципу BYOD з урахуванням виконання вимог системи ІБ;

– абонентські пристрої (мобільні телефони, смартфони, планшетні комп'ютери і т.п.) стандарту IEEE 802.11 повинні відповідати вимогами корпоративного політиці ІБ в ЗКМ;

– обладнання мережі Wi-Fi також має відповідати вимогами корпоративної політики ІБ в ЗКМ.

Очевидно, що доступність захищених інформаційно-комунікаційних послуг зв'язку при використанні особистих МАП в ЗКМ істотно обмежена. Відкриті послуги, що надаються з використанням особистих МАП, можуть бути і зовсім недоступні. Разом з тим сучасні МАП дозволяють отримувати доступ до широкому переліку послуг. Порівняльний аналіз кількості поданих різними МАП [2] послуг представлений на рис. 1.2.

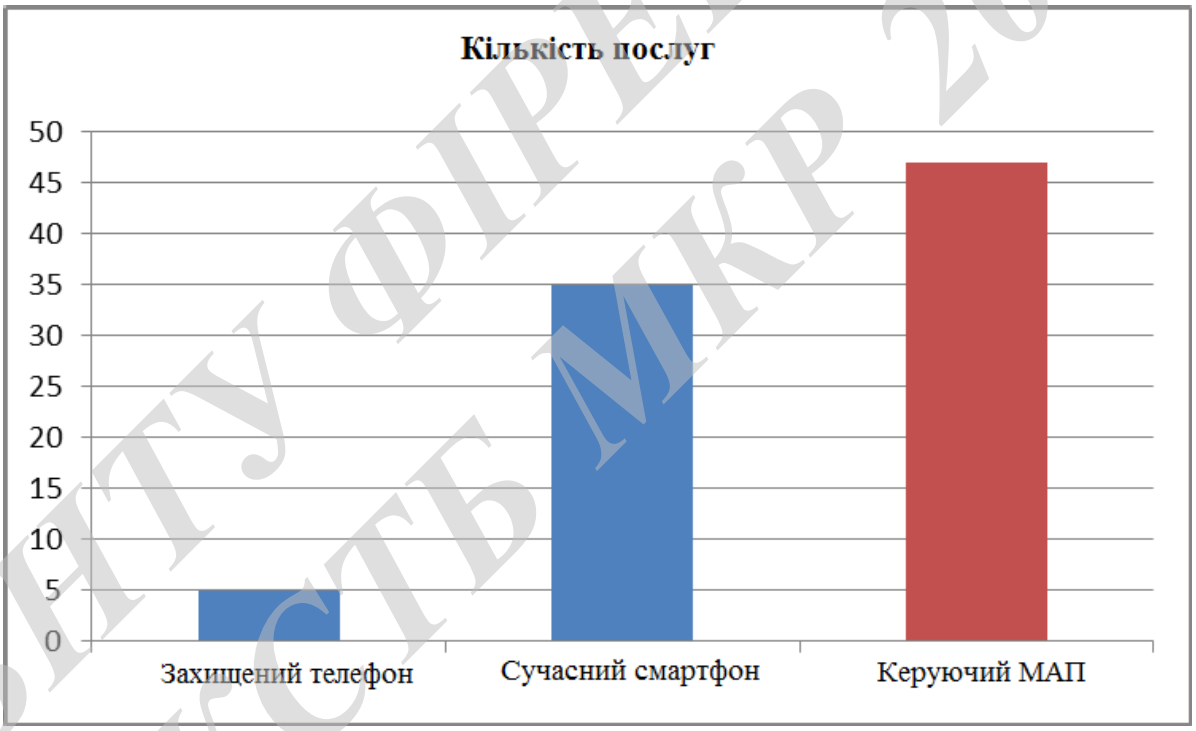



Рисунок 1.2 – Порівняльний аналіз кількості послуг, що надаються МАП

У зв'язку з відсутністю ефективних СЗІ, що дозволяють забезпечити безпеку інформації, експлуатація МАП для доступу до переліку послуг, що включають у себе, як захищені, так і незахищені, в ЗКМ істотно обмежена. Підвищити ймовірність забезпечення безпеки інформації при доступі до послуг і ресурсів ЗКС пропонується за рахунок використання керованого МАП, що взаємодіє з системою управління безпекою МАП, що дозволяє управляти програмно-апаратною конфігурацією МАП в залежності від умов його експлуатації. Структура і топологія системи управління безпекою

МАП в корпоративній мережі в цьому випадку може виглядати так, як показано на рис. 1.3[13].


Рисунок 1.3 - Структура і топологія системи управління безпекою МАП в корпоративній мережі

Основним недоліком подібної архітектури системи управління безпекою МАП є відсутність формальної моделі безпеки МАП, яка враховує при цьому місце розташування МАП в корпоративній мережі, докази її коректності, а також недостатньо ефективні існуючі технології з визначення місця розташування МАП в приміщеннях всередині будівлі. Зазначені фактори свідчать про актуальність даної проблеми та необхідність вирішення поставленого наукового завдання.

## 1.2 Моделі безпеки комп'ютерних систем, що включають в свій склад мобільні абонентські пристрої

Для формального опису процесу забезпечення безпеки інформації в комп'ютерних системах і обґрунтування її захищеності використовують формальні моделі безпеки, на основі яких будуються різні механізми захисту інформації, включаючи систему контролю доступу. Основним завданням системи контролю доступу є запобігання будь-якої діяльності, яка може призвести до порушення безпеки комп'ютерної системи [6]. Це завдання може вирішуватися шляхом запобігання дій або операцій, 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 управління доступом будується на основі

моделі Лемпсона, описаної в роботах [12] і представленої на рис. 1.4.

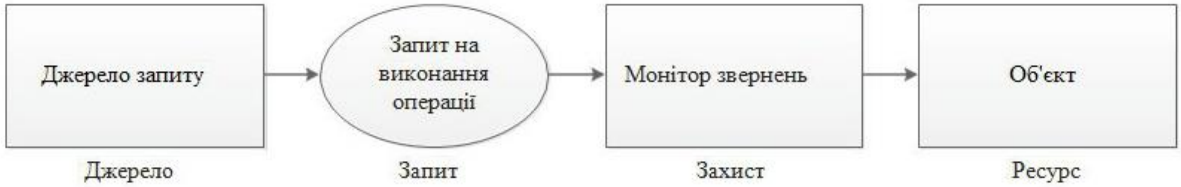



Рисунок 1.4 - Модель системи управління доступом Лемпсона

У даній моделі завдання контролю доступу покладається на монітор звернень, що є посередником при кожній спробі джерела запиту звернення до ресурсів системи (об'єктів доступу).

В існуючій теорії комп'ютерної безпеки для опису елементів комп'ютерної системи (КС) використовується ряд понять, таких як "сутність", "об'єкт", "суб'єкт", "доступ", "контейнер" [5]. Залежно від поточних умов будь-яка сутність КС може бути позначена тим чи іншим поняттям.

Для виконання операцій над сутностями КС суб'єкти здійснюють до них доступи. У більшості випадків розглядаються:

- доступ на читання із сутності;
- доступ на запис в сутність;
- доступ на запис в кінець слова, що описує стан сутності;
- доступ на активізацію (виконання) суб'єкта із сутності.

Решта види доступів, як правило, можуть бути реалізовані з використанням розглянутих [15].

Система контролю доступу в КС створюється як засіб захисту від загроз безпеки інформації. Згідно [16] при класифікації загроз виділяють три основних властивості: конфіденційність, цілісність і доступність інформації [18], які і визначають три класичних загрози безпеки інформації - загрози конфіденційності, цілісності та доступності інформації, а також ще одну - загрозу розкриття параметрів КС [5].

У відповідність з [19] управління доступом є однією з послуг захисту, що входять в загальну архітектуру захисту інформації поряд з такими послугами як аутентифікація, конфіденційність даних, цілісність даних, безвідмовність. Для забезпечення тих чи інших послуг захисту існують спеціальні механізми захисту [19], одним з яких є механізм управління доступом. У деяких випадках для надання ряду послуг захисту можуть бути задіяні кілька механізмів захисту.

У КС доступ суб'єкта до суті дозволяється системою управління

доступом при наявності у суб'єкта відповідного права доступу до суті. Спосіб завдання дозволених прав доступу суб'єктів до сутностей КС регламентується реалізованої в КС політикою управління доступом, що є складовою частиною політики безпеки КС [7].

Відомі такі види політик управління доступом, що визначають спосіб завдання дозволених прав доступу суб'єкта до сутностей:

- дискреційна політика управління доступом [1];
- мандатна (повноважна) політика управління доступом [10];
- політика рольового управління доступом [13];
- політика безпеки інформаційних потоків [14];
- політика безпеки ізольованою програмного середовища (ІПС) [17].

Формальні моделі безпеки КС [6], що описують порядок функціонування тієї чи іншої політики управління доступом, використовуються для обґрунтування захищеності сучасних і перспективних КС. Очевидно, що технологічний розвиток КС знаходиться в постійному русі і з появою нових функціональних можливостей виникають і нові чинники, що створюють загрозу безпеці інформації, захист від яких в існуючих формальних моделях безпеки не передбачена. Тому кожна нова формальна модель намагається врахувати знову виникають чинники, що призводять до появи нових загроз безпеки інформації. Класифікація та взаємозв'язок ряду формальних моделей безпеки КС зображена на рис. 1.5.

В даний час існують і безліч різних формальних моделей безпеки КС, що ставлять перед собою мету з одного боку здійснити більш повний облік всіх факторів, досягнення якої дозволити зробити модель безпеки КС більш гнучкою і адаптивною до умов функціонування реальних КС, а з іншого - використовувати більш досконалі механізми управління доступом, що спрощують процедури адміністрування складних КС.

До таких моделей безпеки КС можна віднести наступні:

– політика безпеки на основі решіток - LBAC (Lattice-Based Access Control) [13];

– політика безпеки на основі розташування - LBAC (Location- Based Access Control) [10];

– політика безпеки на основі контексту - CBAC (Context-Based Access Control) [11];

– атрибутна політика безпеки - ABAC (Attribute-Based Access Control) [27].

Крім впливу припущень на безпеку КС при її розробці серйозний вплив надає і неможливість врахувати всі можливі умови функціювання КС в реальному середовищі і, відповідно, виконання вимог безпеки КС.

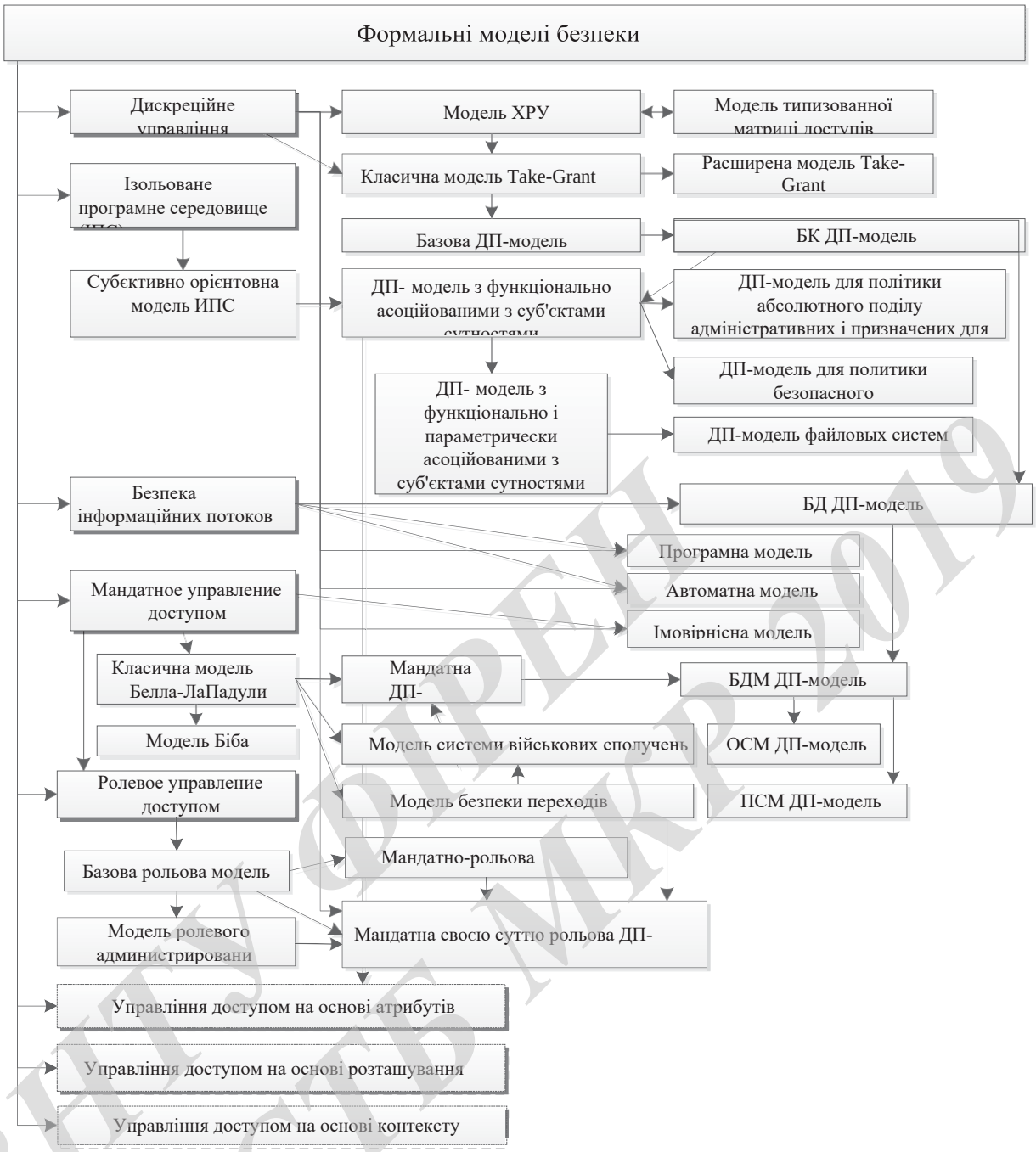



Рисунок 1.5 – Класифікація та взаємозв'язок окремих формальних моделей безпеки КС

З точки зору реалізації формальних моделей безпеки для управління доступом користувачів МАП виникає об'єктивна потреба враховувати розташування як фактор, що впливає на стан безпеки інформації в КС. У роботах [12] наведено опис формальних моделей безпеки КС, які враховують місце розташування користувачів і пристроїв. Однак при більш детальному розгляді проблеми обліку місця розташування в даних моделях чітко видно ряд недоліків, що серйозно впливають на адекватність моделі реальним КС і безпеку функціонування таких систем. До даних недоліків

відносяться наступні:

– питання безпосереднього визначення місцеположення як координат користувачів і пристроїв або приміщень, в яких знаходяться користувачі, виноситься за рамки розгляду даних робіт;

– не враховується помилка визначення місця розташування пристроїв, виникаюча внаслідок недосконалості сучасних методів позиціонування МАП, як на відкритій місцевості, так і в приміщеннях всередині будівлі;

– не розглядається питання оцінки вимог безпеки до пристроїв, в залежності від їх місця розташування і рівня вимоги по захищеності спеціальних приміщень, в яких вони знаходяться, а також рівня конфіденційності інформації та послуг, до яких вони вимагають доступ;

– як СЗІ в КС не використовуються можливості інтелектуального блокування МАп або їх окремих функціональних блоків, що представляють в певних умовах доступу загрозу інформаційній безпеці в ЗКМ.

Висновок: наявність зазначених недоліків свідчить про те, що існуючі моделі безпеки КС, що враховують такий фактор як місце розташування пристроїв і користувачів, вимагають серйозного доопрацювання, оскільки не є адекватними реальним КС і не гарантують безпеку інформації при використанні МАП.

## 1.3 Моделі загроз і порушника інформаційної безпеки при експлуатації мобільних абонентських пристроїв і аналіз технічних рішень для захисту від них

### 1.3.1 Характеристика та особливості сучасних мобільних абонентських пристроїв

Сучасні МАП, що володіють і обчислювальними і комунікаційними ресурсами, є багатофункціональне медіапристроїв, в якому функція телефонних переговорів не є першочергово важливою [31]. Для поліпшення показника економічності основні вузли сучасних МАП агреговані в складі мікросхеми класу SoC (System-on-Chip - системі на чіпі), на яку покладається весь перелік завдань збору, обробки, зберігання та обміну користувальницької і службовою інформацією [18]. Така SoC часто об'єднує на одному кристалі декілька ядер процесора, комунікаційний процесор, графічний співпроцесор і ін. Додавання при необхідності мікроконтролерів для кодування мови, високочастотних блоків для роботи в різних стандартах мережі стільникового зв'язку, інтерфейсних блоків Wi-Fi або

інший бездротової мережі, модулів GPS / ГЛОНАСС / Galileo / Beidou, а також набір інтерфейсів для взаємодії з різними типами пристроїв (USB, SD, MMC, UART і ін.) забезпечує конфігурація МАП для вирішення різних завдань і вимог користувачів й і забезпечує багатофункціональність сучасних МАП.

При експлуатації МАП існує ряд важливих особливостей, наданий істотний вплив на стан захищеності інформаційного взаємодії в рамках роботи в ЗКС [9]. До них відносяться:

1. Мініатюрність МАП. Дана властивість МАП призводить до обмеження можливостей інтерфейсу взаємодії з користувачем, впливає на обчислювальні і функціональні можливості, підвищує ризик втрати МАП і, відповідно, використання його неавторизованих користувачем.

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

3. Обмеженість обчислювальних ресурсів МАП. Даний фактор впливає на виконувані в МАП обчислювальні процеси. Оскільки процеси, що відповідають за функції захисту інформації (ЗІ), як правило, повинні виконуватися у фоновому режимі і постійно задіяти певну частину обчислювальних ресурсів, то в умовах обмеженості цих ресурсів в МАП виникають і обмеження на функціональність і можливості таких процесів.

4. Багатофункціональність МАП. До сучасних функцій МАП можна віднести:

- використання МАП в вигляді фото- і відеокамери;
- використання МАП як навігаційного пристрою;
- використання МАП в якості модему;
- використання МАП як переносну точки доступу;
- використання МАП в якості диктофона;
- використання МАП в якості змінного носія інформації.

5. Доступ до послуг корпоративної мережі на основі використання принципу одноразового входу SSO ("Single Sign-On"). Дана особливість є наслідком мініатюрності МАП і складності людино-машинного взаємодії, характерного для МАП. У поєднанні з мобільністю і мініатюрністю МАП використання режиму SSO призводить до збільшення ризиків використання МАП неавторизованих користувачем.

6. Доступ до інформаційних ресурсів мереж з різними вимогами по захищеності. Використання МАП для доступу до мереж з різними вимогами

по захищеності в даний час обмежений, оскільки не існує ефективних СЗІ, що забезпечують безпеку інформації. Існуючі підходи по ЗІ, використовувані в стаціонарних СВТ, не застосовні в повній мірі до МАП через обмеженість їх обчислювальних ресурсів, а також особливостей їх програмно-апаратної архітектури.

Зазначені особливості збільшують ймовірність здійснення погроз ІБ при роботі з МАП в умовах ЗКМ, тому необхідно враховувати фактори, що впливають на безпеку інформації.

Істотне значення при розробці СЗІ для МАП мають питання їх конфігурації з урахуванням показників ресурсоспоживання [17], що передбачають вибір та розробку СЗІ шляхом комбінування окремих компонентів захисту з урахуванням їх властивостей, обмежень і вимог до них з боку МАП.

### 1.3.2 Актуальні чинники, що впливають на безпеку інформації при використанні мобільних абонентських пристроїв

На основі ГОСТ Р 51275-2006 [16] і з урахуванням того, що експлуатація МАП передбачається в мережах з різними вимогами по захищеності, а також з огляду на зазначені відмінні риси МАП в порівнянні зі стаціонарними СВТ, були виділені актуальні фактори, що впливають на безпечність інформації при використанні МАП в ЗКМ. Перелік зазначених факторів представлений в табл. 1.1.

Аналіз представлених факторів дозволяє зробити наступні висновки:

1) значна частка чинників, що впливають на ІБ при роботі з МАП, є суб'єктивною, тобто залежної від користувачів;

2) велика частина виділених об'єктивних внутрішніх чинників, що впливають на безпеку інформації, є наслідком наявності в складі МАП функціональних блоків (модулів), що створюють технічні канали витоку інформації при їх використанні всередині або поблизу спеціальних приміщень ЗКС, а також при незахищеному доступі до конфіденційної інформації.

Проведений аналіз актуальних чинників, що впливають на безпеку інформації при роботі з МАП, дозволяє сформувати перелік загроз безпеки інформації, а також модель порушника при експлуатації МАП в ЗКМ.

### 1.3.3 Модель загроз і порушника безпеки при використанні мобільність них абонентських пристроїв в корпоративних мережах з різними вимогами по захищеності

Сукупність перерахованих актуальних чинників, що впливають на безпеку інформації при експлуатації МАП, дозволяє сформувати модель загроз інформації в ЗКС при доступі до неї користувачів МАП. У ряді випадків інформаційний доступ може бути підданий загрозам ІБ, які виникають внаслідок використання сторонніх додатків, а також пристроїв, які з'єднано МАП в рамках інформаційної взаємодії всередині ЗКМ. У роботах [8] наводиться опис моделі доступу до інформаційних сервісів, при якій можлива реалізація атаки типу "відмова в обслуговуванні" в зв'язку з наявністю подібних сторонніх додатків та інформаційної взаємодії з ними, методика розрахунку оцінки захищеності такої системи, а також методики виявлення і протидії даному виду атак.

При розробці моделі загроз необхідно враховувати особливості МАП, відрізняючи їх від стаціонарних СВТ, а також принципи забезпечення ІБ в ЗКМ з використанням МАП [3]:

1. Принцип відсутності довіри до імпортної електроніці на базі SoC, а також архітектури найбільш поширених процесорів з ARM- архітектурою з апаратної віртуалізації основний ОС (наприклад, Android) і закритою довіреної ( "Trusted OS"). Засобами захисту може виступати власна довірена ОС з довіреною початковим завантажувачем (апаратно програмним модулем довіреної завантаження) для процесорів з ARM- архітектурою з контролем відсутності прихованих апаратних не декларований можливостей.

2. Принцип ненадійності МАП. Вимагає наявності СЗІ, що дозволяють гарантувати необхідний рівень захисту інформації в ЗКМ за умови відсутності довіри до МАП. Засобами захисту можуть виступати:

- заборона або обмеження на використання особистих МАП;
- запуск корпоративних додатків в ізольованих контейнерах;
- використання додатків, які відстежують стан МАП;
- використання довіреної програмно-апаратної середовища.

3. Принцип небезпеки бездротових з'єднань, використовуваних МАП. Вимагає наявності СЗІ, що дозволяють гарантувати автентичність сторін, що беруть участь в бездротовому мережному взаємодії, а також захищеність переданих даних. Засобами захисту можуть виступати:

- застосування шифрування при передачі даних;
- використання взаємної аутентифікації на основі криптографічних алгоритмів.

4. Принцип небезпеки сторонніх додатків. Передбачається, що будь-які зовнішні програми небезпечні і створюють канали витоку інформації,

що захищається з МАП і з ЗКС. Вимагає наявності СЗІ, що забезпечують довіреність використовуваних в МАП додатків, а також відсутність каналів витоку інформації, що виникають в процесі запуску встановлених в МАП додатків. Засобами захисту можуть виступати:

– ізольована програмне середовище (ІПС);

– безпечний ізольований контейнер для корпоративних додатків (наприклад, засоби програмної або апаратної віртуалізації);

– термінальний доступ до додатків, розташованим на віддаленому захищеному корпоративному сервері;

– довірений гіпервізор для запуску додатків в ізольованій захищеній оболонці.

5. Принцип небезпеки пристроїв, які з'єднано МАП. Сучасне МАП є багатофункціональним медіапристроїв з багатьма функціями, здатне взаємодіяти з великою кількістю різноманітних пристроїв і носіїв інформації. Забезпечення необхідної захищеності передбачає гарантованість того, що все що підключаються і взаємодіючі з МАП пристрої безпечні і є довіреними. Засобами захисту можуть бути:

– засоби контролю підключаються до МАП пристроїв;

– засоби контролю стану і функціональних можливостей окремих модулів МАП;

– засоби контролю переданих даних в процесі взаємодії МАП з іншими пристроями.

З урахуванням даних принципів, а також на основі досліджень [10] і проведеного аналізу факторів, що впливають на безпеку інформації при експлуатації МАП, виділені актуальні загрози ІБ. Загрози ІБ при експлуатації МАП представлені у вигляді: <Загроза>: = <джерело загрози »,« вразливість »,« спосіб реалізації загрози »,« об'єкт впливу (програма, протокол, дані і т.д. "," Деструктивний вплив>.

Основним джерелом загроз ІБ, що розглядаються в даній роботі, є внутрішній порушник, оскільки для ефективного захисту від інших джерел придатні наявні СЗІ:

1) для захисту від зовнішнього порушника - комплекс організаційно-технічних заходів щодо виконання вимог ІБ в ЗКМ;

2) для захисту від програмно-апаратних закладок і шкідливих програм - комплекс заходів з ліцензування та сертифікації МАП, а також застосування ізольованою програмного середовища в складі системного ПО МАП, довіреної ОС і АПМДЗ.

Основними уразливими є:

– уразливості, пов'язані з недоліками організації ЗІ від НСД;

– наявність технічних каналів витоку інформації (ТКВІ) [33] в МАП в умовах експлуатації МАП в заборонених режимах роботи.

У зв'язку з необхідністю використання єдиного МАП для доступу до корпоративних мереж з різними вимогами по захищеності важливим завданням є створення умов для такого управління програмно апаратної конфігурацією МАП, при якому буде виключена наявність ТКВІ при доступі з використанням єдиного МАП до ресурсів корпоративних мереж з різними вимогами по захищеності. Типова схема ТКВІ в МАП представлена на рис. 1.6.


Рисунок 1.6 – Схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки

Одним з ефективних засобів запобігання витоку інформації по ТКВІ може бути система управління програмно-апаратною конфігурацією МАП, що дозволяє відключати модулі МАП (наприклад, мікрофон, радіоінтерфейс, що запам'ятовують пристрої), що створюють інформаційні джерела сигналу, в залежності від умов (атрибутів доступу), в яких знаходиться МАП і до яких можна віднести, в тому числі, місце розташування. При відсутності такої системи внутрішній порушник має технічну можливість використовувати МАП як засіб зв'язку незалежно від умов доступу і свого місця розташування в організації. Наприклад, в разі несанкціонованого або випадкового проносу МАП в спеціальне приміщення, в якому заборонена обробка відкритої інформації і використання МАП, даний пристрій стає джерелом інформаційних сигналів, що містять конфіденційну інформацію. Схема витоку інформації представлена на рис. 1.7.

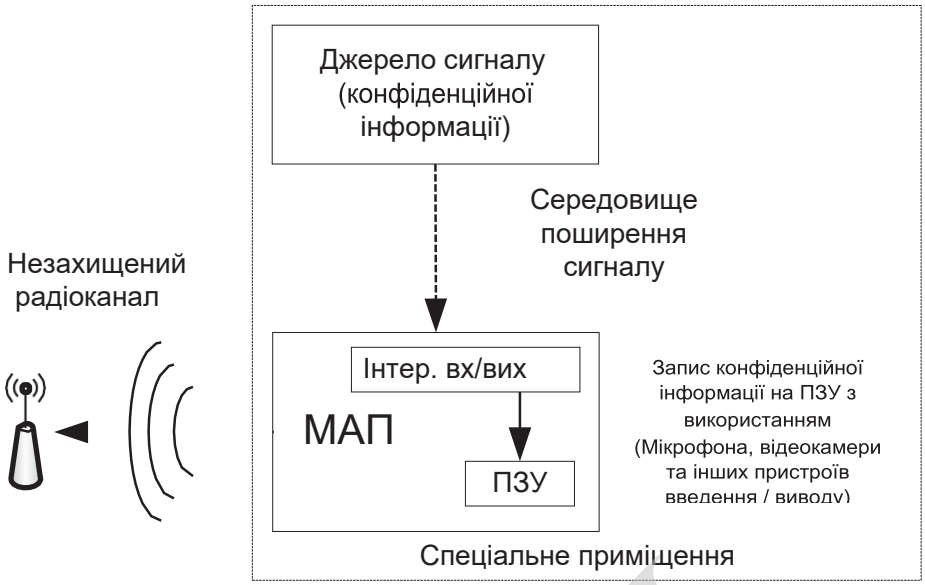



Рисунок 1.7 – Схема витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні

В даний час існує ряд СЗІ у вигляді MDM-рішень, що дозволяють блокувати роботу МАП в заборонених режимах. Дані рішення не припускають апаратної переконфігурації пристрою і працюють на рівні додатків, що є істотним недоліків з урахуванням принципів відсутності довіри до імпортної електроніки, ненадійності МАП і відсутності довіри до сторонніх додатків.

Контроль вносити незахищених МАП здійснюється, як правило, організаційно-технічними заходами, які порівняно легко долаються за відсутності ефективного контролю виконання даних заходів.

Таким чином, існує об'єктивна потреба в розробці таких СЗІ, які дозволять в автоматичному режимі управляти не тільки програмної, але і апаратною конфігурацією МАП, блокуючи можливі канали витоку інформації при використанні пристрою в організаціях, в яких передбачена обробка конфіденційної інформації, незалежно від місцезнаходження МАП на території даної організації.

Розробляється система управління безпекою МАП направлена в першу чергу на захист від загроз, пов'язаних з:

– обходом СЗІ;

– деструктивними впливами на СЗІ;

– перехопленням і модифікації інформації, що передається;

– розголошенням і організації витоку інформації в незахищених місцях доступу;

– використанням нештатного ПО;

– внесенням вразливостей з використанням штатних засобів.

Основними об'єктами захисту інформації при реалізації розроблюваної СЗІ є:

– інформація, що обробляється МАП;

– інформація в засобах, що реалізують мережеве взаємодія, а також в каналах передачі даних в мережі;

– інформація, що обробляється в спеціальних приміщеннях ЗКМ.

Зазначені описові моделі загроз і порушника ІБ при використанні МАП дозволяють більш детально сформувати вимоги до розроблюваної системі управління безпекою МАП та реалізованих СЗІ для забезпечення безпеки інформації в корпоративних мережах з різними вимогами по захищеності.

### 1.3.3 Технічні рішення для захисту інформації при експлуатації мобільних абонентських пристроїв

В даний час для захисту інформації при експлуатації МАП в ЗКМ розроблено досить велику кількість програмних, програмно-апаратних рішень, що виконують функції СЗІ. Серед ПО для захисту інформації в МАП і управління доступом до послуг ЗКС відомі такі продукти, як програмні комплекси "ViPNet Client" [14], CISCO для управління доступом Cisco Unified Access, Cisco Identity Services Engine [18], Cisco Secure ACS [20] , "MobileIron", "Kaspersky Security 10" для мобільних пристроїв, "McAfee Enterprise Mobility Management", "Afaria", "SOTI Mobicontrol", "AirWatch MDM", "Samsung Enterprise Access Layer", "Juniper Junos Pulse MSS".

Дані рішення є реалізації технології MDM (Mobile Device Management - управління МАП), MAM (Mobile Application Management - управління корпоративними додатками на МАП) і MIM (Mobile Information Management - управління корпоративними документами з використанням МАП), що представляють собою елементи комплексного ПО для роботи з корпоративними системами за допомогою МАП, що забезпечує безпеку, контроль і підтримку МАП, використовуваних персоналом компаній. Як видно з назви технології, управління МАП здійснюється на рівні додатків і доступів до документів.

Істотним недоліком даних рішень є використання лише програмного управління МАП, що не дозволяє в повній мірі гарантувати безпеку інформації при доступі до захищеної служби, а також відсутність

математично доведеного коректного формального апарату моделювання безпеки МАП в ЗКМ.

До апаратних і програмно-апаратним захищеним технічним рішенням в даний час відносяться [4]:

– захищені мобільні телефони;
– технічні засоби захищеного термінального доступу;
– захищені планшетні комп'ютери;
– захищені мобільні комп'ютери.

В даний час відомі наступні рішення в області захищених мобільних телефонів:

1. Захищений телефон стандарту GSM "Талісман 395" [18].
2. Спеціалізований термінал мобільного зв'язку "Сапфір-К" [19].
3. Спеціальний стільниковий телефон "SMP-АТЛАС / 2" [20].
4. Апаратура шифрування мовних повідомлень "Апаратура 605" [2].
5. Спеціальний мікростільниковий телефон "М-549М" [22].

До відомих технічних засобів захищеного термінального доступу можна віднести:

1. Термінальний клієнт "ViPNet Terminal" [14].
2. Термінальний клієнт "КАМІ-Термінал" [12].
3. Термінальний клієнт "HELIOS ProfyShield LT-A330-1s" [11]..

Відомий захищений планшетний комп'ютер "Континент Т-10" [15], сертифікований ФСТЕК і ФСБ, а також ряд таких захищених мобільних комп'ютерів як:

1. Мобільний захищене автоматизоване робоче місце доступу в мережу Інтернет "МАРМ ДСІ" [14].
2. Мобільний обчислювальний комплекс "ІНФОПРО" МВК-2 [25].

Більшість представлених технічних рішень дозволяють забезпечувати захищений доступ до конфіденційної інформації. Деякі забезпечують захищений доступ до відомостей, які містять інформацію, віднесену до державної таємниці. Однак на даний момент відсутні технічні рішення, що дозволяють забезпечувати доступ до мереж з різними вимогами по захищеності з використанням одного МАП. Іншим недоліком є те, що не існує ефективних СЗІ, які враховують місце розташування МАП. Дані недоліки СЗІ в даний час усуваються шляхом застосування організаційних заходів щодо МАП і їх користувачів, що включають в себе, в тому числі, заборона на пронос особистих МАП і їх використання в ЗКМ.

Існує ряд технічних рішень від іноземних виробників, таких як у компанії CISCO [20], що дозволяють забезпечувати управління доступ користувачів МАП в залежності від їх місця розташування в ЗКМ. Однак в

даних рішеннях розташування визначається лише точкою підключення до БМПД ЗКМ, при цьому рівень конфіденційності доступу визначається рівнем конфіденційності точки доступу, а не реальним місцем розташування користувача МАП.

Одним з найбільш істотних недоліків сучасних захищених МАП є обмежений перелік послуг, що надаються. Відсутність можливості поєднувати функціональність сучасних смартфонів і захищених технічних мобільних рішень, які допустимо використовувати в ЗКМ за умови виконання вимог ІБ, позначається на доступності та своєчасності надання абонентам послуг. Це пов'язано з відсутністю ефективних СЗІ, що дозволяють гарантовано виключити роботу МАП в небезпечних режимах (конфігураціях), а також забезпечити відсутність технічних каналів витоку інформації в період знаходження користувача МАП в зоні доступу ЗКМ.

Таким чином, на основі проведеного аналізу існуючих захищених технічних мобільних рішень виділені наступні недоліки:

– відсутність СЗІ, що дозволяють забезпечити безпечний доступ до мереж з різними вимогами по захищеності з використанням одного пристрою;

– відсутність технічних рішень, що дозволяють визначати місцезнаходження МАП і враховувати вимоги ІБ до МАП, що пред'являються до СВТ у Вашій місцевості в ЗКМ;

– обмежена кількість наданих користувачам МАП послуг в захищених мобільних рішеннях.

## 1.4 Способи побудови комплексної системи захисту інформації при доступі до мереж з різними вимогами по захищеності

Для захисту інформації, що обробляється в ЗКМ, застосовуються СЗІ, параметри яких визначаються політикою безпеки даної ЗКМ на підставі рівня конфіденційності оброблюваної інформації і відповідними нормативно-правовими актами [16]. При забезпеченні доступу МАП до конфіденційної інформації і мереж з різними вимогами по захищеності в даний час застосовується схема, представлена на рис. 1.8 [15].

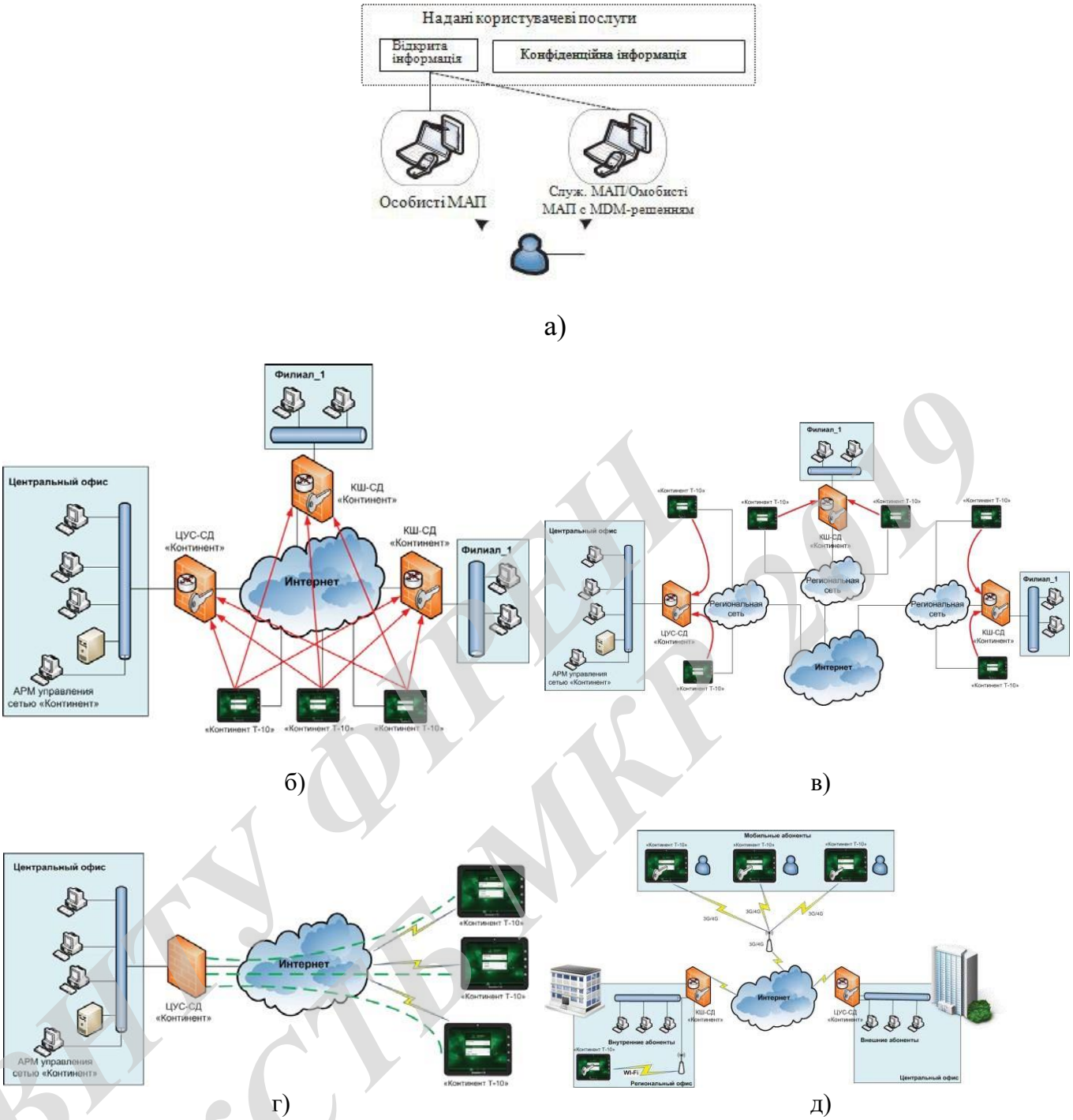



Рисунок 1.8 – Схема доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП: а) узагальнена; б-д) варіанти підключення на прикладі захищеного планшета "Континент Т-10"

Порядок і режим доступу до конфіденційної інформації з використанням зазначеної схеми визначається, в тому числі, і комплексом організаційних і організаційно-технічних заходів щодо ЗІ в ЗКМ.

Як видно з рис. 1.8 в даний час можуть застосовуватися кілька МАП

для роботи в мережах з різними вимогами по захищеності. Однак в ряді випадків потребує об'єднання у пару даних мереж (контурів обробки інформації з різними вимогами по захищеності). При цьому виконання вимог по ІБ має відповідати рівню захисту, висунутій до контуру з більш високими вимогами по захищеності.

В даний час відомі кілька підходів для сполучення контурів обробки інформації з різними вимогами по захищеності. До них відносяться:

1. Технології односпрямованих шлюзів. Гарантують передачу інформації в одному напрямку. В даний час відомі такі технічні рішення як односпрямований шлюз "Атлікс-Шлюз-К" [27], система односпрямованої передачі даних "ДИОД" [16] та інші.

2. Технології віртуалізації. Використання довірених гіпервізора, що дозволяють в одному корпусі об'єднати кілька захищених програмно апаратних контейнерів, в яких допустимо обробляти інформацію з різних вимог по захищеності.

3. Технологічне об'єднання в єдиному корпусі програмно-апаратних платформ, виконане з використанням оптоелектронної, трансформаторної розв'язки, що дозволяє розділити і ізолювати тракти проходження інформації з різними вимогами по захищеності один від одного.

4. Термінальний доступ. Реалізація технологій тонкого клієнта з використанням серверів додатків.

З точки зору реалізації сполучення контурів обробки інформації з різними вимогами по захищеності при експлуатації МАП технології односпрямованих шлюзів застосовні лише як допоміжні засоби. Технології віртуалізації вимагають серйозних обчислювальних ресурсів, якими володіють тільки планшетні та мобільні комп'ютери і досить обмежено - смартфони.

Технологічне об'єднання в єдиному корпусі програмно-апаратних платформ, що дозволяє розділити і ізолювати тракти проходження інформації, до яких пред'являються різні вимоги по захищеності, один від одного, в даний час реалізовано тільки для стаціонарних обчислювальних систем. У той же час даний напрямок є перспективним для МАП, оскільки технічний рівень в даний час дозволяє об'єднувати в єдиному корпусі багатопроцесорні системи, в тому числі і в МАП.

Термінальний доступ є найбільш оптимальним засобом при доступі до інформації з різними вимогами по захищеності. Однак реалізація даних технологій не дозволяє здійснювати управління функціональністю МАП, виключаючи його роботу і роботу окремих функціональних модулів МАП в заборонених режимах, а також не вирішує завдання визначення

місцеположення МАП.

Таким чином, для усунення проблеми реалізації сполучення контурів обробки інформації з різними вимогами по захищеності в МАП необхідне рішення наступних завдань:

1) розробка формальної моделі безпеки МАП, що враховує програмно-апаратну конфігурацію МАП і його розташування;

2) розробка системи визначення місця розташування МАП, що дозволяє з необхідною достовірністю визначати місцезнаходження МАП в спеціальних приміщеннях ЗКМ в режимі реального часу;

3) розробка системи управління безпекою (програмно-апаратної конфігурації) МАП в залежності від його місця розташування та інших атрибутів доступу, а також вимог щодо якості послуг, що надаються;

4) розробка технічних пропозицій по реалізації системи управління безпекою МАП, що дозволяє функціонувати Цей пристрій в мережах з різними вимогами по захищеності, з урахуванням місця розташування МАП та інших атрибутів доступу.

Рішення даних завдань можливо за допомогою застосування агентноорієнтірованного підходу [14], що є елементом штучного інтелекту і побудованого на основі класичної клієнт-серверної архітектури.

Узагальнена схема доступу в цьому випадку може мати вигляд, представлений на рис. 1.9.


Рисунок 1.9 – Схема доступу до інформації з використанням різних конфігурацій МАП

Для вирішення завдання визначення місцеположення МАП в якості

агентів можуть виступати точки доступу БМПД, що збирають відомості про рівень сигналу МАП, на основі якого буде здійснюватися розрахунок місцеположення МАП в межах області покриття БМПД. Даний розрахунок може здійснюватися, як в контролері бездротової мережі, так і централізовано в точці прийняття рішення по управлінню конфігурацією МАП. Прототип такої багатоагентної системи представлений на малюнку 1.10.

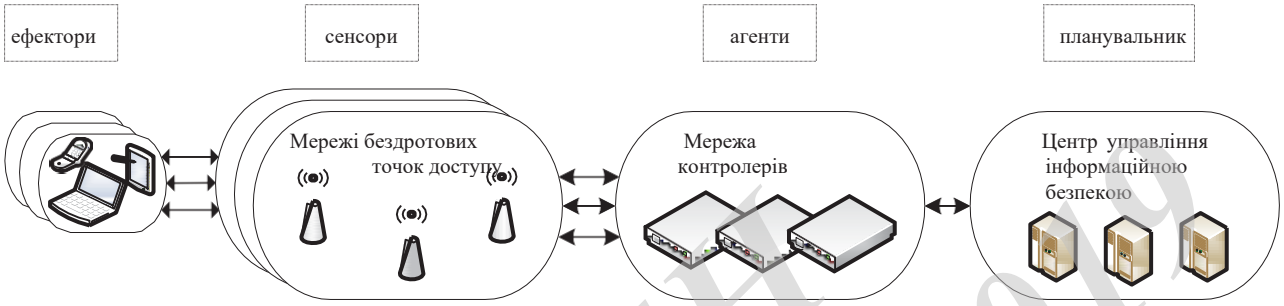



Рисунок 1.10 – Багатоагентна система позиціонування МАП

Завдання з управління конфігурацією МАП в залежності від представлених вимог ІБ може вирішуватися за рахунок впровадження в МАП програмно-апаратного агента, наприклад, на базі довіреної апаратно-програмного модуля довіреною завантаження (АПМДЗ), обмінюється інформацією по захищеному каналу управління через довірену бездротову мережу доступу з центром управління інформаційної безпеки (ЦУІБ) ЗКМ. Схема такої системи управління конфігурацією МАП представлена на рис. 1.11.


Рисунок 1.11 – Схема підсистеми управління конфігурацією МАП

Реалізація представлених систем спільно з використанням технологій термінального доступу, віртуалізації або оптоелектронної розв'язки об'єднаних програмно-апаратних платформ в єдиному корпусі дозволить забезпечити захищений віддалений доступ до мереж з різними вимогами по захищеності з використанням одного МАП.

Для підвищення ймовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами по захищеності, необхідно розробити систему управління безпекою МАП, що дозволяє управляти програмно апаратної конфігурацією МАП і доступом мобільних користувачів до інфокомунікаційних послугами та ресурсів в залежності від атрибутів доступу, включаючи місце розташування пристрою, а також вимог щодо безпеки інформації та якості послуг, що надаються.

Формальна постановка задачі дослідження: на основі теорії машинного навчання, математичний статистики та чисельних методів розробити модель безпеки МАП і алгоритм управління безпекою МАП, що враховує атрибути доступу, включаючи місце розташування пристрою, вимоги з безпеки інформації та якості послуг, що надаються..

Початкові дані:

1) універсальне мобільне абонентський пристрій (МАП) MD, його технічних характеристики;

2) безліч можливих конфігурацій МАП - CONF;

3) розташування і параметри приміщень:

$$Rooms = \left\{ \text{room}_i = \left( (x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), \text{L}_{Room_i} \right) \right\}, i = \overline{1, N}_{Rooms}, \quad (1.1)$$

$_i$

де $L_{Rooms_i}$ - рівень вимог по захищеності приміщення, $(x_{i1},y_{i1}),(x_{i2},y_{i2}),...,(x_{in},y_{in})$ - координати n кутів приміщень; $N_{Rooms}$ - кількість приміщень

4) розташування точок доступу бездротової мережі $AP = \left\{ AP_j = (x_i, y_i) \right\}$, $j = \overline{1, N}_{AP}$, де $(x_i, y_i)$ - координати точок доступу, $N_{AP}$ - кількість точок доступу;

5) безліч порогових значень приватних показників ефективності: $H = \left\{ P_\beta \left( \overset{\circ}{L}_{Room} > L_{Room} \right) \le P_\beta^{\text{потр}}, T_{RECONF} \le T_{RECONF}^{\text{доп}} \right\}$ ;

6) сукупність атрибутів доступу $A = \{ a_i \}$ включає:

– ідентифікаційні дані про користувача, МАП, операційній системі (ОС) і додатках МАП;

– мережева адресна інформація;

– рівень конфіденційності і ідентифікатор запитуваної послуги (ресурсу).

Потрібно:

1) розробити модель безпеки МАП Z, що враховує ймовірність знаходження МАП в спеціальних приміщеннях, обгрунтувати її коректність і оцінити якість;

2) розробити алгоритм управління безпекою МАП шляхом реалізації вирішального правила F віднесення сукупності атрибутів доступу, що включають в себе, в тому числі, ймовірність знаходження МАП в спеціальному приміщенні до дозволеної конфігурації (станом) МАП, що забезпечує безпеку інформації при доступі до послуг корпоративних мереж з різними вимогами по захищеності і задану якість надання послуг, оцінити властивості алгоритму:

$$\begin{cases} Z \xrightarrow{F(MD,Rooms,AP,A)} \{CONF_i\}_{t+1}; \\ P_{БІ}(T) > P_{БІ}^{потр}(T) \end{cases} \quad (1.2)$$

3) розробити науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП, що дозволяє підвищити безпеку інформації при експлуатації МАП в корпоративних мережах з різними вимогами по захищеності при наступних обмеженнях і припущеннях:

– до складу корпоративної мережі входить довірена бездротова мережа передачі даних (БМПД);

– канал управління між довіреними точками доступу і МАП захищений криптографічними засобами захисту інформації;

– МАП має можливість функціонувати в різних програмно-апаратних конфігураціях;

– в складі МАП функціонує апаратно-програмний модуль довіреної завантаження (АПМДЗ), що є програмно-апаратним агентом, управляючим конфігурацією (станом) МАП;

– на МАП функціонує довірена операційна система (ДОС);

– в ДОС МАП функціонує ізольована програмне середовище (ІПС);

– користувач МАП в корпоративній мережі аутентифікований;

4) оцінити ефективність розробленої системи управління безпекою МАП.

Для отримання оцінки ефективності запропонованої системи управління безпекою МАП, а також оцінки ступеня досягнення мети дослідження доцільно скористатися критерієм переваги [24], виходячи із специфіки пропонованих до системи вимог.

Система показників якості [5] побудована з таких міркувань. Оскільки мета розробляється - забезпечення безпеки інформації (захисту інформації)

при експлуатації МАП в корпоративних мережах з різними вимогами по захищеності, то ступінь досягнення даної мети відповідно до теорії ефективності цілеспрямованих процесів [24] може бути представлена у вигляді виразу:

$$P_{ЗІМАП} = P\left( REZ \geq REZ^{\text{тр}} \right) \cdot P\left( RES \leq RES^{\text{доп}} \right) \cdot P\left( OPR \leq OPR^{\text{доп}} \right), \quad (1.3)$$

де $REZ$ – результативність процесу захисту інформації; $REZ^{\text{тр}}$ – необхідне значення результативності процесу захисту інформації; $RES$ – ресурсомісткість процесу захисту інформації; $RES^{\text{доп}}$ – максимально допустимий витрата ресурсів для процесу захисту інформації; $OPR$ – витрати оперативного часу для досягнення мети функціонування системи; $OPR^{\text{доп}}$ – максимально допустимий час для досягнення мети функціонування системи.

У відповідність з [19] безпеку інформації є комплексним властивістю і забезпечується за рахунок виконання вимог щодо забезпечення конфіденційності, цілісності та доступності інформації. Виходячи з цього, результативність процесу захисту інформації при експлуатації МАП може бути представлена у вигляді виразу:

$$P_{БІ}(T) = P_{КІ}(T) \cdot P_{ЦІ}(T) \cdot P_{ДІ}(T). \quad (1.4)$$

де $P_{КІ}(T)$ – імовірність забезпечення конфіденційності інформації в поточному часі T; $P_{ЦІ}(T)$ – імовірність забезпечення цілісності інформації; $P_{ДІ}(T)$ – імовірність доступності інформації.

Питання цілісності інформації в роботі не розглядаються тому показник при підрахунках прийнятий рівним одиниці: $P_{ЦІ}(T) = 1$.

Імовірність забезпечення доступності інформації пропонується оцінювати по своєчасності обробки запитів на доступ до послуг [18] з урахуванням кількості доступним послуг $N_{ДУ}$ щодо їх загального числа $N_{У}$. Тоді ймовірність надання інформації або послуг $P_{ДИ}(T_{ДИ})$ за заданий час $T_{ДІ}^{\text{зад}}$ буде визначатися за допомогою табульованих неповної гамма-функції [18]:

$$P_{ДІ}(T_{ДІ}) = \frac{N_{ДП}}{N_{П}} \cdot P_{ДІ}^{У}(T_{ДІ}) = \frac{N_{ДП}}{N_{П}} \cdot \int_{0}^{\theta} \exp(-\tau) \cdot \tau^{\gamma} d\tau / \Gamma(\gamma), \quad (1.5)$$

де $\Gamma(\gamma)=\int_0^{\theta}\exp(-\tau)\cdot\tau^{\gamma}d\tau/\Gamma(\gamma)$ - гама функція,

$$\gamma=\frac{T_{повн}}{\sqrt{T_2-T_{повн}^2}},\theta=T_{ДІ}^{зад}\cdot\frac{\gamma^2}{T_{повн}}, \quad (1.6)$$

де $T_{повн},T_2$ - розраховуються відповідно середній час і 2-й момент часу реакції системи при обробці запитів системі (повного часу перебування на обробці з урахуванням очікування в черзі), $T_{ДІ}^{зад}$ - заданий час (гранично допустимий) для обробки запиту на доступ до інформації (послуг).

Метою даного дослідження є підвищення ймовірності забезпечення безпеки інформації при експлуатації МАП для доступу до інфокомунікаційних послуг і ресурсів корпоративних мереж з різними вимогами щодо захищеності, відповідно, необхідно довести, що показник ймовірності забезпечення конфіденційності інформації буде не гірше, ніж в діючих прототипах. Для забезпечення конфіденційності інформації необхідно забезпечити захист від несанкціонованого доступу (НСД), а також забезпечити збереження конфіденційності на заданому періоді часу [18]. Виходячи з цих міркувань, показник ймовірності забезпечення конфіденційності може бути представлений у вигляді виразу:

$$P_{KI}(T)=(1-P_{НДС})\cdot P_{ЗК}(T), \quad (1.7)$$

де $P_{НДС}$ - можливість НДС до інформації; $P_{ЗК}(T)$ - ймовірність збереження конфіденційності інформації на заданому періоді часу.

Імовірність НСД за умови коректно заданої політики безпеки, буде визначатися величиною ймовірності помилки 2-го роду при визначенні місця розташування МАП, яка буде безпосередньо впливати на вибір конфігурації МАП в системі управління безпекою МАП. Тоді показник ймовірності несанкціонованого доступу можна представити у вигляді виразу:

$$P_{НДС}=1-P(CONF\subset CONF^{доп})=1-P\left[\beta\left(\overset{\circ}{L}_{Room}>L_{Room}\right)\le\beta^{доп}\right], \quad (1.8)$$

$$P(CONF\subset CONF^{доп})=P\left[P_{\beta}\left(\overset{\circ}{L}_{Room}>L_{Room}\right)\le P_{\beta}^{доп}\right], \quad (1.9)$$

де $CONF$ - конфігурація МАП, сформована системою управління безпекою МАП; $CONF^{доп}$ - безліч допустимих конфігурацій МАП при поточних умовах доступу.

Показник ймовірності збереження конфіденційності інформації на заданому періоді часу визначається своєчасністю переконфігурації МАП при зміні атрибутів доступу і за умови призначення конфігурації з допустимого безлічі $P\left[\left(T_{RECONF} \le T_{RECONF}^{доп}\right)/\left(CONF \subset CONF^{доп}\right)\right]$, а також ймовірністю подолання СЗІ за даний період часу $P_{Пр3}$ [18]. Даний показник може бути представлений у вигляді виразу:

$$P_{СК}\left(T_{RECONF}\right) = P\left[\left(T_{RECONF} \le T_{RECONF}^{доп}\right)/\left(CONF \subset CONF^{доп}\right)\right]\cdot\left(1-P_{Пр3}\right). \quad (1.10)$$

У відповідність з [18] показник $P_{Пр3}$ може бути розрахований як

$$P_{Пр3} = 1 - \prod_{m=1}^{k} P_{НДС_m}, \quad (1.11)$$

де k - кількість перепон, яке необхідно подолати порушнику, щоб отримати доступ до інформаційних і програмних ресурсів, $P_{НДС_m}$ - ймовірність подолання порушником m-й перепоні (засоби захисту).

$$P_{НДС_m} = \frac{f_m}{f_m + u_m}, \quad (1.12)$$

де $f_m$ - середній час між сусідніми змінами параметрів m-й перешкоди системи захисту (час між зміною конфігурацій); $u_m$ - середній час розшифровки (розтину) значень параметрів m-й перешкоди системи захисту. Показник $P_{Пр3}$ в рамках роботи винесено в обмеження і прийнятий рівним нулю.

Ресурсомісткість процесу захисту інформації [7] при експлуатації МАП може бути визначена, виходячи з виразу:

$$RES_{ЗІМАП} = K_{ВОР}\cdot B_{ОР} + K_{ВТР}\cdot B_{ТР} + K_{ВСУ}\cdot B_{СУ} + K_{ВСВМ}\cdot \cdot B_{СВМ} + \left(\sum_{i=1}^{N_{МАП}} B_{МАП_i}\right)\cdot N_{Кор}, \quad (1.13)$$

де $K_{BOP}$ - коефіцієнт використання обчислювальних ресурсів; $B_{OP}$ - вартість обчислювальних ресурсів; $K_{BTP}$ - коефіцієнт використання телекомунікаційних ресурсів; $B_{TP}$ - вартість телекомунікаційних ресурсів; $K_{BCУ}$ - коефіцієнт використання системи управління безпекою МАП; $B_{CУ}$ - вартість системи управління безпекою МАП; $K_{BCBM}$ - коефіцієнт використання системи визначення місця розташування МАП; $B_{CBM}$ - вартість системи визначення місця розташування МАП; $B_{МАП_i}$ - вартість і - го МАП, необхідного для доступу до послуг; $N_{МАП}$ - кількістю МАП, необхідних для доступу до всього переліку послуг; $N_{Кор}$ - кількість користувачів МАП.

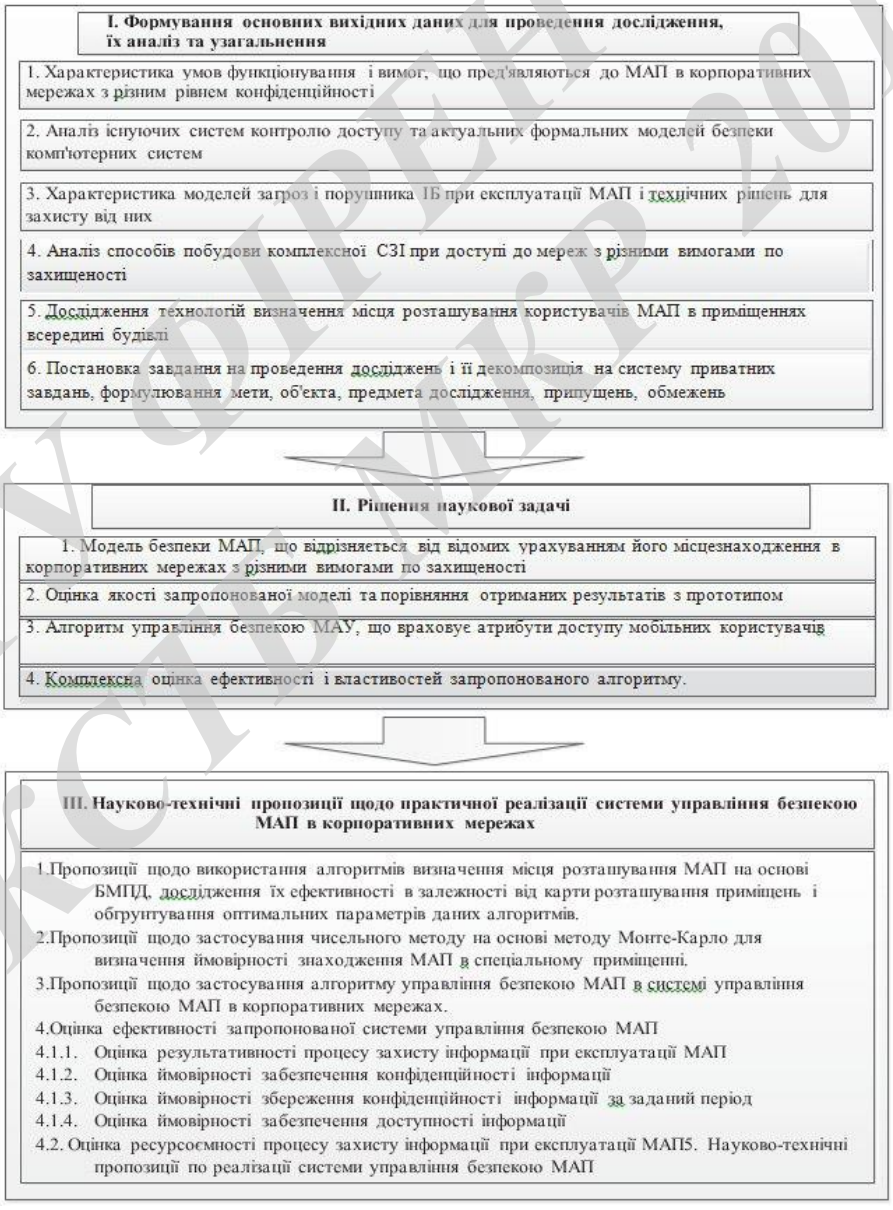



Рисунок 1.12 – Структурно-логічна схема дослідження

Для експоненційної апроксимації розподілів вихідних характеристик при їх незалежності:

Вирішення наукового завдання передбачається проводити в рамках структури дослідження, представленої на рис. 1.12

## 1.5 Висновки по 1 розділу

1. Використання обчислювальних ресурсів сучасних МАП в корпоративних мережах і забезпечення доступу до широкого переліку послуг корпоративних мереж, в тому числі, захищених є актуальним завданням. В даний час вона не вирішена, оскільки відсутні ефективні СЗІ, що нейтралізують загрози ІБ, пов'язані з використанням МАП, в тому числі при доступі до мереж з різними вимогами по захищеності.

2. Існує ряд недоліків сучасних формальних моделей безпеки комп'ютерних систем стосовно забезпечення безпеки інформації при використанні МАП, включаючи існуючі технічні та програмно-апаратні рішення:

1) відсутні технічні рішення щодо визначення місця розташування МАП, що володіють достатньою точністю;

2) відсутня технічна можливість інтелектуального програмно апаратного блокування МАП або їх окремих функціональних блоків, що представляють за певних умов загрозу ІБ в ЗКМ;

3) доступ до мереж з різними вимогами по захищеності з використанням МАП здійснюється або з використанням різних МАП відповідних необхідному рівню захищеності або з ручним перемиканням режимів роботи; відсутня автоматичне керування програмно-апаратною конфігурацією МАП в залежності від рівня конфіденційності послуг, що надаються, розташування МАП та інших атрибутів доступу.

Наявність зазначених недоліків свідчить про необхідність врахування такого чинника як місце розташування МАП, а також доопрацювання формальних моделей безпеки і обгрунтування їх коректності. Необхідна розробка нових технічних пропозицій щодо реалізації програмно-апаратної платформи універсального єдиного МАП, що дозволяє забезпечити захищений доступ до послуг мереж з різними вимогами по захищеності.

3. Для вирішення завдання сполучення контурів обробки інформації з різними вимогами по захищеності в сучасних МАП пропонується використовувати агентно-орієнтований підхід, який є елементом штучного інтелекту і побудований на основі клієнт-серверної архітектури. Даний підхід дозволить застосувати технологію віддаленого управління програмно

апаратної конфігурацією МАП на основі інформації про його місцезнаходження на і інших атрибутах доступу.

4. Постановка завдання дослідження сформульована як задача автоматичного управління з елементами машинного навчання. Для її вирішення пропонується використовувати теорію машинного навчання, теорії ймовірності та математичної статистики, апарат прихованих марківських моделей, теорію алгоритмів, теорію управління, теорію оптимізації, теорію множин, чисельні методи та методи математичного та імітаційного моделювання.

.

# 2 СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇ, ЩО ЗАБЕЗПЕЧУЮТЬ ПІДВИЩЕННЯ ІМОВІРНОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ПРИ ДОСТУПІ ДО ІНФОКОМУНІКАЦІЙНИХ ПОСЛУГ І ІНФОРМАЦІЇ КОРПОРАТИВНИХ МЕРЕЖ З РІЗНИМИ ВИМОГАМИ ПО ЗАХИЩЕНОСТІ ПІД ЧАС ВИКОРИСТАННЯ ЄДИНОГО МАП

## 2.1 Науково-технічні пропозиції по складу, структури та місця системи управління безпекою мобільними абонентськими пристроями в складі корпоративних мереж з різними рівнями захищеності

Розроблена система управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності передбачає наявність таких компонентів:

– центр управління інформаційною безпекою (ЦУІБ);
– контролер доступу мобільних пристроїв [29];
– довірена бездротова мережа передачі даних;
– підсистема визначення місця розташування [29];
– довірені багатофункціональні мобільні пристрої, до складу яких входить агентний модуль, здатний приймати сигнали управління і керувати програмно-апаратною конфігурацією пристрою [30].

В рамках управління інформаційною безпекою можуть бути також реалізовані механізми віддаленого моніторингу, засновані на використання особливостей реалізації мережевих протоколів. У роботах [26] описані спосіб віддаленого моніторингу та управління інформаційною безпекою мережевої взаємодії на основі використання системи доменних імен та програмне забезпечення, що дозволяє реалізувати даний спосіб. Для захисту ЗКС від комп'ютерних атак, а також запобігання перевантажень в мережі і помилок функціонування необхідно використовувати механізми між мережевого екранування. Реалізація таких механізмів захисту розглянута в роботі [27], що описують спосіб аналізу інформаційного потоку і визначення стану захищеності мережі на основі адаптивного прогнозування та пристрій для його здійснення, а також варіанти побудова систем дистанційного керування і моніторингу перспективних між мережевих екранів.

Для вирішення завдання безпечного доступу мобільного користувача до послуг мереж з різними вимогами по захищеності має забезпечуватися виконання наступних умов:

1. Існує бездротова мережа довірених точок доступу з відомим

місцеположенням точок доступу.

1. Канал управління між довіреними точками доступу і МАП захищений криптографічними засобами захисту інформації.

2. МАП має можливість функціонувати в різних програмноаппаратних конфігураціях.

3. На МАП функціонує апаратно-програмний модуль довіреної завантаження (АПМДЗ).

4. На мобільному пристрої функціонує довірена операційна система (ДОС).

5. У ДОС МАП функціонує ізольована програмне середовище.

6. Користувач МАП успішно аутентифікований в системі управління доступом корпоративної мережі.

В [27] запропоновано спосіб побудови захищеного віддаленого доступу до інформаційних ресурсів.

На рис. 2.1 представлена загальна структура основних компонентів ЗКС, що забезпечують функціонування розробленої системи.

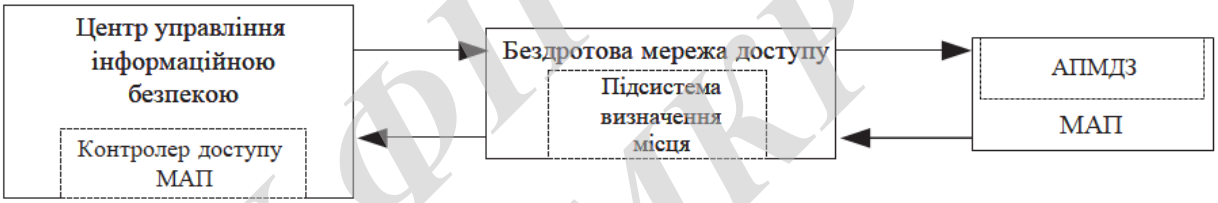



Рисунок 2.1 – Узагальнена структура основних компонентів ЗКМ

Для забезпечення наявності керованої конфігурації, а також можливості незалежної обробки інформації в МАП, даний пристрій може включати до свого складу дубльовані компоненти, що відповідають за обробку даних. Дублювання компонентів повинно забезпечувати оптоелектронну чи іншу розв'язку трактів проходження сигналів з різними вимогами по захищеності (різними рівнями конфіденційності оброблюваної інформації). Приклад такої компоновки в складі МАП представлений на рис. 2.2.

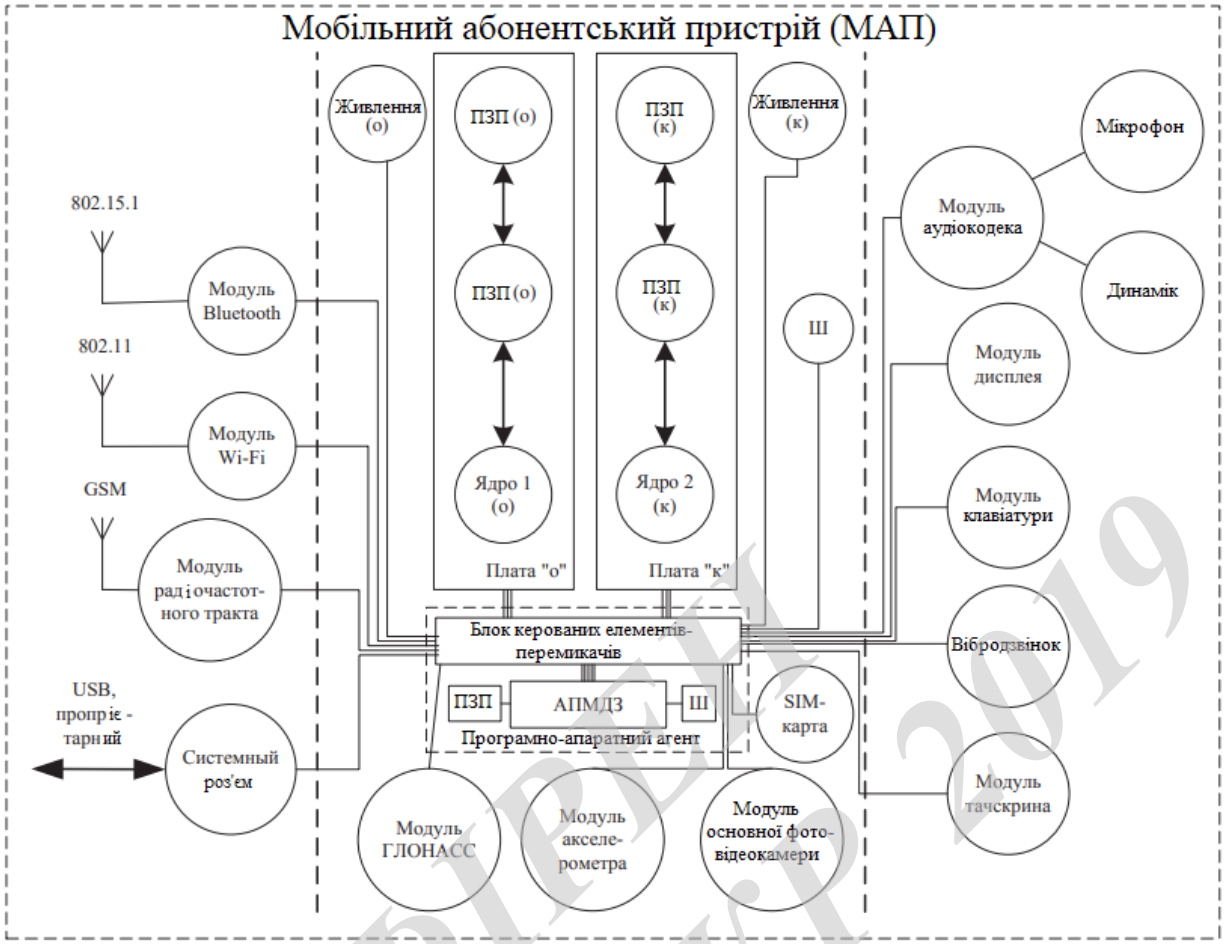



Рисунок 2.2 – Склад і структура мобільного абонентського пристрою з дублюванням функціональних блоків, що відповідають за обробку інформації в мережах з різними вимогами по захищеності

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

2.1.1 Пропозиції щодо складу і структури логічної моделі бази даних для зберігання вимог політики безпеки

Логічна модель відображає логічні зв'язки між елементами даних незалежно від їх змісту і середовищі зберігання, і будується в термінах

інформаційних одиниць, але без прив'язки до конкретної СУБД. Більш того, логічна модель даних необов'язково повинна бути виражена засобами саме реляційної моделі даних. Основним засобом розробки логічної моделі даних в даний момент є різні варіанти ER-діаграм. Одну і ту ж ER-модель можна перетворити як в реляційну модель даних, так і в модель даних для ієрархічних і мережевих СУБД, або в постреляційних модель даних.

Для зберігання вимог політики безпеки МАП необхідна наявність захищеної бази даних і системи управління базою даних (СКБД). Серед існуючих сертифіковані систем криптографічного захисту інформації (СКЗИ) відомі такі технічні рішення як "Кріпто БД" компанії "Алладин Р.Д." [26], що представляє собою ЗКЗІ для організацій, що використовують СУБД Oracle, MS SQL, Tibero.

Логічна структура містить наступні сутності: політика безпеки (ПБ); політика безпеки для групи користувачів; політика безпеки для групи пристроїв; пристрою за групами; пристрою; група пристроїв; призначені пристроїв конфігурації; власники пристроїв; конфігурації пристроїв; користувачі; користувачі по групам; група користувачів; базова станція; район; кутова точка; точка з координатами.

На сервері необхідно використовувати захищену СУБД з відповідним рівнем захищеності і сертифікації, в якій має значення узгодження і цілісність даних. Узгодження даних забезпечується створенням таблиць, відповідних сутностей логічної моделі бази даних.

### 2.1.2 Пропозиції щодо реалізації захищеного каналу управління між контролером доступу і мобільним абонентським пристроєм

Відомо, що управління повинне мати властивості стійкості, безперервності, оперативності та скритності. Для забезпечення цих якостей канал управління повинен володіти додатковими механізмами захисту. Оскільки між контролером доступу і МАП можливий канал управління тільки через МСПД, то можливі наступні варіанти:

– VPN-з'єднання в БМПД, наприклад, на базі протоколу HTTPS;
– захищені SMS-повідомлення;
– VPN-з'єднання в складі інкапсульованих даних протоколів низьких рівнів (канального, мережевого, транспортного).

Варіант побудови захищеного каналу управління між контролером доступу МАП на прикладі протоколу HTTPS представлений на рис. 2.3.

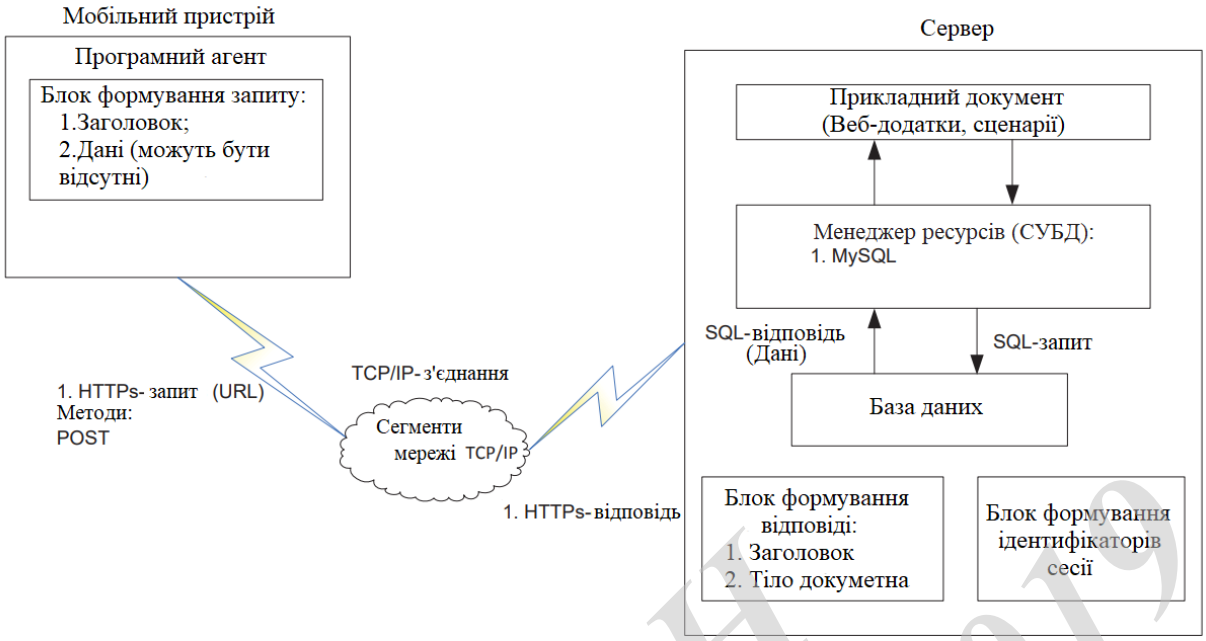
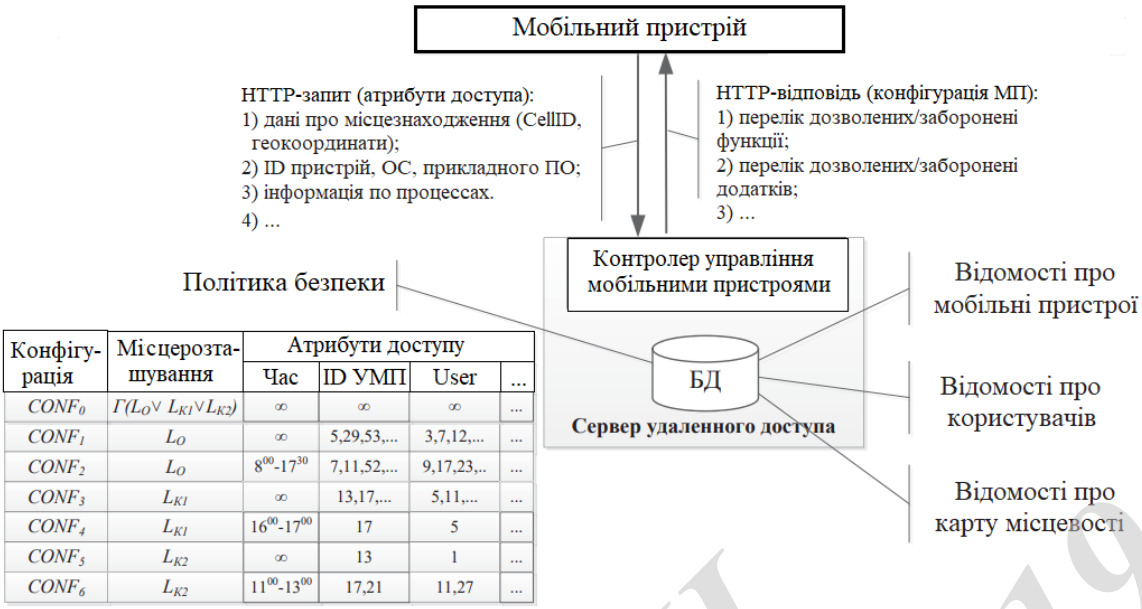



Рисунок 2.3 – Варіант побудови захищеного каналу управління на базі протоколу HTTPS

Розширена схема взаємодії МАП і контролера доступу представлена на прикладі протоколу HTTPS на рис. 2.4. Доцільно канал управління між мобільним пристроєм і віддаленим сервером доступу реалізувати захищеним з встановленням VPN-каналу. У разі якщо розголошення місця розташування користувача мобільного пристрою критично, можуть бути використані протоколи, які реалізують конфіденційні розподілені обчислення, такі як "Забудькувата передача" [36] або "Передача даних на зберігання" [39].

Необхідно відзначити, що реалізація захищеного каналу управління на базі протоколу прикладного рівня HTTPS має суттєві недоліки щодо стійкості, оперативності, скритності, надійності і захищенності. Одним з варіантів вирішення даної проблеми може бути використання можливостей протоколів низького рівня для реалізації такого захищеного каналу управління.




| Конфігу-рація | Місцерозта-шування | Атрибути доступу | | | |
|---|---|---|---|---|---|
| | | Час | ID УМП | User | ... |
| $CONF_0$ | $\Gamma(L_O \vee L_{K1} \vee L_{K2})$ | ∞ | ∞ | ∞ | ... |
| $CONF_1$ | $L_O$ | ∞ | 5,29,53,... | 3,7,12,... | ... |
| $CONF_2$ | $L_O$ | $8^{00}$-$17^{30}$ | 7,11,52,... | 9,17,23,.. | ... |
| $CONF_3$ | $L_{K1}$ | ∞ | 13,17,... | 5,11,... | ... |
| $CONF_4$ | $L_{K1}$ | $16^{00}$-$17^{00}$ | 17 | 5 | ... |
| $CONF_5$ | $L_{K2}$ | ∞ | 13 | 1 | ... |
| $CONF_6$ | $L_{K2}$ | $11^{00}$-$13^{00}$ | 17,21 | 11,27 | ... |

Рисунок 2.4 – Структурна схема, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв

На рис. 2.4 представлений варіант реалізації захищеного каналу управління в складі MAC-підрівня канального рівня стека протоколів.

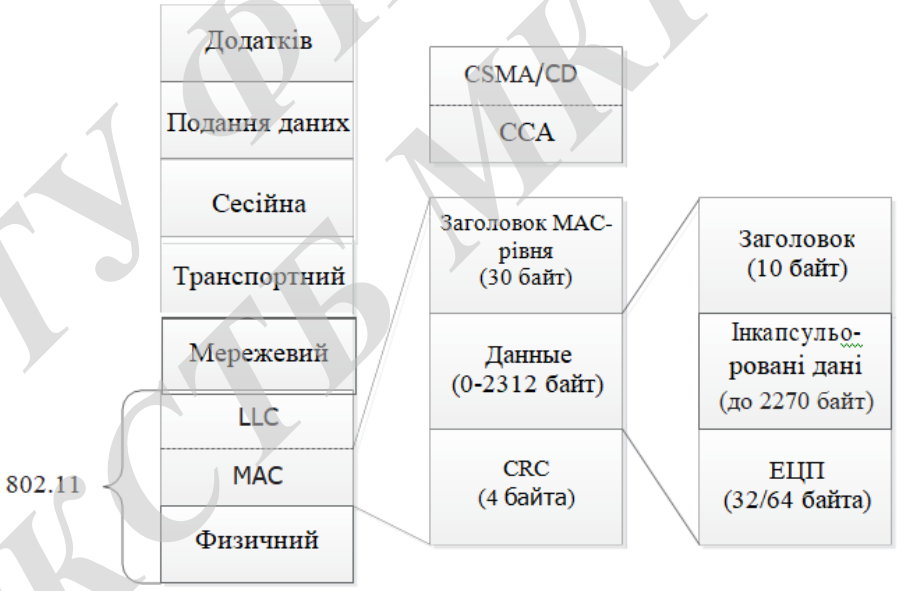



Рисунок 2.5 – Захищений канал керування МАП в складі інкапсульованих даних MAC-підрівня канального рівня 802.11

За рахунок використання інкапсульованих даних в складі пакету може передаватися зашифровані сигнали управління. Варіант побудови структури даних в складі пакету інкапсульованих даних представлений на рис. 2.6.

Обробка сигналів управління повинна бути покладена на програмно-апаратний модуль в складі АПМДЗ МАП або на елементи програмного коду

драйверів інтерфейсів бездротової передачі даних.

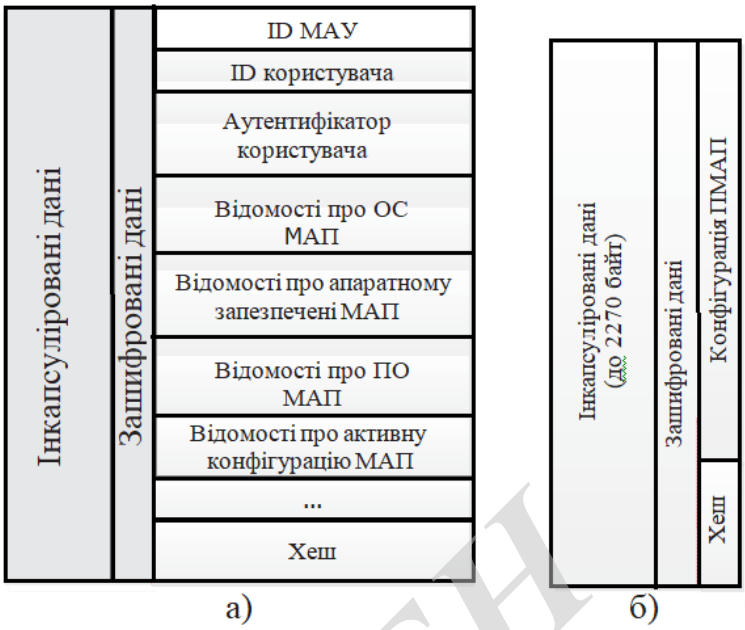



Рисунок 2.6 – Варіанти реалізації структури даних: а) при передачі атрибутів доступу контролера МАП; б) при передачі МАП керуючого впливу у вигляді конфігурації

2.2 Розробка рекомендацій з проектування підсистеми визначення місця розташування в системі управління безпекою мобільних абонентських пристроїв в корпоративних мережах з різними вимогами по захищеності

Ефективність підсистеми визначення місця розташування в системі управління безпекою мобільних абонентських пристроїв в корпоративних мережах з різними вимогами по захищеності визначається її параметрами, які повинні налаштовуватися в залежності від умов експлуатації. Для вибору оптимальних параметрів алгоритмів визначення місця розташування була проведена група експериментів, результати яких представлені в роботі [23]. Як інструмент дослідження в експериментах використовувалася розроблена імітаційна модель [24].

2.2.1 Рекомендації з оптимального взаємного розташування точок доступу бездротової мережі в системі визначення місця розташування

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

$$\begin{cases} e_L \to \min, \\ \text{var } AP_j = (x_j, y_j),\ j = \overline{1,\text{N}}_{\text{AP}} \\ \text{var } N_{AP} = 3..5, \end{cases} \quad (2.1)$$

де $e_L$ - помилка визначення місця розташування, $N_{AP}$ – кількість точок доступу з заданими координатами ($x_j$, $y_j$), j = $\overline{1, N}_{AP}$.

Результати експериментів для трьох точок доступу представлені в табл. 2.1, для чотирьох - в табл. 2.2 і для п'яти - в табл. 2.3.

Таблиця 2.1 – Статистичні параметри помилки позиціонування для різного розташуванням трьох точок доступу на мапі приміщень

| № карти розташування точок доступу | Вибіркове середнє, м | Вибіркове середньоквадратичне відхилення, м | Максимальне значення, м | Мінімальне значення, м | Довірчий інтервал для середнього |
|---|---|---|---|---|---|
| 1 | 7,533 | 4,063 | 23,669 | 0,069 | 0,101 |
| 2 | 8,877 | 5,11 | 30,573 | 0,036 | 0,133 |
| 3 | 4,984 | 10,378 | 52,716 | 0,212 | 0,284 |
| 4 | 5,45 | 3,759 | 56,847 | 0,068 | 0,098 |
| 5 | 5,924 | 4,623 | 25,037 | 0,055 | 0,125 |
| 6 | 5,297 | 3,456 | 22,087 | 0,097 | 0,094 |
| 7 | 5,883 | 4,379 | 26,92 | 0,026 | 0,119 |
| 8 | 7,705 | 4,712 | 25,493 | 0,079 | 0,125 |
| 9 | 6,484 | 3,766 | 27,166 | 0,078 | 0,102 |
| 10 | 6,088 | 4,387 | 32,627 | 0,115 | 0,12 |
| 11 | 5,561 | 4,221 | 28,042 | 0,031 | 0,115 |
| 12 | 9,538 | 3,66 | 29,606 | 0,047 | 0,096 |
| 13 | 9,547 | 4,471 | 29,685 | 0,115 | 0,119 |
| 14 | 15,548 | 7,393 | 39,889 | 1,616 | 0,198 |

а) б)

Рисунок 2.7 – Схема оптимального розташування трьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування: а) карта № 3, б) карта № 6

Таблиця 2.2 – Статистичні параметри помилки позиціонування для різного розташуванням чотирьох точок доступу на мапі приміщень

| № карти розташування точок доступу | Вибіркове середнє, м | Вибіркове середньоквадратичне відхилення, м | Максимальне значення, м | Мінімальне значення, м | Довірчий інтервал для середнього |
|---|---|---|---|---|---|
| 1 | 5,592 | 3,43 | 20,495 | 0,023 | 0,078 |
| 2 | 5,305 | 3,351 | 26,896 | 0,054 | 0,089 |
| 3 | 6,499 | 4,167 | 20,79 | 0,024 | 0,112 |
| 4 | 5,024 | 2,89 | 21,372 | 0,037 | 0,078 |
| 5 | 4,904 | 3,213 | 19,442 | 0,05 | 0,087 |
| 6 | 5,132 | 3,271 | 22,431 | 0,09 | 0,088 |
| 7 | 4,967 | 3,341 | 21,898 | 0,121 | 0,089 |
| 8 | 5,806 | 3,447 | 23,277 | 0,072 | 0,09 |
| 9 | 8,505 | 3,057 | 24,891 | 0,096 | 0,078 |
| 10 | 15,467 | 7,591 | 38,175 | 1,496 | 0,201 |
| 11 | 5,742 | 3,484 | 18,007 | 0,041 | 0,091 |

Для чотирьох точок доступу найкраща точність визначення місця розташування досягається при взаємному розташуванні точок доступу так, як показано на рис. 2.8.

а) б)

Рисунок 2.8 – Схема оптимального розташування чотирьох точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення місця розташування: а) карта № 5, б) карта № 7

Таблиця 2.3 – Статистичні параметри помилки позиціонування для різного розташуванням п'яти точок доступу на мапі приміщень

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

Для п'яти точок доступу найкраща точність визначення місця розташування досягається при взаємному розташуванні точок доступу так, як показано на рис. 2.9.

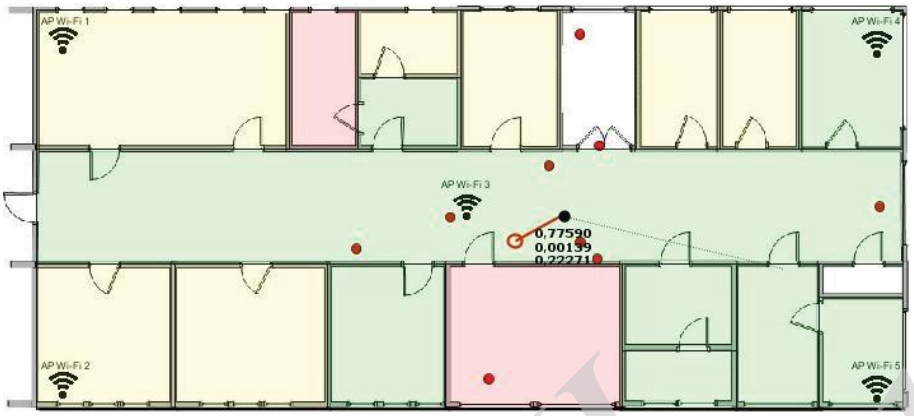



Рисунок 2.9 – Схема оптимального розташування п'яти точок доступу на досліджуваній схемі поверху з точки зору мінімальної помилки визначення

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

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

У табл. 2.4 представлені результати експериментів, в яких досліджувалась залежність точності визначення місця розташування для методу k - найближчих сусідів в залежності від числа $k$ .

Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10, \\ \operatorname{var}(x_i, y_i) \mid X^{N_{kNN}} = \left\langle \{(x_i, y_i), \upsilon_i\}, P_{r_i}^{RSS} \right\rangle, i = \overline{1, N_{kNN}}, \\ \operatorname{var} N_{kNN} \mid X^{N_{kNN}} = \left\langle \{(x_i, y_i), \upsilon_i\}, P_{r_i}^{RSS} \right\rangle, i = \overline{1, N_{kNN}}, \end{cases} \quad (2.2)$$

де $e_L$ - помилка визначення місця розташування, $(\tilde{x}, \tilde{y})$ - реальні координати місця розташування MAG; k - число "сусідів" в сигнальному просторі; $(x_i, y_i)$ - координати і -й точки карти сигнального простору; $\upsilon_i$ - кут

орієнтації в просторі МАП; $P_{r_i}^{RSS}$ - рівень потужності сигналу від МАП; i= $\overline{1, N}_{kNN}$ - індекс точки вимірювань карти сигнального простору, а $N_{kNN}$ - їх кількість.

Експерименти здійснювалися для п'яти точок доступу і карти приміщень, зображених на рис. 2.10.

Таблиця 4.4 – Статистичні параметри помилки позиціонування для методу k -ближніх сусідів в залежності від числа k

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

Як видно з таблиці найкраща точність визначення місцезнаходження досягалась при значеннях $k = 6$ і $k = 9$ .

На рис. 2.10 представлений графік залежності вибіркового середнього і середньоквадратичного відхилення (СКВ) для помилки визначення місцеположення від числа "сусідів".

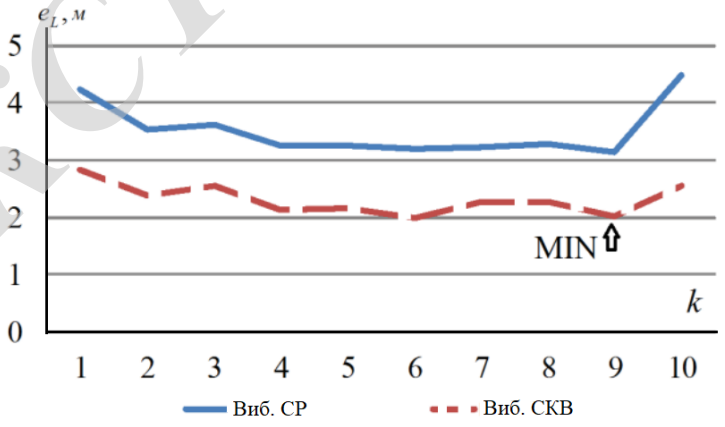



Рисунок 2.10 – Графік залежності вибіркового середнього і СКО для помилки визначення місця розташування від числа "сусідів"

Для значень числа врахованих найближчих "сусідів" $k = 6$ и $k = 9$ були проведені експерименти з метою дослідження впливу розташування точок вимірювань рівня сигналу на мапі сигнального простору. Розташування точок вимірювання в імітаційній моделі вибиралось в вигляді сітки квадратів або прямокутників, сторони яких визначаються кроком сітки по горизонталі и вертикалі. Наприклад, крок сітки карти сигнального простору $h$ = 1,5*x*1,5 означає ширину і довжину прямоугольника сітки, равні 1,5 м. В табл. 2.5 представлені результати данного експеримента.

Таблиця 2.5 – Статистичні параметри помилки позиціонування для методу k - ближніх сусідів в залежності від кроку сітки карти сигнального простору

| Крок сітки карти h, м | Вибіркове середнє, м | Вибіркове середньоквадратичне відхилення, м | Максимальне значення, м | Мінімальне значення, м | Довірчий інтервал для середнього |
|---|---|---|---|---|---|
| $k = 6$ | | | | | |
| 0,5x0,5 | 3,27 | 2,33 | 22,995 | 0,073 | 0,064 |
| 1x1 | 3,185 | 1,994 | 19,923 | 0,098 | 0,055 |
| 1,5x1,5 | 3,162 | 2,072 | 22,075 | 0,003 | 0,056 |
| 2x2 | 3,067 | 2,058 | 22,306 | 0,007 | 0,051 |
| 2,5x2,5 | 3,36 | 2,079 | 14,773 | 0,043 | 0,053 |
| 3x3 | 3,484 | 2,205 | 17,341 | 0,023 | 0,06 |
| $k = 9$ | | | | | |
| 0,5x0,5 | 3,18 | 2,021 | 18,224 | 0,035 | 0,037 |
| 1x1 | 3,147 | 2,028 | 19,336 | 0,009 | 0,054 |
| 1,5x1,5 | 2,603 | 1,702 | 21,212 | 0,023 | 0,046 |
| 2x2 | 3,104 | 2,181 | 22,769 | 0,034 | 0,06 |
| 2,5x2,5 | 3,291 | 1,894 | 14,394 | 0,072 | 0,049 |
| 3x3 | 4,472 | 2,393 | 14,033 | 0,067 | 0,065 |

Графік залежності статистичних параметрів помилки визначення місця розташування від кроку сітки вимірів карти сигнального простору представлений на рис. 2.11.

З таблиці і рисунка видно, що найкраща точність визначення місця розташування для методу k -бліжайших сусідів досягається при значеннях кроку сітки вимірів карти сигнального простору рівного h = 1,5x1,5 м і h= 2,0x2,0 м як при k = 6, так і k = 9.

Найкращі значення статистичних параметрів помилки визначення місця розташування в проведених експериментах були досягнуті при значеннях $k = 9$ и $h$ =1,5x1,5 м.

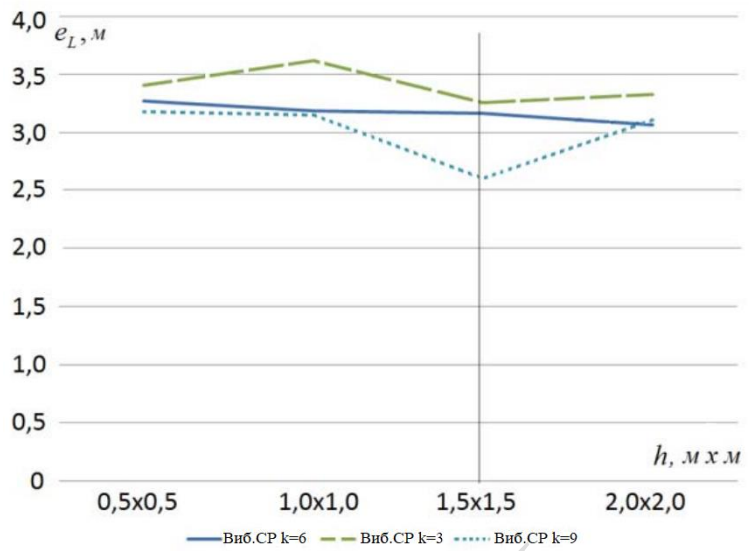



Рисунок 2.11 – Графік залежності помилки визначення місця розташування від кроку сітки вимірів карти сигнального простору

2.2.3 Рекомендації по значенням параметрів методу на основі байєсівського підходу в системі визначення місця розташування

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

– числа "сусідів" - кількості найбільш ймовірних станів, врахованих при обчисленні розташування;

– розташування точок вимірювань на карті сигнального простору;

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

Формальна постановка оптимізаційної задачі має вигляд:

$$\begin{cases} e_L \to \min, \\ \operatorname{var} k = 1..10, \\ \operatorname{var}(x_i, y_i) \mid X^{N_{HMM}} = \left\langle (x_i, y_i), P_{r_i}\left[\lambda_i / (x_i, y_i)\right]\right\rangle, i = \overline{1, N_{HMM}}, \\ \operatorname{var} N_{HMM} \mid X^{N_{HMM}} = \left\langle (x_i, y_i), P_{r_i}\left[\lambda_i / (x_i, y_i)\right]\right\rangle, i = \overline{1, N_{HMM}}, \end{cases} \quad (2.3)$$

де $e_L$ - помилка визначення місця розташування, $(\tilde{x}, \tilde{y})$ - реальні координати місця розташування МАП; k - число найбільш ймовірних станів; $(x_i, y_i)$ - координати і -й точки карти сигнального простору; $P_{r_i}\left[\lambda_i / (x_i, y_i)\right]$ - умовна ймовірність отримання вимірювань сигналу передавача МАП зі

статистичним розподілом $\lambda_i$ в точці з координатами $(x_i, y_i)$; $N_{НММ}$ - кількість точок сигнального простору навчальної вибірки.

У табл. 2.6 представлені результати експерименту, в якому досліджувалася залежність статистичних параметрів помилки визначення місця розташування від числа "сусідів" - кількості найбільш ймовірних станів, що враховуються при обчисленні розташування, на основі байєсівського підходу.

Таблиця 2.6 – Статистичні параметри помилки позиціонування для методу на основі байєсівського підходу в залежності від числа k

| Значення числа k | Вибіркове середнє, м | Вибіркове середньоквадратичне відхилення, м | Максимальне значення, м | Мінімальне значення, м | Довірчий інтервал для середнього |
|---|---|---|---|---|---|
| 1 | 3,86 | 2,309 | 16,367 | 0,124 | 0,063 |
| 2 | 3,376 | 2,076 | 13,538 | 0,082 | 0,056 |
| 3 | 2,445 | 1,448 | 9,764 | 0,024 | 0,039 |
| 4 | 2,512 | 1,616 | 11,514 | 0,07 | 0,043 |
| 5 | 2,466 | 1,705 | 11,458 | 0,033 | 0,042 |
| 6 | 2,689 | 1,769 | 12,948 | 0,039 | 0,047 |
| 7 | 2,641 | 1,84 | 11,8 | 0,018 | 0,05 |
| 8 | 3,195 | 2,084 | 10,996 | 0,034 | 0,056 |
| 9 | 2,62 | 1,809 | 11,17 | 0,02 | 0,041 |
| 10 | 2,651 | 1,812 | 11,246 | 0,01 | 0,049 |

Графік залежності статистичних параметрів помилки визначення місця розташування від числа "сусідів" - кількості найбільш ймовірних станів, що враховуються при обчисленні розташування, представлений на рис. 2.12.

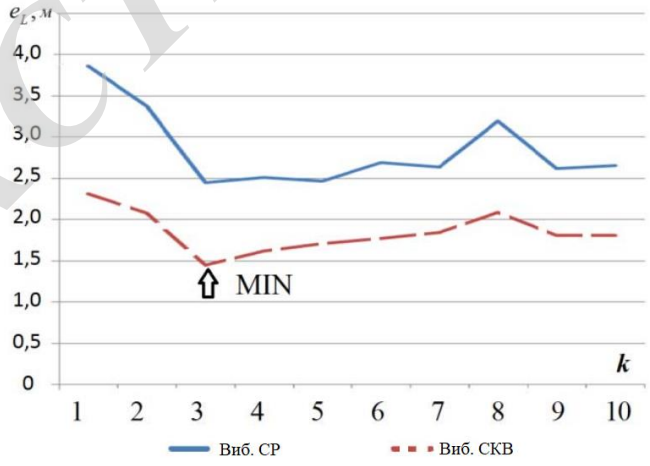



Рисунок 2.12 – Графік залежності вибіркового середнього і СКО для помилки визначення місця розташування від кількості найбільш ймовірних

станів

З таблиці і рисунка видно, що найкраща точність визначення місця розташування для байєсівського підходу досягається при значенні $k = 3$

У табл. 2.7 представлені результати експерименту, в якому досліджувалася залежність статистичних параметрів помилки визначення місця розташування від кроку сітки карти сигнального простору для методу на основі байєсівського підходу.

Графік залежності статистичних параметрів помилки визначення місця розташування від кроку сітки вимірів карти сигнального простору представлений на рис. 2.13.

Таблиця 2.7 - Статистичні параметри помилки позиціонування для методу на основі байєсівського підходу в залежності від кроку сітки карти сигнального простору

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

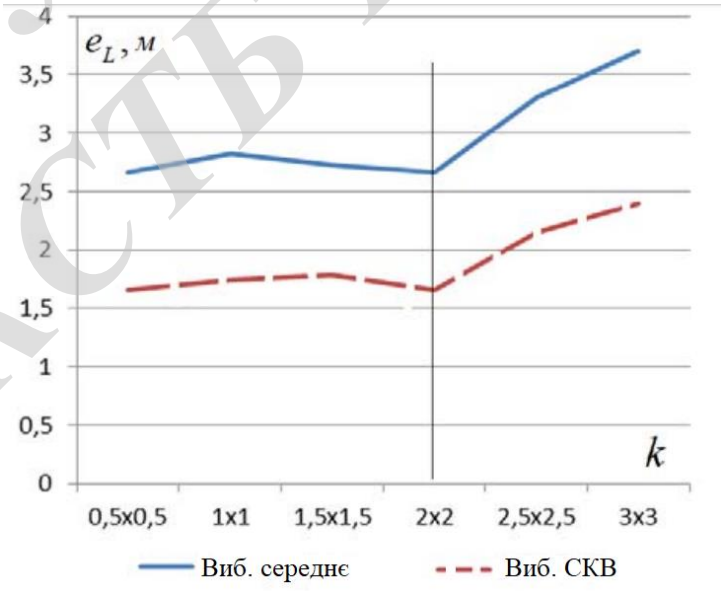



Рисунок 2.13 – Графік залежності вибіркового середнього і СКО для помилки визначення місця розташування від кроку сітки вимірів карти

сигнального простору

З таблиці і рисунка видно, що найкраща точність визначення місця розташування для методу на основі байєсівського підходу досягається при значеннях кроку сітки вимірів карти сигнального простору h = 1,5x1,5 м і h = 2,0x2,0 м

Таким чином, результати для даного методу збігаються з аналогічним експериментом для методу k -ближніх сусідів.

У табл. 2.8 і на рис. 2.14 представлені результати експерименту, вкотором досліджувалася залежність статистичних параметрів помилки визначення місця розташування від кількості вимірювань M в кожній точці карти вимірювань при формуванні статистики розподілу ймовірностей рівнів потужності сигналу МАПУ для методу на основі байєсівського підходу.

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

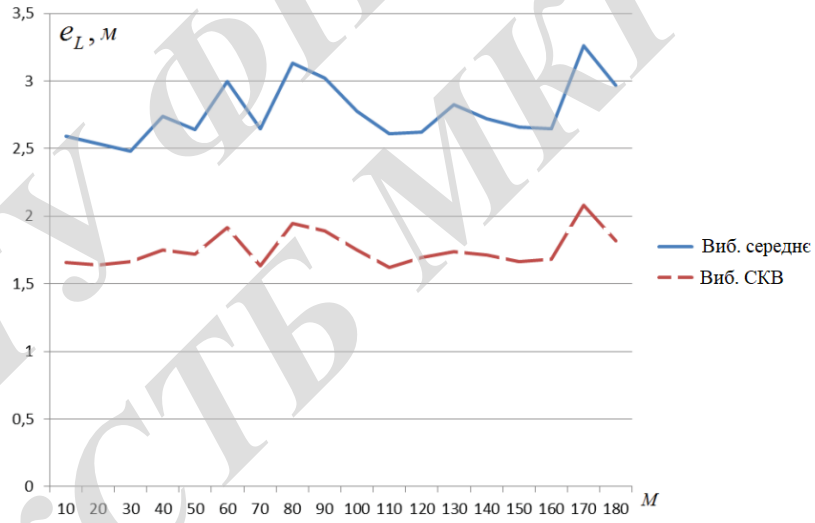



Рисунок 2.14 – Графік залежності помилки визначення місця розташування від кількості вимірювань в кожній точці карти вимірювань при формуванні статистики розподілу ймовірностей рівнів потужності сигналу МАП

Таблиця 4.8 – Статистичні параметри помилки позиціонування для методу на основі байєсівського підходу в залежності від кількості вимірювань М в кожній точці карти вимірювань

| кількість вимірювань М | Вибіркове середнє, м. | Вибіркове середньоквадратичне відхилення, м. | Максимальне значення, м. | Мінімальне значення, м. | Довірчий інтервал для середнього |
|---|---|---|---|---|---|
| 10 | 2,59 | 1,66 | 10,855 | 0,031 | 0,045 |
| 20 | 2,537 | 1,638 | 12,393 | 0,012 | 0,044 |
| 30 | 2,481 | 1,661 | 12,596 | 0,025 | 0,045 |
| 40 | 2,739 | 1,751 | 11,709 | 0,019 | 0,047 |
| 50 | 2,642 | 1,72 | 11,966 | 0,063 | 0,045 |
| 60 | 2,997 | 1,913 | 13,744 | 0,053 | 0,052 |
| 70 | 2,649 | 1,632 | 11,509 | 0,026 | 0,044 |
| 80 | 3,131 | 1,949 | 12,307 | 0,048 | 0,052 |
| 90 | 3,023 | 1,893 | 12,842 | 0,031 | 0,051 |
| 100 | 2,778 | 1,75 | 11,938 | 0,051 | 0,048 |
| 110 | 2,61 | 1,618 | 12,347 | 0,005 | 0,043 |
| 120 | 2,623 | 1,695 | 11,726 | 0,022 | 0,046 |
| 130 | 2,822 | 1,74 | 12,191 | 0,038 | 0,047 |
| 140 | 2,722 | 1,712 | 12,316 | 0,055 | 0,046 |

# 3 ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ АБОНЕНТСЬКИХ ПРИСТРОЇВ В КОРПОРАТИВНИХ МЕРЕЖАХ

Для вироблення пропозицій щодо застосування розробленої системи управління безпекою МАП необхідно провести розрахунок оцінок окремих показників ефективності, що характеризують процес функціонування даної системи. Однією з ключових підсистем в роботі системи управління безпекою МАП є підсистема визначення місця розташування, реалізованна з використанням технологій на базі методів трилатерації, k - найближчих сусідів і байєсівського підходу, а також запропонованого підходу щодо підвищення достовірності визначення місця розташування МАП.

## 3.1 Розрахунок оцінки часу, необхідного для зміни конфігурації мобільного абонентського пристрою

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

Процес зміни конфігурації МАП здійснюється в кілька етапів:

1. Вимірювання рівня сигналу МАП на точках доступу бездротової мережі передачі даних ($T_{RSS}$).

2. Позиціонування МАП ($T_{LOC}$).

3. Відправка атрибутів доступу (запиту на доступ до послуг) з МАП ($T_{REQ}$).

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

5. Формування та відправка керуючої команди на зміну конфігурації МАП ($T_{RESP}$).

6. Прийом і обробка керуючої команди на стороні МАП, застосування нової конфігурації ($T_{CONF}$).

Таким чином, оцінка загального часу, необхідного для зміни конфігурації МАП, може бути представлена у вигляді

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF}. \quad (3.1)$$

Розрахунок часу, необхідного на кожному етапі, здійснимо для найбільш поширеного стандарту бездротової передачі даних - IEEE 802.11 [37] при наступних обмеженнях і припущеннях:

– доступ до бездротової мережі передачі даних встановлено, мобільний пристрій пройшло аутентифікацію і знаходиться в зоні дії довіреної бездротової мережі передачі даних;

– розрахунок часових параметрів проводиться на найгірший випадок.

В відповідність зі стандартом IEEE 802.11 передача пакета даних на канальному рівні, що володіє ідентифікаційної інформацією про передавачі здійснюється в 4 етапи. Дані етапи представлені на рис. 3.1.

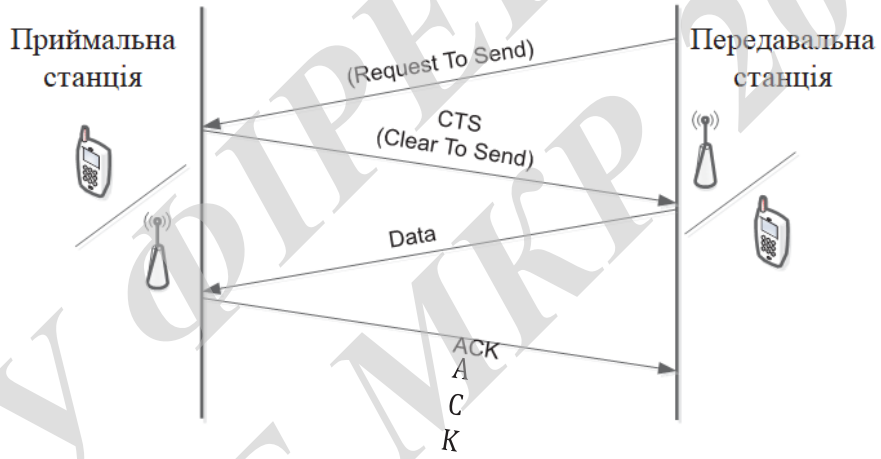



Рисунок 3.1 – Чотирьох етапний протокол передачі даних, який реалізує метод колективного доступу до середовища з мінімізацією ймовірності виникнення зіткнень

У стандарті IEEE 802.11 використовується метод колективного доступу з виявленням несучої і униканням колізій (Carrier Sense Multiple Access/Colli- sion Avoidance, CSMA / CA). Перед початком передачі даних здійснюється вибір вільного каналу на основі алгоритму оцінки чистоти каналу (Channel Clearance Algorithm, CCA). В основі даного алгоритму лежить вимір енергії сигналу на антені і потужності прийнятого сигналу (Received Signal Strength Indicator, RSSI). Якщо потужність прийнятого сигналу нижче заданого порогу, то канал оголошується вільним і MAC-рівень отримує статус CTS (Clear To Send).

Перед початком передачі даних, МАП відправляє повідомлення RTS

(Ready To Send), що містить інформацію про готовність відправки даних, адресата і тривалості передачі. Якщо приймальна станція (точка доступу) відповідає посилкою сигналу CTS, то МАП починає передачу даних. По завершенні передачі даних точка доступу повертає кадр ACK, підтверджує безпомилковий прийом.

Максимальна дальність дії бездротової мережі визначається множиною параметрів і в першу чергу потужністю передавача, чутливістю приймача і 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 буде здійснюватися за час, що визначається:

$$t_{data} \approx \frac{4 \cdot l}{c} = \frac{4 \cdot 100}{299792458} = 1.334256 \cdot 10^{-6} c. \qquad (3.2)$$

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

Виходячи з тих же 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 і запитуваної послуги, а у відповіді на запит - інформація про призначення конфігурації, то розмір переданих даних може перевищувати максимальний розмір пакету, тому для значень $T_{REQ}$ і $T_{RESP}$ передбачимо 10-кратне перевищення максимального розміру пакета. Тоді з урахуванням (3.2) отримаємо:

$$T_{REQ} \approx T_{RESQ} \approx 10 \cdot t_{data} = 1.334256 \cdot 10^{-5} c. \qquad (3.3)$$

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

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

В процесі імітаційного моделювання та функціонування розроблених

програм для ЕОМ [31] були отримані наступні результати: $T_{LOC} \approx 2{,}92 \cdot 10^{-3}$ с, $T_{POLICY} \approx 0{,}71 \cdot 10^{-3}$ с, $T_{CONF} \approx 1{,}12 \cdot 10^{-3}$ с.

Виходячи з отриманих оцінок часу виконання процедур і вирази (3.1) отримаємо оцінку значення часу, необхідного для зміни конфігурації мобільного пристрою:

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \approx$$
$$\approx 0.001334256 \cdot 10^{-3} + 0.01334256 \cdot\cdot 10^{-3} + 0.71 \cdot 10^{-3} +$$
$$+ 0.01334256 \cdot 10^{-3} + 1.12 \cdot 10^{-3} = 4.778019376 \cdot 10^{-3} c \approx 4.778 мс$$

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

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

Для оцінювання залежності часу переконфіграції МАП від числа випробувань в методі Монте-Карло був проведений експеримент, результати якого представлені на рис. 3.2.

З аналізу даних експерименту видно, що для поточних умов при числі випробувань в чисельному методі Монте-Карло M < 5000 Час переконфігурації МАП знаходиться в межах допустимих значень. Також з аналізу графіка видно, що залежність має ростом складності. Даний факт висуває підвищені вимоги до продуктивності обладнання системи управління доступом і умов її експлуатування.

На підставі отриманих значень може бути отримана оцінка ймовірності збереження конфіденційності інформації при доступі до послуг мереж з різними вимогами по захищеності згідно з прийнятою системою показників ефективності.

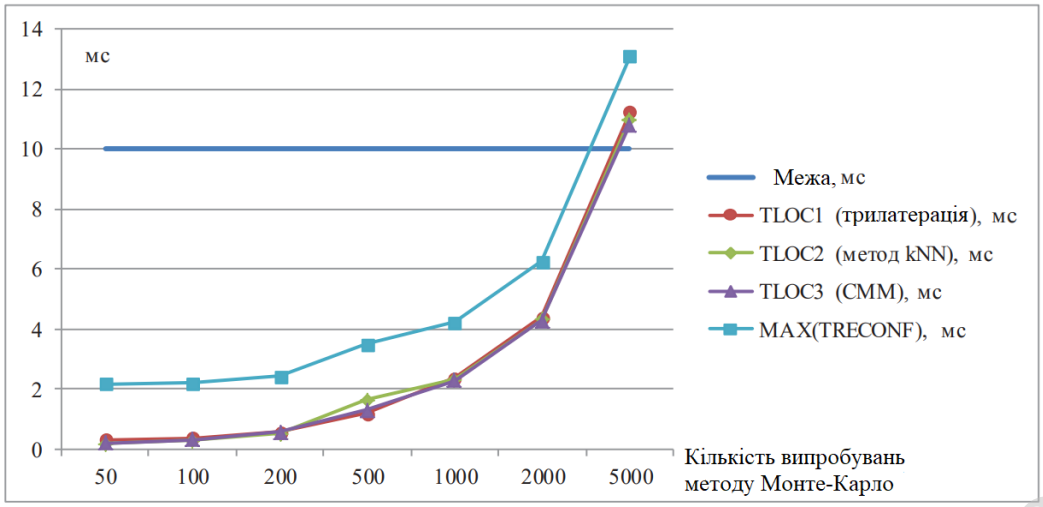



Рисунок 3.2 - Графік залежності часу переконфігурації МАП від числа випробувань в методі Монте-Карло

Імовірність збереження конфіденційності інформації запропоновано оцінювати за допомогою формули (1.10), при цьому прийнято, що ймовірність подолання системи захисту $P_{Пр3} \rightarrow 0$. Таким чином, за умови $CONF \subset CONF^{доп}$, прийнятих обмеженнях і припущеннях ($P_{Пр3} \rightarrow 0$), а також отриманої оцінки часу переконфігурації $T_{RECONF} = 4{,}778 \cdot 10^{-3}$ с, що знаходиться в межах заданих замовником значень $T_{RECONF}^{доп} = 10^{-2}$ с, можна зробити висновок про те, що $P_{СК}(T_{RECONF}) \rightarrow 1$.

3.2 Розрахунок ймовірності загрози порушення конфіденційності інформації за рахунок формування некоректної конфігурації мобільного абонентського пристрою

Формування некоректної конфігурації і, відповідно, профілю захисту МАП можливо внаслідок неправильних налаштувань політики безпеки, а також неточного визначення рівня захищеності приміщення, в якому знаходиться користувач МАП - виникненні помилок 2-го роду. Перший випадок неправильні налаштування політики безпеки виноситься за рамки розгляду даної роботи, тому для обчислення оцінки ймовірності витоку інформації за рахунок некоректної конфігурації і профілю захисту МАП буде використовуватися значення помилки 2-го роду при визначення рівня захищеності приміщення, в якому знаходиться користувач МАП.

Результати дослідження ефективності визначення рівня захищеності приміщення чисельним методом Монте-Карло при використанні різних технологій визначення місця розташування представлені в табл. 2.9. У

таблиці: П - прототип, С - розроблена система.

Результати отримані при оптимальних параметрах підсистеми визначення місцеположення МАП, виявлені в процесі попереднього імітаційного моделювання.

Як видно з аналізу таблиці, незалежно від технології визначення місця розташування оцінка ефективності визначення рівня захищеності у вигляді помилки 2-го роду не перевищує 1% при заданому критерії прийняття рішення. Однак при цьому критерії високі значення має помилка 1-го роду.

Графічна ілюстрація результатів імітаційного моделювання представлена на рис. 3.2.

Таблиця 3.1 - Результати дослідження ефективності визначення рівня захищеності чисельним методом Монте-Карло при використанні різних технологій визначення місця розташування і їх комбінацій

| № п/п | Метод | Правильно | | Помилка 1-го роду | | Помилка 2-го роду | |
|---|---|---|---|---|---|---|---|
| | | П | С | П | С | П | С |
| 1. | Трилатерація | 72,104 | 16,779 | 5,325 | 81,614 | 22,569 | 0,906 |
| 2. | k-ближніх сусідів | 76,881 | 14,333 | 9,247 | 84,447 | 13,871 | 0,919 |
| 3. | Байєсівський підхід | 75,572 | 11,153 | 17,726 | 87,786 | 6,700 | 0,906 |
| 4. | 1,2 | 71,934 | 6,255 | 8,982 | 93,225 | 19,083 | 0,519 |
| 5. | 1,3 | 72,069 | 8,349 | 9,615 | 90,997 | 18,314 | 0,653 |
| 6. | 2,3 | 75,728 | 15,055 | 10,44 | 82,88 | 13,831 | 2,064 |
| 7. | 1,2,3 | 76,327 | 8,727 | 7,938 | 90,235 | 15,786 | 1,037 |

З аналізу табл. 3.1 і результатів імітаційного моделювання на рис. 3.3 видно, що оцінка ймовірності витоку інформації за рахунок формування некоректної конфігурації мобільних пристроїв $P(CONF \subset CONF^{доп}) = P\left[ P_{\beta}(L_{Room} > L_{Room}) \le P_{\beta}^{доп} \right]$ при $P_{\beta}^{доп} = 0{,}01$ знаходиться в межах допустимих значень.

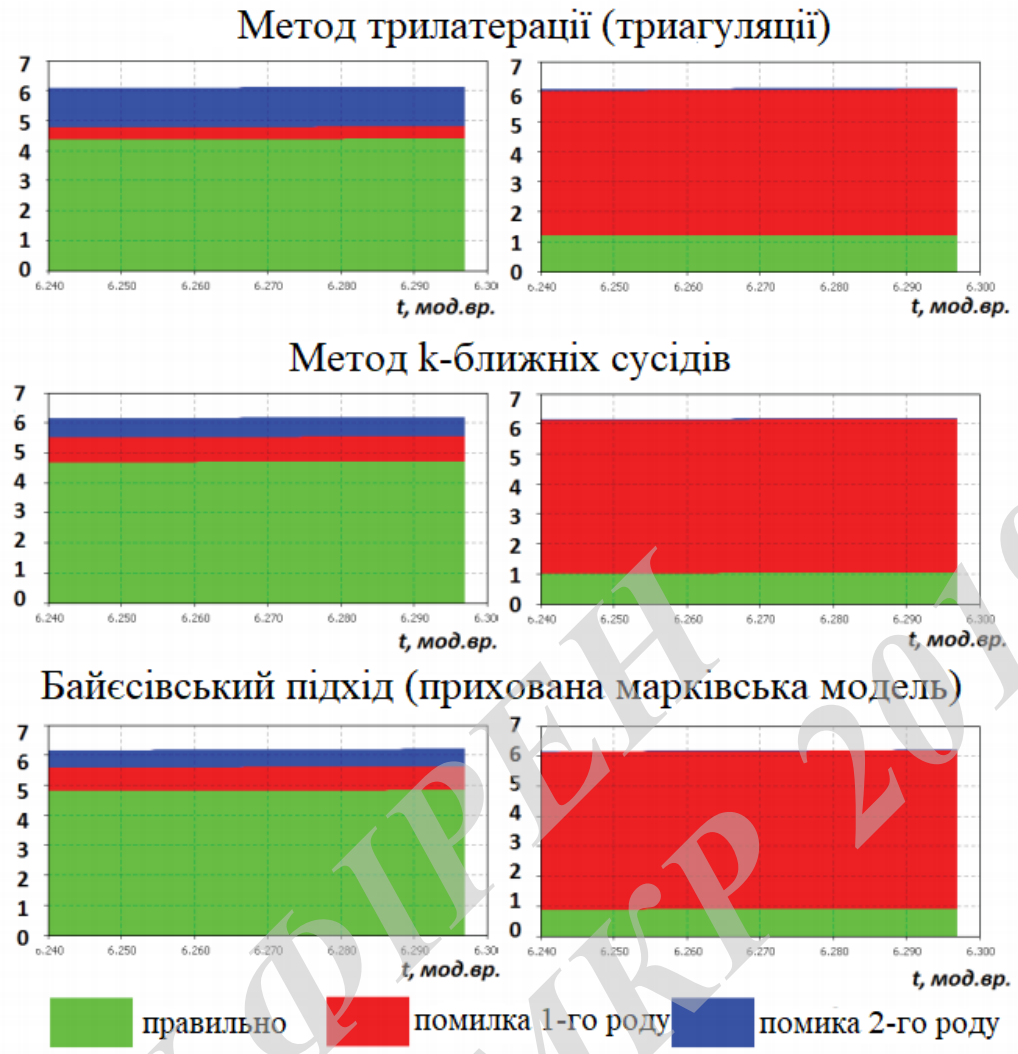



Рисунок 3.3 - Результати імітаційного моделювання дослідження ефективності визначення рівня захищеності приміщення чисельним методом Монте-Карло

3.3 Розрахунок ресурсоємності технічних рішень з надання послуг для прототипу і запропонованої системи управління безпекою мобільних абонентських пристроїв

Ресурсомісткість процесу захисту інформації [7] при експлуатації МАП може бути визначена, виходячи з виразу:

$$RES_{ЗІМАП} = K_{BOP} \cdot B_{OP} + K_{BTP} \cdot B_{TP} + K_{BCУ} \cdot B_{CУ} + K_{BCBM} \cdot \\ \cdot B_{CBM} + \left( \sum_{i=1}^{N_{МАП}} B_{МАП_i} \right) \cdot N_{Кор}, \quad (3.4)$$

де $K_{BOP}$ - коефіцієнт використання обчислювальних ресурсів; $B_{OP}$ -

вартість обчислювальних ресурсів; $K_{BTP}$ - коефіцієнт використання телекомунікаційних ресурсів; $B_{TP}$ - вартість телекомунікаційних ресурсів; $K_{BCУ}$ - коефіцієнт використання системи управління безпекою МАП; $B_{CУ}$ - вартість системи управління безпекою МАП; $K_{BCBM}$ - коефіцієнт використання системи визначення місця розташування МАП; $B_{CBM}$ - вартість системи визначення місця розташування МАП; $B_{МАП_i}$ - вартість і - го МАП, необхідного для доступу до послуг; $N_{МАП}$ - кількістю МАП, необхідних для доступу до всього переліку послуг; $N_{Кор}$ - кількість користувачів МАП.

Аналіз відкритих джерел інформації і середньої вартості захищених мобільних технічних рішень, а також середня вартість проектування і розгортання захищеної БСПД і серверної складової, яка виконує функції ЦУІБ, дозволив виявити залежність між витратами і кількістю користувачів МАП для прототипу і розробленої системи управління безпекою МАП. Графік цієї залежності представлений на рис. 3.4.

Аналіз рис. 3.4 показує, що спочатку ресурсомісткість пропонованого технічного рішення перевищує аналогічний показник для прототипу на величину витрат на систему управління і систему позиціонування $K_{BCУ} \cdot B_{CУ} + K_{BCBM} \cdot B_{CBM}$, при цьому вартість керованого МАП також не дозволяє отримати економічний ефект незалежно від кількості користувачів МАП.

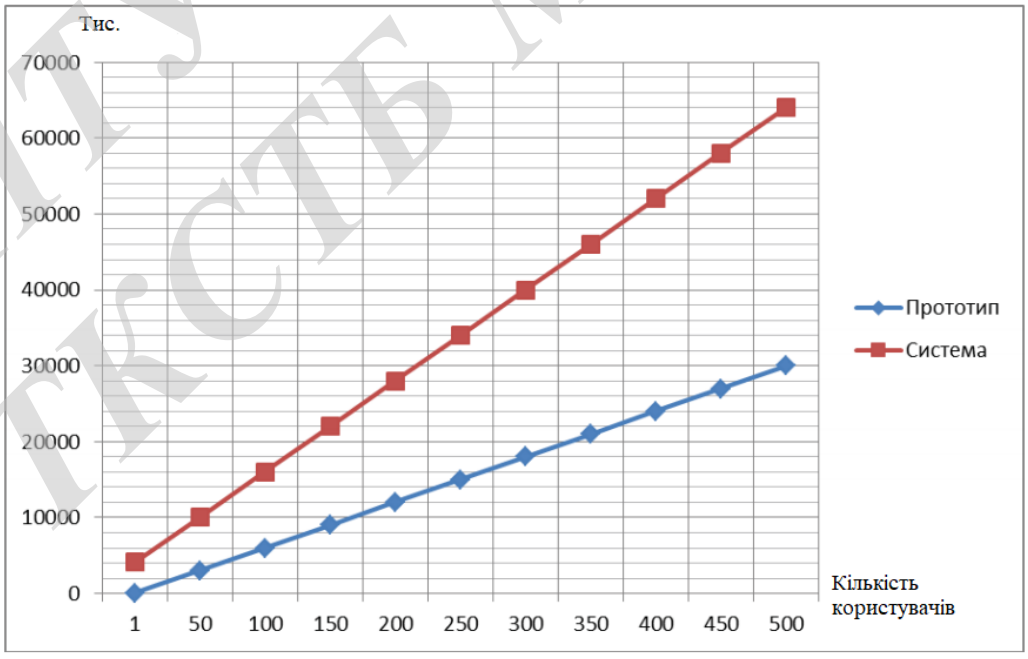



Рисунок 3.4 - Графік залежності ресурсоємності технічних рішень з надання послуг для прототипу і запропонованої системи управління безпекою МАП від кількості користувачів МАП

3.4 Розрахунок своєчасності доступу до послуг та інформації з використанням мобільних абонентських пристроїв

Своєчасність обробки запитів на доступ до послуг оцінювалася відповідно до стандарту. Імовірність надання інформації або послуг $P_{ДІ}$ ($T_{ДІ}$) за заданий час $T_{ДІ}^{зад}$ буде визначатися за допомогою табульованих неповних гамма-функцій [38]:

$$P_{ДІ}^{У}(T_{ДІ}) = \int_0^{\theta} \exp(-\tau)\cdot\tau^{\gamma} d\tau / \Gamma(\gamma), \qquad (3.5)$$

де $\Gamma(\gamma) = \int_0^{\theta} \exp(-\tau)\cdot\tau^{\gamma} d\tau$ - гама функція, $\gamma = \frac{T_{повн}}{\sqrt{T_2 - T_{повн}^2}}$, $\theta = T_{ДІ}^{зад}\cdot\frac{\gamma^2}{T_{повн}}$,

$T_{повн}, T_2$ - розраховуються відповідно середній час і 2-й момент часу реакції системи при обробці запитів системі (повного часу перебування на обробці з урахуванням очікування в черзі), $T_{ДІ}^{зад}$ - заданий час (гранично допустимий) для обробки запиту на доступ до інформації (послуг).

У відповідність з виразом (2.4) розраховане часом, що вимагається для переконфігурації МАП становить $T_{RECONF}$ = 4,778019376 • $10^{-3}$ с. Відповідне йому значення ймовірності своєчасності обробки запиту, отримане за допомогою табульованих неповної гамма-функції дорівнює:

$$P_{ДІ}^{У}(T_{ДІ}) = \Gamma(\gamma) = \Gamma\left(\frac{T_{RECONF}}{\sqrt{D[T_{RECONF}] + T_{RECONF}^2}}\right) = \Gamma(1.033804) = 0.9983.$$

Таким чином, при однакових умовах отримання доступу до послуг для розроблюваної системи та її прототипу в умовах, МАП в розроблюваної системі необхідно здійснити реконфігурацію, додатково витративши на це час, що дорівнює $T_{RECONF}$ = 4,778019376 • $10^{-3}$ с.

3.5 Оцінка ступеня досягнення мети дослідження МКР

Метою дослідження МКР є підвищення ймовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації в корпоративних мережах з різними вимогами по захисту пра щенности при використанні єдиного МАП. Результативність процесу [25] оцінюється за допомогою ймовірності забезпечення безпеки інформації при доступі до

послуг з використанням МАП відповідно до виразу (1.4). використовуючи вирази (1.4), (1.5), (1.7) - (1.11) і прийнятні обмеження і припущення ($P_{ЦІ} \to 1$, $P_{Прз} \to 0$, $P_{СК}$ ($T_{RECONF}$) $\to$ 1), отримаємо підсумковий вираз для оцінювання результативності процесу захисту інформації при експлуатації МАП :

$$P_{БІ}(T) = \left(1 - P\left[\beta\left(L^{\%}_{Room} > L_{Room}\right) \le \beta^{дод}\right]\right) \cdot \frac{N_{ДП}}{N_{П}} \cdot P^{У}_{ДІ}(T_{ДІ}). \qquad (3.6)$$

Значення ймовірності правильної переконфігурації керованого МАП $P(CONF \subset CONF^{дод}) = P\left[P_{\beta}(L^{\%}_{Room} > L_{Room}) \le P^{дод}_{\beta}\right]$ представлені в таблиці 3.1. Для системи-прототипу даний показник дорівнює одиниці, оскільки МАП системи прототипу некеровані. Порівняльний аналіз кількості доступних послуг для МАП розроблюваної системи і прототипу представлений на рис. 1.2. На підставі представлених даних отримана оцінка ступеня досягнення мети дослідження, представлена на рис. 3.5.

Як прототип оцінювалася система доступу до послуг, заснована на типових захищених МАП з кількістю послуг, що надаються, рівним 5, і системою з організаційно-технічним заходів щодо захисту інформації, що забезпечують вимоги щодо інформаційної безпеки.

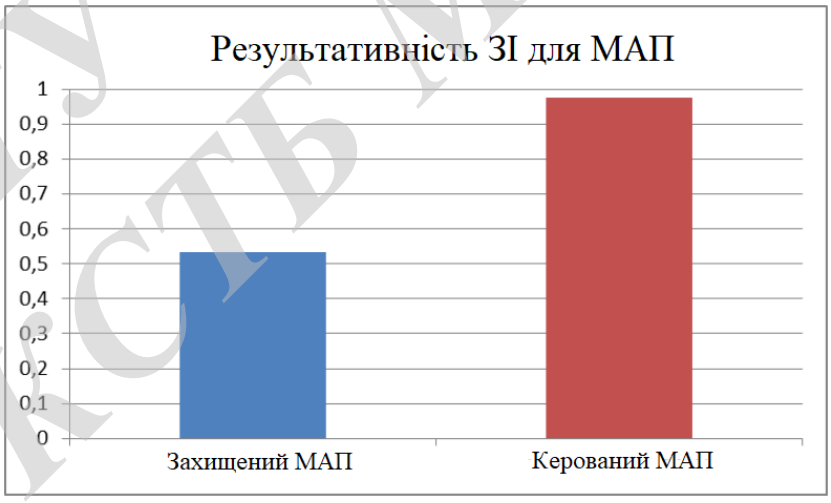



Рисунок 3.5 - Оцінка ступеня досягнення результатів дослідження МКР

Отриманий ефект (нормований на логарифмічною шкалою) при впровадженні розробленої системи управління МАП з урахуванням виразів (1.3), (1.13), (4.8) може бути оцінений як

$$E = \frac{\left|\lg\left(\frac{REZ}{RES}\right)\right|}{\max\left[\left|\lg\left(\frac{REZ}{RES}\right)\right|\right]}. \quad (3.7)$$

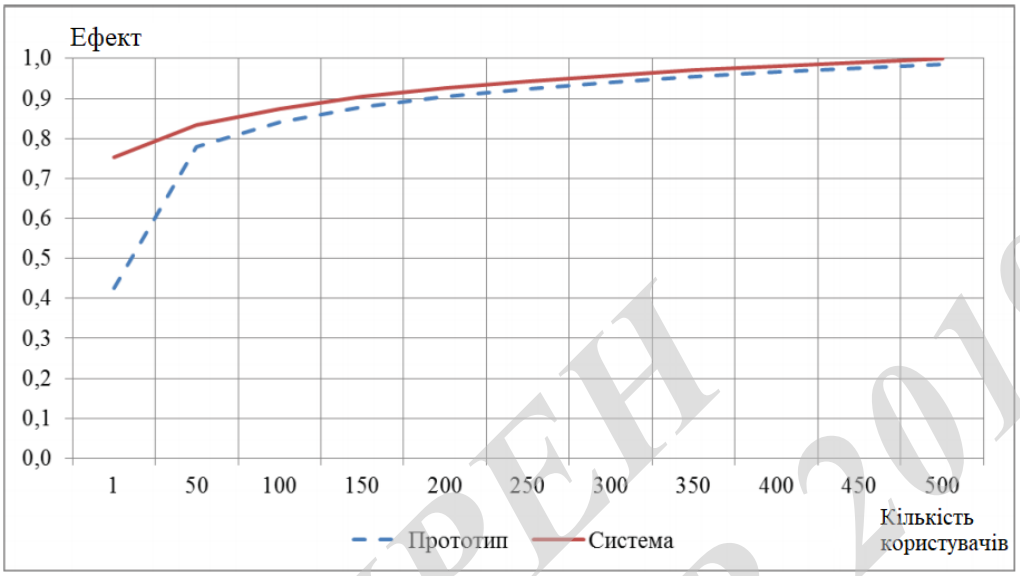



Рисунок 3.7 - Порівняльний аналіз одержуваного ефекту для прототипу і розробленої системи

Таблиця 3.2 - Розрахунок чисельних значень ефектів від впровадження розробленої системи управління безпекою МАП і керованих МАП в порівнянні з прототипом і в залежності від кількості користувачів МАП (П - прототип, С - розроблена система)

| Кількість користувачів | | 1 | 100 | 200 | 300 | 400 | 500 |
|---|---|---|---|---|---|---|---|
| Загальна вартість, тис. грн. | П | 60 | 6000 | 12000 | 18000 | 24000 | 30000 |
| | С | 4120 | 16000 | 28000 | 40000 | 52000 | 64000 |
| Ефект | П | 0,00887 | 0,00009 | 0,00004 | 0,00003 | 0,00002 | 0,00002 |
| | С | 0,00024 | 0,00006 | 0,00003 | 0,00002 | 0,00002 | 0,00002 |
| Ефект на лог-шкалі | П | -2,052 | -4,052 | -4,353 | -4,529 | -4,654 | -4,751 |
| | С | -3,625 | -4,214 | -4,457 | -4,612 | -4,726 | -4,816 |
| Нормований ефект на лог-шкалі | П | 0,426 | 0,841 | 0,904 | 0,940 | 0,966 | 0,986 |
| | С | 0,753 | 0,875 | 0,925 | 0,958 | 0,981 | 1,000 |

Чисельні значення ресурсоємності RES представлені на рисунку 3.6. З урахуванням виразу (3.7) і даних про чисельні значень, а також в залежності від кількість користувачів МАП були отримані оцінки одержуваного ефекту від впровадження розробленої системи управління безпекою МАП і керованих МАП в порівнянні з застосовуваним в даний час прототипом. Порівняльний аналіз отриманих ефектів представлений на рис. 3.7. Чисельні значення представлені в табл. 3.2.

Аналіз рис. 3.7 показує, що отриманий ефект для розробленої системи вище, ніж для використовуваного в даний час прототипу. При цьому необхідно зазначити, що істотний внесок в отриманий ефект вносить підвищення числа доступних користувачеві МАП послуг.

## 3.6 Висновки по 3 розділу

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

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

1) метод трилатерації:

– кількість точок доступу - 5;

– оптимальне розташування точок доступу показано на рис. 2.3;

2) метод k -ближній сусідів:

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

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

– кількість точок доступу - 5;

– оптимальне розташування точок доступу показано на рис. 2.3;

3) метод на основі байєсівського підходу:

– число врахованих найближчих «сусідів» k = 3;

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

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

– кількість точок доступу - 5;

– розташування точок доступу оптимально для карти, зображено на рис. 2.3.

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

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

– кількість випробувань M = 1000;

– емпіричний закон розподілу ймовірностей.

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

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

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

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

# 4 ЕКОНОМІЧНИЙ РОЗДІЛ

## 4.1 Технологічний аудит результатів проведених наукових досліджень

У попередніх розділах цієї магістерської кваліфікаційної роботи було зазначено, що стрімкий розвиток сучасних багатофункціональних мобільних абонентських пристроїв та інформаційних технологій призводить до постійного зростання потреб користувачів в доступі до інформації незалежно від того, де вони перебувають. До таких мереж відносяться інформаційні системи загального користування, інформаційні системи, які обробляють персональні дані, а також геоінформаційні системи.

При цьому віддалений доступ до корпоративних мереж з використанням мобільних абонентських пристроїв передбачає застосування відповідних систем захисту, що дозволяє забезпечити необхідний рівень забезпечення безпеки інформації незалежно від рівня захищеності сегмента захищеної корпоративної мережі.

Разом з тим, загальновідомо, що використання сучасних мобільних абонентських пристроїв зі значними обчислювальними і комунікаційними ресурсами має певні обмеження у зв'язку з низкою суттєвих особливостей, які стосуються їх експлуатації: розмірами, мобільністю користувачів, багатофункціональністю тощо.

Перспективним напрямом удосконалення сучасних корпоративних мереж є забезпечення надання захищеного доступу абонентам до інформації та послуг з різними вимогами по захисту при використанні єдиного мобільного абонентського пристрою.

Разом з тим, існуючі технічні рішення, що дозволяють управляти функціональністю (конфігурацією) мобільних абонентських пристроїв, не передбачають визначення ймовірності знаходження користувача мобільного абонентського пристрою в спеціальних приміщеннях, до яких пред'являють підвищені вимоги щодо забезпечення інформаційної безпеки в корпоративній мережі.

Тому наразі продовжуються активні дослідження моделей забезпечення безпеки управління функціональністю (конфігурацією) мобільних абонентських пристроїв як у вітчизняній, так і закордонній літературі.

Не є винятком і виконана нами магістерська кваліфікаційна робота, в якій було поставлено задачу підвищити ймовірність забезпечення безпеки інформації при використанні мобільних абонентських пристроїв і

гарантувати безпечний доступ до послуг корпоративних мереж з різними вимогами по захищеності.

Для цього нами було розроблено модель і алгоритм управління безпекою мобільних абонентських пристроїв, що дозволяє підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного мобільного абонентського пристрою, а також було зроблено науково-технічні пропозиції по реалізації системи управління безпекою мобільних абонентських пристроїв в корпоративних мережах з різними вимогами по захищеності.

Для встановлення рівня комерційного потенціалу результатів проведених нами досліджень проведемо їх технологічний аудит.

Для цього запросимо 3-х фахівців-експертів, що займаються цієї проблематикою: кандидатів технічних наук, доцентів Городецьку О.М., Михалевського Д. В. та Васильківського М.В.

Технологічний аудит запрошені експерти здійснювали за критеріями, які наведено в Методичних рекомендаціях з комерціалізації розробок, створених в результаті науково-технічної діяльності (див. табл. 4.1) [49].

Таблиця 4.1 – Критерії за якими проводиться технологічний аудит

| Критерії оцінювання та бали (за 5-ти бальною шкалою) | | | | | |
|---|---|---|---|---|---|
| Кри-терій | 0 | 1 | 2 | 3 | 4 |
| Технічна здійсненність концепції: | | | | | |
| 1 | Достовірність концепції не підтверджена | Концепція підтверджена експертними висновками | Концепція підтверджена розрахунками | Концепція перевірена на практиці | Перевірено роботоздатність продукту в реальних умовах |
| Ринкові переваги (недоліки): | | | | | |
| 2 | Багато аналогів на малому ринку | Мало аналогів на малому ринку | Кілька аналогів на великому ринку | Один аналог на великому ринку | Продукт не має аналогів на великому ринку |

Продовження таблиці 4.1

| Критерії оцінювання та бали (за 5-ти бальною шкалою) | | | | | |
|---|---|---|---|---|---|
| Кри-терій | 0 | 1 | 2 | 3 | 4 |
| 3 | Ціна продукту значно вища за ціни аналогів | Ціна продукту дещо вища за ціни аналогів | Ціна продукту приблизно дорівнює цінам аналогів | Ціна продукту дещо нижче за ціни аналогів | Ціна продукту значно нижче за ціни аналогів |
| 4 | Технічні та споживчі властивості продукту значно гірші, ніж в аналогів | Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів | Технічні та споживчі властивості продукту на рівні аналогів | Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів | Технічні та споживчі властивості продукту значно кращі, ніж в аналогів |
| Ринкові перспективи | | | | | |
| 5 | Експлуатаційні витрати значно вищі, ніж в аналогів | Експлуатаційні витрати дещо вищі, ніж в аналогів | Експлуатаційні витрати на рівні експлуатаційних витрат аналогів | Експлуатаційні витрати трохи нижчі, ніж в аналогів | Експлуатаційні витрати значно нижчі, ніж в аналогів |
| 6 | Ринок малий і не має позитивної динаміки | Ринок малий, але має позитивну динаміку | Середній ринок з позитивною динамікою | Великий стабільний ринок | Великий ринок з позитивною динамікою |
| 7 | Активна конкуренція великих компаній на ринку | Активна конкуренція | Помірна конкуренція | Незначна конкуренція | Конкурентів немає |
| Практична здійсненність | | | | | |
| 8 | Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї | Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців | Необхідне незначне навчання фахівців та збільшення їх штату | Необхідне незначне навчання фахівців | Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї |
| 9 | Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування | Потрібні незначні фінансові ресурси. Джерела фінансування | Потрібні значні фінансові ресурси. Джерела фінансуван | Потрібні незначні фінансові ресурси. Джерела фінансування | Не потребує додаткового фінансування |

| | | | | | |
|---|---|---|---|---|---|
| | ідеї відсутні | відсутні | ня є | є | |

Продовження таблиці 4.1

| Критерії оцінювання та бали (за 5-ти бальною шкалою) | | | | | |
|---|---|---|---|---|---|
| Кри-терій | 0 | 1 | 2 | 3 | 4 |
| 10 | Необхідна розробка нових матеріалів | Потрібні матеріали, що використовуються у військово-промисловому комплексі | Потрібні дорогі матеріали | Потрібні досяжні та дешеві матеріали | Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві |
| 11 | Термін реалізації ідеї більший за 10 років | Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років | Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років | Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років | Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років |
| 12 | Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту | Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу | Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу | Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту | Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту |



Встановлення рівня комерційного потенціалу результатів проведених нами досліджень та розроблених моделей і алгоритмів управління безпекою

мобільних абонентських пристроїв здійснювалося за рекомендаціями, наведеними в табл. 4.2 [2].

Таблиця 4.2 – Рівні комерційного потенціалу отриманих результатів

| Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів | Рівень комерційного потенціалу |
|---|---|
| 0 – 10 | Низький |
| 11 – 20 | Нижче середнього |
| 21 – 30 | Середній |
| 31 – 40 | Вище середнього |
| 41 – 48 | Високий |

Запрошені експерти оцінили результати проведених нами наукових досліджень та розроблених моделей і алгоритмів управління безпекою мобільних абонентських пристроїв за допомогою бальної системи оцінок, які зведено в табл. 4.3.

Таблиця 4.3 – Результати технологічного аудиту отриманих наукових результатів

| Критерії | Прізвище, ініціали експерта | | |
|---|---|---|---|
| | Городецька О.М. | Михалевський Д.В. | Васильківський М.В. |
| | Бали, виставлені експертами: | | |
| 1 | 4 | 4 | 4 |
| 2 | 4 | 4 | 4 |
| 3 | 3 | 4 | 4 |
| 4 | 3 | 4 | 4 |
| 5 | 3 | 4 | 4 |
| 6 | 4 | 4 | 4 |
| 7 | 4 | 3 | 4 |
| 8 | 4 | 4 | 4 |
| 9 | 4 | 3 | 3 |
| 10 | 4 | 4 | 4 |
| 11 | 4 | 4 | 4 |
| 12 | 4 | 4 | 4 |
| Сума балів | $СБ_1 = 45$ | $СБ_2 = 46$ | $СБ_3 = 47$ |
| Середньоарифметична сума балів $\overline{СБ}$ | $\overline{СБ} = \frac{\sum_{1}^{3} СБ_i}{3} = \frac{45+46+47}{3} = \frac{138}{3} = 46,00.$ | | |

Оскільки середньоарифметична сума балів, що їх виставили експерти, дорівнює 46-ти балам, то можна зробити висновок, що результати проведених нами досліджень та розроблені моделі і алгоритми управління безпекою мобільних абонентських пристроїв мають рівень комерційного потенціалу, який є «високим».

Це пояснюється тим, що на основі дослідження формальної моделі безпеки мобільних абонентських пристроїв було розроблено оригінальний алгоритм управління безпекою мобільних абонентських пристроїв, що враховує атрибути доступу користувачів до мобільних абонентських пристроїв незалежно від місця їх перебування, а також враховує вимоги до якості цих послуг, що надаються, тощо, що дозволяє підвищити ймовірність забезпечення безпеки інформації при доступі користувачів до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного мобільного абонентського пристрою.

## 4.2 Розрахунок витрат на проведення наукових досліджень

Для проведення наукових досліджень та розробки моделей і алгоритмів управління безпекою мобільних абонентських пристроїв були зроблені такі витрати: [2]:

### 4.2.1 Основна заробітна плата $З_о$ дослідників:

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

де М – місячний посадовий оклад дослідника (науковця), грн.

Для науковців ВНТУ дані оклади не є високими і коливаються в межах:

М = (4173…18000) грн. за місяць;

$Т_р$ – число робочих днів в місяці; приймемо, що $Т_р$ = 20 днів;

t – число робочих днів роботи науковців (дослідників).

Зроблені розрахунки основної заробітної плати зведемо до табл. 4.4:

Таблиця 4.4 – Основна заробітна плата дослідників (науковців)

| Найменування посади виконавця | Місячний посадовий оклад, грн | Оплата за робочий день, грн | Число днів роботи | Витрати на оплату праці, грн | Примітка |
|---|---|---|---|---|---|
| 1. Науковий керівник магістерської роботи | 12950 | 648 | 25 годин | 2700 | 6-год. робочий день |
| 2. Магістрант – дослідник | 2400 | 120 | 65 | 7800 | |
| 3. Консультант з економічної частини | 11565 | 578 | 2,5 годин | 241 | |
| Загалом витрат на оплату праці | | | | $З_о$ = 10741 грн | |

4.2.2 Додаткова заробітна плата $З_д$ розраховується за формулою:

$$З_д = (0{,}1...0{,}12) \cdot З_о. \qquad (4.2)$$

Для нашого випадку отримаємо:

$$З_д = 0{,}12 \times 10741 = 1289 \text{ грн.}$$

4.2.3 Нарахування на заробітну плату $Н_{зп}$ розраховуються за формулою:

$$Н_{зп} = (З_о + З_д) \cdot \frac{\beta}{100}, \qquad (4.3)$$

де $\beta$ = 22% – ставка єдиного внеску на загальне державне соціальне страхування.

Для нашого випадку отримаємо:

$$Н_{зп} = 10741+1289) \times 0{,}22 = 2647 \text{ грн.}$$

4.2.4 Амортизація А основних засобів, комп'ютерів, принтерів, приміщень, обладнання тощо розраховується за формулою:

$$А = \frac{Ц \cdot Н_а}{100} \cdot \frac{Т}{12} \text{ грн}, \qquad (4.4)$$

де Ц – загальна балансова вартість основних засобів, які використовувалися під час проведення досліджень, грн;

$Н_а$ – річна норма амортизаційних відрахувань. Спрощено можна прийняти, що

$Н_а$ = (2,25...22,5)%;

Т – термін, використання кожного виду основних засобів, місяці.

Зроблені нами розрахунки зведемо у табл. 4.5.

Таблиця 4.5 – Розрахунок амортизаційних відрахувань (округлено до цілих чисел)

| Найменування основних засобів | Балансова вартість, грн. | Норма амортизації, % | Термін використання, міс. | Величина амортизаційних відрахувань, грн. |
|---|---|---|---|---|
| 1. Основні засоби, принтери, обладнання, комп'ютери | 38000 | 20 | 2,8 міс. при 45% використанні | 798 |
| 2. Приміщення університету, кафедри та офакультету | 17500 | 2,5 | 2,8 міс. при 45% використанні | 46 |
| Разом | | | | А = 844 |

4.2.5. Витрати на матеріали М розраховуються за формулою:

$$M = \sum_{1}^{n} H_i \cdot Ц_i \cdot K_i - \sum_{1}^{n} B_i \cdot Ц_в \text{ грн}, \quad (4.5)$$

де $Н_i$ – витрати матеріалу *і*-го найменування, кг; $Ц_i$ – вартість матеріалу *і*-го найменування, грн/кг.; $К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15); $В_i$ – маса відходів матеріалу *і*-го найменування, кг; $Ц_в$ – ціна відходів матеріалу *і*-го найменування, грн/кг; n – кількість видів матеріалів.

4.2.6. Витрати на комплектуючі К розраховуються за формулою:

$$K = \sum_{1}^{n} H_i \cdot Ц_i \cdot K_i \text{ грн.}, \quad (4.6)$$

де $Н_і$ – кількість комплектуючих *і*-го виду, шт.; $Ц_і$ – ціна комплектуючих *і*-го виду, грн; $К_і$ – коефіцієнт транспортних витрат, $К_і$ = (1,1…1,15); n – кількість видів комплектуючих.

Загальна вартість основних матеріалів, які були використані під час проведення даних досліджень, складає приблизно 1290 грн.

4.2.7. Витрати на силову електроенергію $В_е$, що була використана при виконанні даної роботи, розраховуються за формулою:

$$B_e = \frac{B \cdot П \cdot Ф \cdot K_п}{K_д}, \quad (4.7)$$

де В – вартість 1 кВт-год. електроенергії, в 2019 р. В ≈ 2,50 грн/кВт;

П – установлена потужність обладнання, кВт; П = 1,62 кВт;

Ф – фактична кількість годин роботи обладнання, годин.

Приймемо, що Ф = 158 годин;

$К_п$ – коефіцієнт використання потужності; $К_п$ < 1 = 0,82.

$К_д$ – коефіцієнт корисної дії, $К_д$ = 0,73.

Тоді витрати на силову електроенергію складуть:

$$В_е = \frac{В \cdot П \cdot Ф \cdot К_п}{К_д} = \frac{2,50 \cdot 1,62 \cdot 158 \cdot 0,82}{0,73} \approx 719 \text{ грн.}$$

4.2.8. Інші витрати $В_{ін}$ (опалення, освітлення тощо) розраховуються як (100…300)% від основної заробітної плати виконавців цієї роботи, тобто:

$$В_{ін} = (1..3) \times З_о. \quad (4.8)$$

Для нашого випадку отримаємо:

$$В_{ін} = 2,125 \times 10741 = 22825 \text{ грн.}$$

4.2.9. Сума всіх попередніх статей дає витрати на проведення наукових досліджень та розробку моделей і алгоритмів управління безпекою мобільних абонентських пристроїв безпосередньо магістрантом – В.

$$В = 10741 + 1289 + 2647 + 844 + 1290 + 719 + 22825 = 40355 \text{ грн.}$$

4.2.10 Загальні витрати на виконання цієї роботи розраховуються за формулою:

$$ЗВ = \frac{B}{\beta}, \tag{4.9}$$

де $\beta$ – коефіцієнт, який характеризує етап виконання даної роботи на шляху до її можливого впровадження:

якщо це тільки науково-дослідні роботи, то $\beta \approx 0{,}1$;

якщо це стадія технічного проектування, то $\beta \approx 0{,}2$;

якщо стадія розробки конструкторської документації, то $\beta \approx 0{,}3$;

якщо це стадія розробки технології, то $\beta \approx 0{,}4$;

якщо це стадія розробки дослідного зразка, то $\beta \approx 0{,}5$;

якщо це стадія розробки промислового зразка, $\beta \approx 0{,}7$;

якщо це стадії впровадження, то $\beta \approx (0{,}8 - 0{,}9)$.

Для нашого випадку доцільно прийняти, що $\beta \approx 0{,}75$.

Тоді: $ЗВ = \frac{40355}{0{,}75} = 53806{,}67$ грн або приблизно 54 тис. грн.

Тобто загальні витрати на завершення проведених нами наукових досліджень та розробку моделей і алгоритмів управління безпекою мобільних абонентських пристроїв становлять приблизно 54 тис. грн.

## 4.3 Оцінювання технічного рівня проведених наукових досліджень

Оскільки на цьому етапі проведення досліджень складно більш-менш реально оцінити можливості комерціалізації отриманих результатів (про які було зазначено у технологічному аудиті), проведемо оцінювання технічного рівня отриманих нами результатів.

Для кількісного оцінювання технічного рівня результатів проведених досліджень та розроблених моделей і алгоритмів управління безпекою мобільних абонентських пристроїв може бути використаний комплексний показник $К_р$, який розраховується за формулою:

$$K_{\text{р}} = \frac{I^n \cdot T_c \cdot R}{B \cdot t}, \tag{4.10}$$

де: I – коефіцієнт важливості досліджень, I = (2…5);

n – коефіцієнт використання результатів досліджень;

n = 0, коли результати роботи не будуть використовуватись;

n = 1, коли результати будуть використовуватись частково;

n = 2, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках;

n = 3, коли результати можуть використовуватись навіть без проведення дослідно-конструктор-ських розробок;

$T_c$ – коефіцієнт складності досліджень, $T_{скл}$ = (1…3);

R – коефіцієнт результативності досліджень:

R = 4, якщо результати роботи плануються вище відомих;

R = 3, якщо результати роботи відповідають відомому рівню;

R = 2, якщо результати нижче відомих;

R = 1, якщо результат роботи не визначений;

B = 33 тис. грн;

t – час проведення подальших досліджень, років.

Якщо $K_р \geq 1$, то технічний рівень отриманих результатів проведених досліджень та розроблених моделей і алгоритмів управління безпекою мобільних абонентських пристроїв є високим.

Для визначення коефіцієнтів, наведених у формулі 4.10, запросимо тих же експертів, які здійснювали технологічний аудит.

Результати висновків експертів занесено у табл. 4.6.

Таблиця 4.6 – Результати оцінювання експертами зазначених коефіцієнтів

| Показник | Експерти | | | Переважаюча оцінка |
|---|---|---|---|---|
| | Городецька О.М. | Михалевський Д.В. | Васильківський М.В. | |
| 1. Коефіцієнт важливості роботи, I | 3 | 4 | 3,5 | 3,5 |
| 2. Коефіцієнт використання результатів роботи, n | 2,0 | 2,0 | 2,5 | 2,25 |
| 3. Коефіцієнт складності роботи, $T_c$ | 2 | 2 | 2 | 2 |
| 4. Коефіцієнт результативності роботи, R | 2 | 3 | 2,5 | 2,5 |
| 5. Вартість роботи, тис. грн. | 54 | 54 | 54 | 54 |
| 6. Час проведення подальших досліджень, роки | 1 | 1 | 1,25 | 1,15 |

Аналізуючи результати, наведені в таблиці 4.6, можна зробити висновок, що переважаючими коефіцієнтами, які були виставлені експертами, будуть такі:

I – коефіцієнт важливості проведених досліджень, I = 3,5;

n – коефіцієнт використання результатів роботи; n = 2,25;

$T_c$ – коефіцієнт складності роботи, $T_{скл}$ = 2;

R – коефіцієнт результативності проведених досліджень; R = 2,5;

B – вартість роботи; B = 54 тис. грн.;

t – час завершення досліджень, t = 1,15 рік.

Тоді показник $K_p$, що визначає технічний рівень результатів, отриманих під час проведених досліджень та розроблення моделей і алгоритмів управління безпекою мобільних абонентських пристроїв, буде дорівнювати:

$$K_p = \frac{I^n \cdot T_c \cdot R}{B \cdot t} = \frac{3,5^{2,25} \cdot 2,0 \cdot 2,5}{54 \cdot 1,15} = \frac{16,75 \cdot 2,0 \cdot 2,5}{54 \cdot 1,15} = 1,348.$$

Оскільки $K_p$ = 1,348 > 1, то це свідчить про те, що технічний рівень результатів проведених наукових досліджень та розроблених моделей і алгоритмів управління безпекою мобільних абонентських пристроїв є досить високим.

Таблиця 4.7 – Результати виконаної економічної частини магістерської кваліфікаційної роботи

| Показники | Задані у ТЗ | Досягнуто у магістерській кваліфікаційній роботі | Висновок |
|---|---|---|---|
| 1. Витрати на виконання роботи | Не більше 60 тис. грн | 54 тис. грн. | Виконано |
| 2. Коефіцієнт використання результатів проведених досліджень | не менше 2 | 2,25 | Виконано |
| 3. Коефіцієнт важливості проведених досліджень | не менше 3 | 3,5 | Виконано |
| 4. Коефіцієнт результативності проведених досліджень | не менше 2 | 2,5 | Виконано |
| 5. Коефіцієнт складності | не менше 2 | 2,0 | Виконано |
| 6. Комплексний показник технічного рівня отриманих результатів | не менше 1,2 | 1,348 | Досягнуто |

Таким чином, основні техніко-економічні завдання, що були поставлені перед магістрантом під час виконання цієї магістерської кваліфікаційної роботи, повністю виконані.

# 5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Забезпечення захисту працюючих під час трудового процесу від небезпечних та шкідливих виробничих факторів, що негативно впливають на здоров'я, життя, а також працездатність людини, забезпечення належних умов праці є основними аспектами безпеки життєдіяльності у виробничому середовищі.

В цьому розділі проводиться розгляд небезпечних, шкідливих [52] і уражаючих для людини і оточуючого середовища чинників, що виникають під час проведення дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу. В ньому висвітлюються, в тому числі, технічні рішення з виробничої санітарії та гігієни праці, визначення розмірів екрану для захисту від шуму, технічні рішення з промислової та пожежної безпеки при проведенні дослідження, безпека у надзвичайних ситуаціях.

## 5.1 Гігієна праці та виробнича санітарія

### 5.1.1 Мікроклімат та склад повітря робочої зони

Визначаємо для приміщення для проведення дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу, категорію важкості робіт за фізичним навантаженням – легка Іа.

У відповідності із [53] допустимі параметри температури, відносної вологості та швидкості руху повітря у робочій зоні для теплого та холодного періодів року приведені в табл. 5.1 додатку Х.

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

Вміст шкідливих речовин в повітрі робочої зони не повинен перевищувати гранично допустимих концентрацій (ГДК) в повітрі робочої зони і підпадає під систематичний контроль для запобігання можливості перевищення ГДК, значення яких для роботи з ЕОМ наведено в табл. 5.2 додатку Х.

При використанні ЕОМ джерелом забруднення повітря є також іонізація молекул речовин, які містяться в повітрі. Рівні позитивних та негативних іонів мають відповідати [55] та наведені в табл. 5.3 додатку Х.

З метою встановлення необхідних за нормативами параметрів мікроклімату і складу повітря робочої зони передбачено: в приміщенні

повинна бути розміщена система опалення для холодного і кондиціонування для теплого періодів року; застосування вентиляції, яка видаляє забруднення або нагріте повітря з приміщення, а також за допомогою неї контролюється швидкість руху повітря і вологість.

### 5.1.2 Виробниче освітлення

З метою забезпечення гігієнічних раціональних умов на робочих місцях великі вимоги пред'являються до кількісних та якісних параметрів освітлення.

З погляду задач зорової роботи в приміщенні, в якому проводиться робота з дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу, відповідно до [54] визначаємо, що вони відповідають IV розряду зорових робіт. Вибираємо контраст об'єкта з фоном – середній та характеристику фону – середню, яким відповідає підрозряд *в*.

Нормовані значення коефіцієнта природного освітлення (КПО) та мінімальні значення освітленості при штучному освітленні наведені в табл. 5.4 додатку Х.

Оскільки приміщення знаходиться в місті Вінниця (2-га група забезпеченості природним світлом), а вікна орієнтовані за азимутом 45°, то для таких обставин КЕО визначатиметься за формулою [55,56]

$$e_N = e_н m_N \ [\%], \qquad (5.1)$$

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

$m_N$ – коефіцієнт світлового клімату;

$N$ – номер групи забезпеченості природним світлом.

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

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

$$e_{N.с} = 0,9 \cdot 0,9 = 0,8 \ (\%).$$

Для встановлення нормативних значень показників освітлення запропоновано: при недостатньому природному освітлені в світлу пору доби доповнення штучним завдяки використанню люмінесцентних ламп з

утворенням системи суміщеного освітлення; застосування загального штучного освітлення у темну пору доби.

### 5.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що під час експлуатації пристроїв крім усього іншого обладнання використовується устаткування, робота якого генерує шум та вібрацію, необхідно передбачити шумовий та вібраційний захист.

Встановлено, що приміщення, в якому проводиться робота з дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу може мати робочі місця із шумом та вібрацією, що спричиняється рухомими елементами ЕОМ.

З метою запобігання травмуванню працівників під дією шуму він підлягає нормуванню. Основним документом з питань виробничого шуму, що діє на території України, є [56], згідно з яким нормовані рівні звукового тиску, рівні звуку та еквівалентні рівні шуму на робочих місцях у промислових приміщеннях не мають бути більшими ніж значення, які приведені у табл. 5.5 додатку Х. Норми виробничих вібрацій наведені в табл. 5.6 додатку Х для локальної вібрації.

Для встановлення нормованих параметрів шуму та вібрації в приміщенні запропоновано: періодичне змащування підшипників вентиляторів блоку живлення ЕОМ та кулерів відеоадаптера та мікропроцесора; передбачено використовувати в приміщені штори із щільної тканини.

Вихідні дані: послаблення шуму $L$ = 115 дБ. Відстань від джерела шуму до екрану $R$ = 2,0 м, відстань від екрану до працівника $D$ = 1,4 м, частота шуму $f$ = 15 кГц.

За величиною $L$ = 115 вибираємо величину $N$ = 7,727.

Розмір сторони квадратного екрану можна визначити з формули

$$N = \frac{2}{\lambda}\left[ R\left( \sqrt{1+\left(\frac{H}{R}\right)^2} - 1 \right) + D\left( \sqrt{1+\left(\frac{H}{D}\right)^2} - 1 \right) \right] \quad , \qquad (5.2)$$

звідки після значних математичних перетворень отримаємо таку ітераційну формулу

$$H = \sqrt{\left( \frac{N\lambda}{2} + R^2 + D^2 - \sqrt{D^2 + H^2} \right)^2 - R^2} \qquad \text{[м]}, \qquad (5.3)$$

де $\lambda$ – довжина хвилі, м;

$R$ – відстань від джерела шуму до екрану, м;

$D$ – відстань від екрану до працівника, м;

$H$ – розмір сторони екрану, м.

Довжину хвилі можна визначити за формулою

$$\lambda = \frac{c}{f} \quad [\text{м}], \tag{5.4}$$

де $c$ – швидкість звуку в повітрі за нормальних умов, м/с ($c$ = 330 м/с);

$f$ – частота коливань, Гц.

Після підстановки відомих значень у формулу (5.4) отримаємо

$$\lambda = \frac{300}{15 \cdot 10^3} = 0{,}02 \text{ (м)};$$

Приймемо початкове значення $H_0$ = 9,1 м.

Після підстановки відомих значень у формулу (5.3), отримаємо в першому наближенні:

$$H_1 = \sqrt{(7{,}727 \cdot 0{,}02 / 2 + 2{,}0^2 + 1{,}4^2 - \sqrt{1{,}4^2 + 9{,}1^2})^2 - 2{,}0^2} = 2{,}4592 \text{ (м)};$$

в другому наближенні:

$$H_2 = \sqrt{(7{,}727 \cdot 0{,}02 / 2 + 2{,}0^2 + 1{,}4^2 - \sqrt{1{,}4^2 + 2{,}4592^2})^2 - 2{,}0^2} = 2{,}507585 \text{ (м)};$$

в третьому наближенні:

$$H_3 = \sqrt{(7{,}727 \cdot 0{,}02 / 2 + 2{,}0^2 + 1{,}4^2 - \sqrt{1{,}4^2 + 2{,}507585^2})^2 - 2{,}0^2} = 2{,}4534418 \text{ (м)};$$

Оскільки $H_2 \approx H_3$, то остаточно приймаємо розмір сторони квадратного екрану для захисту від шуму $H = H_3$ = 2,453 м.

5.1.4 Виробничі випромінювання

Величина напруженості електромагнітного поля на робочих місцях з персональними комп'ютерами мають не перевищувати граничнодопустимі, які складають 20 кВ/м.

Експозиційна доза рентгенівського випромінювання на відстані 5 см від екрана до корпуса монітора при будь-яких положеннях регулювальних пристроїв не повинні перевищувати $7{,}74 \cdot 10^{-12}$ Кл/кг, що відповідає потужності еквівалентної дози 0,1 мБер/год (100 мкР/год) згідно [65].

Для гарантування захисту та досягнення нормованих рівнів випромінювань потрібно використовувати екранування робочого місця і скорочення часу опромінення за рахунок перерв на відпочинок.

## 5.2 Промислова та пожежна безпека при проведенні дослідження

Сучасний етап розвитку техніки, автоматизації розробок та досліджень характеризується широким використанням на робочому місці ЕОМ. Наявність великої кількості прикладних програм сприяє тому, що ЕОМ є основним робочим інструментом інженера в галузі радіотехніки.

### 5.2.1 Безпека щодо організації робочих місць

Робочі місця з відеодисплейним терміналом зобов’язані розміщатися на відстані не менше ніж 1,5 м від стіни з вікнами, від інших стін – на віддалі 1 м, одне від одного на віддалі не менше як 1,5 м. При розміщенні робочих місць потрібно виключити ймовірність прямого засвічування екрану джерелом природного освітлення. Робоче місце раціонально розташовувати таким чином, щоб природне освітлення знаходилось збоку, переважно зліва [69].

Поверхня екрана повинна знаходитись на відстані 400-700 мм від органів зору користувача. Висота робочої поверхні столу під час виконання роботи сидячи має регулюватися в межах 680-800 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною не менше ніж 500 мм, глибиною на рівні колін не менше 450 мм та на рівні витягнутої ноги не менше ніж 650 мм [70].

### 5.2.2 Електробезпека

У середині приміщення, в якому здійснюється робота з дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу, значну увагу потрібно приділити уникненню загрози ураження електричним струмом. У відповідності до [71] дане приміщення відноситься до приміщень із підвищеною небезпекою ураження електричним струмом через наявність високої (більше 75 %)

вологості. Тому безпека експлуатації електрообладнання повинна гарантуватись комплексом заходів, які передбачають використання ізоляції струмоведучих частин, захисних блокувань, захисного заземлення тощо [72].

### 5.2.3 Пожежна безпека

Згідно [73] приміщення, де проводиться робота з дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу, відноситься до категорії пожежної небезпеки В. Дане приміщення відноситься до 2-го ступеня вогнестійкості, в якому приміщення знаходяться в будівлі з несучими та огороджувальними конструкціями з природних або штучних кам'яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості будівельних конструкцій розглядуваного приміщення наведені в таблиці 5.7. В таблиці 5.8 приведено протипожежні норми проектування будівель і споруд.

Встановлюємо, що приміщення, де проводиться робота з дослідження, має бути обладнане двома вогнегасниками, пожежним щитом, ємністю з піском [74].

## 5.3 Безпека в надзвичайних ситуаціях

Підсилювачі зустрічаються всюди, де застосовується звук: у військовій сфері, на вокзалах,в аеропортах, літаках, тому їх функціонування є надзвичайно важливим при НС. Вихід з ладу системи підсилення збільшить кількість жертв в рази і призведе до дезорієнтації. Також вихід з ладу підсилювачів не дозволить вчасно сповістити людей про небезпеку.
Системи зв'язку є пристроями подвійного застосування. В умовах НС вони повинні працювати без перебоїв, тому розробка заходів щодо покращення роботи мобільного абонентського терміналу в умовах ЕМІ та дії іонізуючих випромінювань є актуальною.

Дія електромагнітного імпульсу також може призвести до загоряння чутливих електричних та електронних елементів, а також до серйозних порушень в цифрових і контрольних пристроях. Електромагнітний імпульс пробиває ізоляцію, випалює елементи мікросхем, викликає коротке замикання. Саме тому є необхідність запобіганню при дії цього фактору на електричне та електронне обладнання.

5.3.1 Дослідження безпеки роботи мобільного абонентського терміналу в умовах дії іонізуючих випромінювань

За критерій безпеки роботи РЕС в цих умовах приймається таке максимальне значення дози опромінення елементної бази, при якому в елементній базі можуть виникнути зміни, але РЕС ще буде працювати з необхідною якістю.

Максимально допустимі значення потужності дози елементів мобільного абонентського терміналу наведені в табл. 5.1.

Таблиця 5.1 - Максимально допустимі потужності доз терміналу.

| № | Блок | Елементи приладу | $P_{гр,i}$(Р/год) | $P_{гр}$ (Р/год) |
|---|---|---|---|---|
| 1 | БЖ | Транзистори КТ3102В | $10^5$ | $10^4$ |
| | | Діоди загального призначення S1M | $10^5$ | |
| 2 | БП | Конденсатори SMD1206 lnf, 16V | $10^6$ | |
| | | Резистори SMD1206 0,125 - 10кОм | $10^6$ | |
| 3 | БКП | Мікросхеми PIC16F877 | $10^4$ | |
| | | Діелектрики GTP15 | $10^4$ | |

1. За мінімальним значенням $p_{гр}$ (див. табл. 5.1) межа стійкості $p_{гр}$ роботи системи складає $p_{гр} = 10^4$ (Р/год).

2. Для дослідження безпеки роботи мобільного абонентського терміналу визначається граничне значення потужності дози гамма-випромінювання ($p_{гр}$) за наступною формулою:

$$P_{гр}=K\times p_{гр}\times K_{пос}\,, \qquad (5.5)$$

де: К – коефіцієнт надійності, К = 0,9..0,95;

$p_{гр}$ – рівень радіації, що відповідає початку зворотних зміну найменш стійкого елемента;

$К_{пос}$ – коефіцієнт послаблення радіації ($К_{пос}$ = 7),

$$P_{гр} = 0{,}9 \times 10^4 \times 7 = 6{,}3 \times 10^4 \text{ (Р/год)},$$

1. З вище наведених розрахунків можна зробити висновок, що безпека в умовах дії іонізуючих випромінювань буде забезпечуватись, якщо радіація в умовах експлуатації не перевищуватиме $P_{гр} = 6{,}3 \times 10^4$ (Р/год).

2. Розрахуємо допустимо максимальний час перебування приладу на території в умовах дії іонізуючих випромінювань та ЕМІ:

$$Д_м = \frac{2P_{гр}(\sqrt{t_К{}^2} - \sqrt{t_П{}^2})}{1}, \quad (5.6)$$

де: $\sqrt{t_П{}^2}$ , дорівнює 1;

$Д_м$– дорівнює $10^3$;

$t_{доп} = 12{,}6 \times 10^3$ (год).

Отже підсилювач потужності буде працювати безпечно в умовах іонізуючих випромінювань.

5.3.2 Дослідження стійкості роботи мобільного абонентського терміналу в умовах дії електромагнітного імпульсу

В якості показника безпеки елементів системи до дії електромагнітного імпульсу використовують коефіцієнт безпеки [61]:

$$K_б = 20\lg\frac{U_д}{U_{В(Г)}} \geq 40 дБ \quad , \quad (5.7)$$

де $U_д$ - допустиме коливання напруги живлення;

$U_{В(Г)}$- напруга наведена за рахунок електромагнітного імпульсу у вертикальних (горизонтальних) струмопровідних системах.

Спочатку визначається допустиме коливання напруги живлення:

$$U_д = U_ж + \frac{U_ж}{100} \cdot N \quad , \quad (5.8)$$

де $N$ - допустимі коливання (приймається $N = 5\%$)

Шляхом підстановки числових даних в (5.3) отримується:

$$U_д = 12 + \frac{12}{100} \cdot 5 = 12{,}6(В).$$

Визначається максимально очікувана напруга в горизонтальних лініях[61]:

$$U_B = \frac{U_д}{10^{\frac{K}{20}}} \quad (5.9)$$

Після підстановки числових даних:

$$U_B = \frac{12,6}{10^{\frac{40}{20}}} = 0,126(B).$$

З формули визначається горизонтальна складова напруженості електричного поля[61]:

$$U_B = E_Г \cdot l_B . \quad (5.10)$$

Отже, $E_Г$ визначається:

$$E_Г = \frac{U_B}{l_B} . \quad (5.11)$$

Після підстановки числових даних в формулу (5.11):

$$E_Г = \frac{0,126}{5} = 0,0252(B/м) .$$

Вертикальна складова напруженості електричного поля визначається з формули [61]:

$$E_Г = 10^{-3} \cdot E_B . \quad (5.12)$$

$$E_B = 0,0252 \cdot 1000 = 25,2(B/м).$$

5.4 Розробка заходів по підвищенню безпеки роботи мобільного абонентського терміналу в умовах надзвичайних ситуацій

Дія підвищення безпеки роботи необхідно використовувати екранування мобільного абонентського терміналу. Для цього визначимо перехідне гасіння енергії електричного поля сталевим екраном.

Розрахуємо товщини захисних екранів:

$$t = \frac{A}{5,2 \cdot \sqrt{f}}, \qquad (5.13)$$

де $f$ - найбільш характерна частота, ($f = 15$ кГц).

Для двоканального мобільного абонентського терміналу:

$$t_1 = \frac{40 - 38.72}{5.2 \cdot \sqrt{15000}} = 0.0025 \quad \text{(см);} \qquad .$$

Обираємо товщину стінки на порядок вище, для того щоб забезпечити необхідний захист обладнання. Приймемо t=0,102 см.

$$A=5,2*0,102*\sqrt{15000}=65(\text{дБ}).$$

Отже нам потрібно взяти сталевий екран товщиною 0,102 см, який забезпечує згасання енергії електричного поля 65 дБ.

5.5 Висновки до розділу 5

В результаті написання даного розділу було опрацьовано такі питання охорони праці та безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення розмірів екрану для захисту від шуму, технічні рішення з промислової та пожежної безпеки при проведенні дослідження інформаційної захищеності мобільного абонентського терміналу в корпоративних мережах доступу, безпека в надзвичайних ситуаціях.

Також в результаті проведених розрахунків визначено, що безпека роботи мобільного абонентського терміналу забезпечується при рівні радіації до $6,3 \times 10^4$ (Р/год). До дії ЕМІ в підсилювачі потужності необхідно застосовувати екранування РЕА і це суттєво підвищує його стійкості в умовах дії електромагнітного імпульсу. В результаті застосування екранів мобільного абонентського терміналу буде працювати стійко аж до значення напруженості вертикальної складової 25,2 В/м. Ще одним варіантом підвищення безпеки роботи мобільного абонентського терміналу до дії випромінювання є зменшення струмопровідних провідників шляхом вдосконалення схемоустаткування пристрою.

# ВИСНОВКИ

У МКР отримано рішення актуального завдання по розробці алгоритму і заснованої на ньому системи управління безпекою МАП, що базуються на запропонованій формальній моделі безпеки МАП, в сукупності дозволяють підвищити ймовірність забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП за рахунок обліку атрибутів доступу, включаючи розташування МАП, вимог щодо якості надання сезонних послуг, а також політики безпеки захищених корпоративних мереж.

Новизна пропонованого підходу полягає в розробці та обґрунтуванні коректності формальної моделі безпеки МАП, що відрізняється від відомих урахуванням оцінки його місцезнаходження в спеціальному приміщенні, інших атрибутів доступу, а також реалізацією вимог мандатної і рольової політик безпеки в корпоративних мережах з різними вимогами щодо єдиного МАП і розробці на базі даної моделі нового алгоритму управління безпекою МАП, що відрізняється від відомих визначенням оптимальної, з точки зору забезпечення конфіденційності інформації та якості послуг, що надається користувачеві послуг, програмно-апаратної конфігурації МАП.

В рамках проведення досліджень були отримані наступні результати:

1) проведено аналіз стану наукових досліджень і технічних рішень в області захисту інформації при використанні МАП, виявлені недоліки сучасних формальних моделей безпеки комп'ютерних систем стосовно забезпечення безпеки інформації при використанні МАП, включаючи існуючі технічні та програмно-апаратні рішення; для вирішення завдання віддаленого управління, а також сполучення контурів обробки інформації з різними вимогами по захищеності в сучасних МАП пропонується використовувати агентно-орієнтований підхід, який є елементом штучного інтелекту і побудований на основі клієнт-серверної архітектури;

2) розроблена модель безпеки МАП, що відрізняється від відомих урахуванням його місцезнаходження в корпоративних мережах з різними вимогами по захищеності; обґрунтований вибір технологій, на основі яких доцільно побудова системи визначення місця розташування МАП, а також запропонований підхід, що дозволяє підвищити достовірність визначення місцезнаходження МАП в спеціальних приміщеннях; здійснено апробацію моделі за допомогою імітаційного моделювання, а також проведена всебічна оцінка її якості, що включає в себе перевірку адекватності, чутливості і стійкості; отримані оцінки параметрів приватних моделей, які

впливають на достовірність визначення місця розташування МАП;

3) розроблено алгоритм управління безпекою МАП, що враховує атрибути доступу мобільних користувачів; описана оптимізаційна завдання, яке вирішується в алгоритмі і охарактеризована як задачу багатокритеріальної оптимізації цілочисельного динамічного програмування; представлено опис циклу управління конфігурацією МАП з рівняннями стану і спостереження, обгрунтуванням мети управління; описані основні процедури, що входять до складу алгоритму; досліджено основні властивості алгоритму і його процедур, включаючи тимчасову складність, складність по пам'яті і точність. Отримано їх чисельні оцінки, а також представлений чисельний приклад роботи алгоритму;

4) сформовані науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності; проведена група експериментів і обгрунтований вибір оптимальних параметрів підсистеми визначення місця розташування; здійснено комплексну оцінку ефективності розроблених пропозицій з отриманням чисельних значень для оцінки часу, необхідного для зміни конфігурації МАП, ймовірності загрози порушення конфіденційності при використанні керованих МАП, ресурсоємності запропонованої системи управління безпекою МАП, своєчасності доступу до послуг; отримана чисельна оцінка ступеня досягнення мети дослідження МКР, що дозволяє стверджувати те, що мета досягнута.

Напрямком подальших досліджень автор вважає

– дослідження перспективних технологій визначення місцеположення користувачів МАП в приміщеннях всередині будівлі з метою зниження помилок;

– дослідження технологій агентно-орієнтованого підходу для оптимізації інформаційної взаємодії контролерів бездротових мереж з передачі керуючої інформації;

– вдосконалення підходів щодо управління конфігурацією сучасних мобільних пристроїв з метою створення можливості реалізації розроблених підходів щодо управління доступом стосовно до послуг, які використовують конфіденційні відомості.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вишнякова, О. А. Математическая модель обнаружения точки беспроводного доступа по измерениям можности излучения разнесенными наблюдателями / О. А. Вишнякова, Д. Н. Лавров, С. Ю. Лаврова // Математические структуры и моделирование / Ом. гос. ун-т. Фак. компьютер. наук. – Омск : Изд-во ОмГУ. – 2013. – No 2(28). – С.49–59.

2. Вопросы безопасности мобильных устройств / А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский // Безопасность информационных технологий Москва : Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации, 2012. – С. 5–7.

3. Ворошилин, Е. П. Моделирование процессов и явлений в системах святи : методическое пособие для самостоятельной работы магистров направления 210700.68 "Инфокоммуникационные технологии и системы связи" / Е. П. Ворошили // ТУСУР, 2012.

4. Выборнов, О. В. Прогнозирование потенциальной нагрузки секторов сетей широкополосного доступа на основе анализа отношения сигнал/помеха с использованием геоинформационных технологий / О .В. Выборнов, А. М. Измайлов, С. В. Козлов, В Н. Лаврушев, Е. А. Спирина // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2013. – Выпуск No 4. – С. 130–135.

5. Выборнов, О. В. Тестирование ЭМС оборудования стандарта 802.11n фирмы InfiNet / О. В. Выборнов, А. М. Измайлов, С. В. Козлов, Е. А. Спирина // Вестник КГТУ им. А. Н. Туполева. – 2012. – Выпуск No 2 (68). – С. 160–163.

6. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978-5-9912-0328-9.

7. Десницкий, В. А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления : автореф. дис. ... канд. техн.. наук : 05.13.19 / Десницкий Василий Алексеевич ; [Санкт-Петербургский ин-т информатики и автоматизации РАН]. – Санкт-Петербург, 2013. – 22 с. – Библиогр.: с. 21–22.

8. Маркин, Д. О. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 9. – С. 39–50.

9. Маркин, Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений / Д. О. Маркин // Вестник РГРТУ. – 2015. – No 54-1. – С. 32–39.

10. Маркин, Д. О. Методика обнаружения и способы противодействия распределенной атаке типа "отказ в обслуживании", основанной на использовании SEO-технологий / Д. О. Маркин, М. А. Сазонов // Информация и безопасность. – 2014. – No 2 (7) – С.208–211.

11. Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – No 4 (22). – С. 21–31.

12. Маркин, Д. О. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 10. – С. 40–51.

13. Маркин, Д.О. Модель доступа к информационным системам / Д. О. Маркин, М. А. Сазонов // Телекоммуникации. – 2013. – No 9. – С. 27–31.

14. Маркин, Д.О. Модель и алгоритм адаптивного управления профілем защиты мобильного устройства / Д. О. Маркин, В. В. Комашинский // XII Всероссийское совещание по проблемам управления ВСПУ-2014. Москва, 16-19 июня 2014 г. : Труды. [Электронный ресурс] Москва : Институт проблем управления им. В. А. Трапезникова РАН, 2014. 9616 с. Электрон. текстовые дан. (1074 файл.: 537 МБ). 1 электрон. опт. диск (DVD-ROM). Файл 7449. ISBN 978-5-91450-151-5.

15. Маркин, Д. О. Модель определения местоположения пользователей мобильных устройств внутри помещений на основе сигналов беспроводной сети доступа / Д. О. Маркин, В. В. Комашинский // Перспективные информационные технологии (ПИТ 2015), Том 2: труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2015. – С. 305–309. ISBN 978-5-93424-735-6.

16. Маркин, Д. О. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний / Д. О. Маркин, С. М. Макеев // Известия Тульского государственного университета. Технические науки. – 2016. – No 2. – С. 150–165.

17. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и

защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции [Текст] + [Электронный ресурс] / под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2016. – С. 105–110. ISBN 978-5-89838-886-10.

18. Xin Jin RABAC: Role-Centric Attribute-Based Access Control / Xin Jin, Ravi Sandhu, Ram Krishnan // In MMM-ACNS. – 2012.

19. Девянин, П. Н. Модели безопасности компьютерных систем. Управле- ние доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – Москва : Горячая линия-Телеком, 2013. – 338 с.: ил. ISBN 978- 5-9912-0328-9.

20. Десницкий, В. А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления : автореф. дис. канд. техн.. наук : 05.13.19 / Десницкий Василий Алексеевич ; [Санкт-Петербургский ин-т информатики и автоматизации РАН]. – Санкт-Петербург, 2013. – 22 с. – Библиогр.: с. 21– 22.

21. Озарнов, И. Интеграция сервисов идентификации и контроля доступа. Решение Cisco Identity Services Engine (ISE) / И. Озарнов, Г. Симонов : Презентация доклада, 2012. – 47 с.

22. Салех, Х. М. Мобильные системы предоставления информационных сервисом позиционирования объектов : автореф. дис. ... канд. техн. наук : 05.13.01 / Салех Хади Мухаммед; [Владимирский гос. ун-т]. – Владимир, 2013. – 20 с. – Библиогр.: с. 19–20

23. Сидак, А. А. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи /А. А. Сидак, А. В. Ильин, А. В. Кубарев, // Вопросы кибербезопасности. – 2014. – № 3 (4). – С. 29–34.

24. Чернов, Д. В. О моделях логического управления доступом на основе атрибутов // Математические основы компьютерной безопасности. – 2012. – № 3 (17). – С. 79–82.

25. ViPNet Client для iOS и Android / ОАО "ИнфоТеКС [Електронний ресурс]. – 2019. – Режим доступу: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=2870.

26. ViPNet Terminal / ОАО "ИнфоТеКС" [Електронний ресурс]. – 2019. – Режим доступу: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=5521.

27. Real Time Location System (RTLS) RFID-over-Wi-Fi Technology | Ekahau / Inc. Ekahau // Ekahau [Електронний ресурс]. – 2019. – Режим доступу: http://www.ekahau.com/real-time-location-system/technology.

28. Hur, J. Attribute-based access control with efficient revocation in data out- sourcing systems / J. Hur, D.K. Noh // IEEE Trans. Parallel Distrib.

Syst. – 2011. № 22 (7). – P. 1214–1221.

29. Hybrid WSN and RFID indoor positioning and tracking system / Zhoubing Xiong1, Zhenyu Song1, Andrea Scalera2, Enrico Ferrera2, Francesco Sottile2, Paolo Brizzi2, Riccardo Tomasi2, Maurizio A Spirito2 // EURASIP Journal on Embedded Systems [Електронний ресурс]. – 2019. – Режим доступу: http://jes.eurasipjournals.com/content/2013/1/6.

30. IEEE 802.11, The Working Group Setting the Standards for Wireless / The Institute of Electrical and Electronics Engineers : [Електронний ресурс]. – 2019. – Режим доступу: http://www.ieee802.org/11/.

31. Google Tango Project / Google Inc. [Електронний ресурс]. – 2019. – Режим доступу: https://get.google.com/tango/.

32. Талисман 395 – защищённый телефон стандарта GSM / СовТехКом Ин- формационная безопасность [Електронний ресурс]. – 2019. – Режим доступу: http://www.sovtechcom.ru/product/talisman-395.html.

33. Специальный микросотовый телефон М-549М / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_24.htm.

34. Специальный сотовый телефон SMP-АТЛАС/2 / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_17.htm.

35. Система однонаправленной передачи данных ДИ-ОД / АО ЦНИИ ЭИСУ [Електронний ресурс]. – 2019. – Режим доступу: [Електронний ресурс]. – 2019. – Режим доступу: http://cniieisu.ru/index.php/produsti-i-uslugi/17-produkciya/apparatnoe-obes-pechenie/odnonapravlennyj-informatsionnyj-shlyuz-di-od.

36. Специализированный терминал мобильной связи (СТМС) "Сапфир-К" / НИИ Автоматики Сапфир-К [Електронний ресурс]. – 2019. – Режим доступу: http://niia.ru/document/sapfir.htm.

37. Однонаправленный шлюз "Атликс-Шлюз-К" / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_26.htm.

38. Мобильный вычислительный комплекс "ИНФОПРО" МВК-2 / ЗАО "Инфопро" [Електронний ресурс]. – 2019. – Режим доступу: http://www.infopro.ru/vt.php?id=48.

39. Мобильное защищенное автоматизированное рабочее место доступа в сеть Интернет / ФГУП "НТЦ "АТЛАС"" [Електронний ресурс]. – 2019. – Режим доступу: http://web.stcnet.ru/products_iid_27.htm.

40. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной

системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции / под ред. О.М. Голембиовской, М.Ю

41. Континент Т-10 / Код безопасности [Електронний ресурс]. – 2019. – Режим доступу: http://securitycode.ru/products/kontinent_t_10/.

42. Крипто БД: защита баз данных Oracle // ООО "Алладин Р.Д." [Електронний ресурс]. – 2019. – Режим доступу: https://www.aladdin-rd.ru/catalog/cryptobd/.

43. КАМИ-Терминал / Научно-технический центр КАМИ [Електронний ресурс]. – 2019. – Режим доступу: http://www.kami.ru/ Solutions/КАМИ-Терминал.

44. Инструмент имитационного моделирования AnyLogic [Електронний ресурс]. – 2019. – Режим доступу: http://www.anylogic.ru /overview.

45. Заяц, А. Обзор и тестирование смартфона Caesar A9600, а также знаком- ство с MT6589 - четырехядерной SoC MediaTek для бюджетных решений [Електронний ресурс]. – 2019. – Режим доступу: http://ixbt.com/md/pda/.

46. Груздев, С. Л. Проблемы доверия к импортной электронике на базе ARM-процессоров / С. Л. Груздев // Форум "Технологии безопасности". Красногорск. 7-9 февраля 2017 года : материалы [Електронний ресурс]. – 2019. – Режим доступу: http://new.groteck.ru/images/catalog/ 46978/5cf0f9ab4188375622ef14b54f1b8bfe.pdf.

47. Аппаратура 605 / ОАО "Концерн "Автоматика" [Електронний ресурс]. – 2019. – Режим доступу: http://oaoka.ru/Vremennyj_katalog /Zacshicshennye_telefonnye_apparaty/Apparatura_605.htm.

48. Артамонов, В. А. Безопасность мобильных устройств, систем и приложений // Проект ИТ-защита [Електронний ресурс]. – 2019. – Режим доступу: http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_ Artamonov.pdf.

49. Методичні рекомендації з комерціалізації розробок, створених в результаті науково-технічної діяльності – К.: Наказ Державного комітету України з питань науки, інновацій та інформатики (Лист № 1/06-4-97 від 13.09.2010 р.).

50. Козловський В. О. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт. – Вінниця: ВНТУ, 2012.

51. Козловський В.О. Техніко-економічні обгрунтування та

економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 75 с.

52. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.

53. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

54. ДБН В.2.5-28-2006. Природне і штучне освітлення.

55. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.

56. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

57. ДСН 3.3.6.039-99. Державні санітарні норми виробничої та загальної вібрацій.

58. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.

59. Методичні вказівки до опрацювання розділу "Охорона праці та безпека в надзвичайних ситуаціях" в дипломних проектах і роботах студентів спеціальностей, що пов’язані з функціональною електронікою, автоматизацією та управлінням / Уклад. О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2012. – 64 с.

60. Правила улаштування електроустановок. 2-е вид., перероб. і доп. – Х: "Форт", 2009. – 736 с.

61. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.

62. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.

63. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.

64. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

65. Норми радіаційної безпеки України (НРБУ-97), МОЗ України. – К., 1997.

# ДОДАТКИ

Додаток Б
(обов’язковий)

Типова структура корпоративних мереж з МАП

Додаток В
(обов’язковий)

Структура і топологія системи управління безпекою МАП в корпоративній мережі

Додаток Г
(обов’язковий)

Схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки

Додаток Д
(обов’язковий)

Схема витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні

Додаток Е
(обов’язковий)

Схема доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП

Додаток Є
(обов’язковий)

Схема доступу до інформації з використанням різних конфігурацій МАП

Додаток Ж
(обов’язковий)

Багатоагентна система позиціонування МАП

Додаток З
(обов’язковий)

Схема підсистеми управління конфігурацією МАП

Додаток К
(обов’язковий)

Склад і структура мобільного абонентського пристрою з дублюванням функціональних блоків, що відповідають за обробку інформації в мережах з різними вимогами по захищеності

Додаток Л
(обов’язковий)

Будова захищеного каналу управління на базі протоколу HTTPS

Додаток М
(обов’язковий)

Структурна схема, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв

Додаток А

(обов'язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ ВНТУ,

канд. техн. наук, професор

Г.Г.Бортник

. "__" _____ 2019 р.

**ТЕХНІЧНЕ ЗАВДАННЯ**

на виконання магістерської кваліфікаційної роботи

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ МОБІЛЬНОГО АБОНЕНТСЬКОГО ТЕРМІНАЛУ В КОРПОРАТИВНИХ МЕРЕЖАХ ДОСТУПУ

08-34.МКР.009.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Стальченко О.В.

Виконавець: ст. гр. АРЗ-18м

Стець Д.С.

Вінниця-2019

## 1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 09.12.2019 р.

## 2 МЕТА І ПРИЗНАЧЕННЯ МКР

*Метою* даної магістерської кваліфікаційної роботи є підвищення ймовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг та інформації корпоративних мереж з різними вимогами по захищеності при використанні єдиного МАП.

*Задачами* магістерської кваліфікаційної роботи є:

- розробка технічного завдання;

- аналіз існуючих наукових досліджень і технічних рішень щодо захисту інформації в МАП, а також способів побудови систем захисту інформації при доступі до мереж з різними вимогами по захищеності з використанням єдиного пристрою;

- розробити систему показників якості, що дозволяє оцінити ефективність процесу захисту інформації при експлуатації системи управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності;

- розробити формальну модель безпеки МАП, що відрізняється від відомих урахуванням місцезнаходження МАП в спеціальних приміщеннях, до яких пред'являються підвищені вимоги по ІБ, обгрунтувати її коректність;

- розробити алгоритм управління безпекою МАП, що враховує атрибути доступу користувачів МАП, що включають в себе, в тому числі,

ймовірність знаходження МАП в спеціальному приміщенні, а також вимоги щодо якості послуг, що надаються;

- розробити моделюючий алгоритм і здійснити імітаційне моделювання функціонування системи управління безпекою МАП для отримання оцінки ефективності запропонованих технічних рішень;

- сформувати науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, а також рекомендації щодо вибору параметрів алгоритмів визначення місця розташування МАП в приміщеннях корпоративної мережі і алгоритму обчислення ймовірності знаходження МАП в спеціальному приміщенні.

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

*Предмет дослідження* є моделі та алгоритми управління безпекою МАП.

*Основними завданнями* роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;

- провести аналіз існуючих наукових досліджень і технічних рішень щодо захисту інформації в МАП, а також способів побудови систем захисту інформації при доступі до мереж з різними вимогами по захищеності з використанням єдиного пристрою;

- розробити систему показників якості, що дозволяє оцінити ефективність процесу захисту інформації при експлуатації системи управління безпекою МАП в корпоративних мережах з різними вимогами по захищеності;

- розробити формальну модель безпеки МАП, що відрізняється від відомих урахуванням місцезнаходження МАП в спеціальних приміщеннях, до яких пред'являються підвищені вимоги по ІБ, обгрунтувати її коректність;

- розробити алгоритм управління безпекою МАП, що враховує атрибути доступу користувачів МАП, що включають в себе, в тому числі,

ймовірність знаходження МАП в спеціальному приміщенні, а також вимоги щодо якості послуг, що надаються;

- розробити моделюючий алгоритм і здійснити імітаційне моделювання функціонування системи управління безпекою МАП для отримання оцінки ефективності запропонованих технічних рішень;

- сформувати науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, а також рекомендації щодо вибору параметрів алгоритмів визначення місця розташування МАП в приміщеннях корпоративної мережі і алгоритму обчислення ймовірності знаходження МАП в спеціальному приміщенні;

- аналіз економічної ефективності проведеної розробки;

- дослідження питань безпеки життєдіяльності.

Розроблення офіційного приладу для моделювання безпеки МАП в корпоративних мережах з урахуванням його розташування в спеціальних приміщеннях, а також розробка алгоритму для програмної та апаратної оптимізації конфігурації (безпеки) МАП дозволяє підвищити ймовірність забезпечення безпеки інформації в доступі до інформації та інформації про корпоративні мережі з різними вимогами до безпеки при використанні єдиної карти з урахуванням вимог до ІБ та якості послуг, що надаються в корпоративній мережі.

Дослідження ефективності відомих методів і систем для визначення розташування МАП, коли вони використовуються всередині будівлі в налаштуваннях і обгрунтування оптимальних параметрів алгоритмів для визначення місцезнаходження МАП дозволяє збільшити надійність визначення місцезнаходження МАП в спеціальних приміщеннях.

## 3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах звіту з переддипломної практики “Підвищення інформаційної захищеності мобільного абонентського

терміналу в корпоративних мережах доступу", який виконувався у ВНТУ 2019/2020 н.р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цього звіту.

Список використаних джерел розробки:

3.1 Скляр Б. Цифровая связь. Теоретические основы и применение / Бернард Скляр ; [пер. с англ]. – М.: Изд. Дом "Вильямс", 2003. – 1104 с.

3.2 Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – N 4 (22). – С. 21–31.

3.3 Маркин, Д. О. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – No 10. – С. 40–51.

3.4 Маркин, Д. О. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний / Д. О. Маркин, С. М. Макеев // Известия Тульского государственного университета. Технические науки. – 2016. – No 2. – С. 150–165.

3.5 Положення про кваліфікаційну роботу у Вінницькому національному технічному університеті / Уклад. О. Н. Романюк, Р. Р. Обертюх, Т. О. Савчук, Л. П. Громова – Вінниця : ВНТУ, 2015 – 27 с.

3.6 Кухарчук В.В., Ігнатенко О.Г., Обертюх Р.Р. Методичні вказівки до оформлення дипломних проектів (робіт) для студентів всіх спеціальностей.- В.: ВДТУ, 2002.

3.7 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

3.8 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.9 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.10 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання.- Вінниця:ВНТУ, 2018.- 50 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи АРЗ-18м Стець Д.С.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження розробити науково-технічні пропозиції щодо практичної реалізації системи управління безпекою МАП в корпоративних мережах, що підвищує ймовірність скомпрометованої інформації при приєднані інформації послуги та ресурси в мережах з різними вимогами безпеки при використанні єдиного МАП

Технічні вимоги, яким повинна відповідати розробка, наступні:

- кількість точок доступу для методу трилатерації – 5;
- кількість найблищих «сусідів» для методу k-ближніх сусідів –9;
- крок сітки карти сигнального простору - h=1,5x1,5;
- кількість вимірювань в кожній точці сигнального простору з відомими координатами – 30;
- тривалість пере конфігурації мобільного абонентського пристрою - $4{,}778019376 \cdot 10^{-3}$ с;

- значення ймовірності своєчасного оброблення запиту на обслуговування – 0,9983.

При дослідженні ефективності методів і систем для визначення розташування МАП, коли вони використовуються всередині будівлі в налаштуваннях слід використовувати оптимальні параметри алгоритмів для визначення місцезнаходження МАП, що дозволить збільшити надійність визначення місцезнаходження МАП в спеціальних приміщеннях.

## 6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

| № | Назва та зміст етапу | Термін виконання | | Очікувані результати | Звітна документ-тація |
|---|---|---|---|---|---|
| | | початок | закінчення | | |
| 1. | Розробка технічного завдання (ТЗ) | 02.09.2019р. | 06.09.2019р. | Розроблене ТЗ | Додаток А |
| 2. | Техніко-економічне обґрунтування розробки (ТЕО) | 09.09.2019р. | 13.09.2019р. | Розроблене ТЕО | Вступ. Розділ 1. |
| 3. | Аналіз стану наукових досліджень та технічних рішень в області захисту інформації під час використання мобільних абонентських пристроїв | 16.09.2019р. | 04.10.2019р. | Проведений аналіз | Розділ 2 |
| 4. | Система управління безпекою мобільних абонентських пристроїв | 07.10.2019р | 25.10.2019р. | Розроблений метод | Розділ 3 |

| | | | | | |
|---|---|---|---|---|---|
| 5. | Підвищення імовірності забезпечення безпеки інформації при доступі до інфокомунікаційних послуг і інформації корпоративних мереж з різними вимогами по захищеності під час використання єдиного МАП | 28.10.2019р. | 08.11.2019р. | Характе-ристики і параметри | Розділ 4 |
| 6. | Аналіз економічної ефективності | 11.11.2019р. | 15.11.2019р. | Економічна частина МКР | Розділ 5 |
| 7. | Охорона праці та безпека в надзвичай-них ситуаціях | 18.11.2019р. | 22.11.2019р. | Частина ОТ та БНС | Розділ 6 |
| 8. | Оформлення пояснюв-альної записки (ПЗ) та графічної частини | 25.11.2019р. | 29.11.2019р. | Оформлена документа-ція | ПЗ та графічна частина |
| 9. | Нормоконтроль, попередній захист, рецензування МКР | 02.12. 2019р. | 06.12.2019р. | Позитивні відзиви | Відзив. рецензія |
| 10. | Захист МКР ЕК | | 09.12. 2019р. | Позитивний захист | Протокол ЕК |

## 7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- типова структура корпоративних мереж з МАП;
- структура і топологія системи управління безпекою МАП в корпоративній мережі;
- схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки;
- схема витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні;

- схема доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП;
- схема доступу до інформації з використанням різних конфігурацій МАП;
- багатоагентна система позиціонування МАП;
- схема підсистеми управління конфігурацією МАП;
- склад і структура мобільного абонентського пристрою з дублюванням функціональних блоків, що відповідають за обробку інформації в мережах з різними вимогами по захищеності;
- будова захищеного каналу управління на базі протоколу HTTPS;
- економічна частина МКР;
- розділ ОП та БНС;
- рекомендації щодо подальшого використання розробленої структурної схеми, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв.

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій:

- при дослідженні ефективності відомих методів і систем для визначення розташування МАП, коли вони використовуються всередині будівлі в налаштуваннях і обгрунтовуючи оптимальні параметри алгоритмів для визначення місцезнаходження МАП, що дозволяє збільшити надійність визначення місцезнаходження МАП в спеціальних приміщеннях;
- при впровадженні запропонованих алгоритмів у вигляді набору програм для ЕОМ і для перевірки працездатності їх використання в корпоративній мережі;
- при розробці науково-технічних пропозицій з практичної реалізації системи управління безпекою МАП, підвищення ймовірності підвищення безпеки інформації в доступі до інформації та інформації з корпоративних мереж різні вимоги до безпеки при використанні єдиного МАП.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення ймовірності надання безпеки інформації в експлуатації МАП в корпоративних мережах з різними вимогами до захисту.

## 8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

## 9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

## 10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

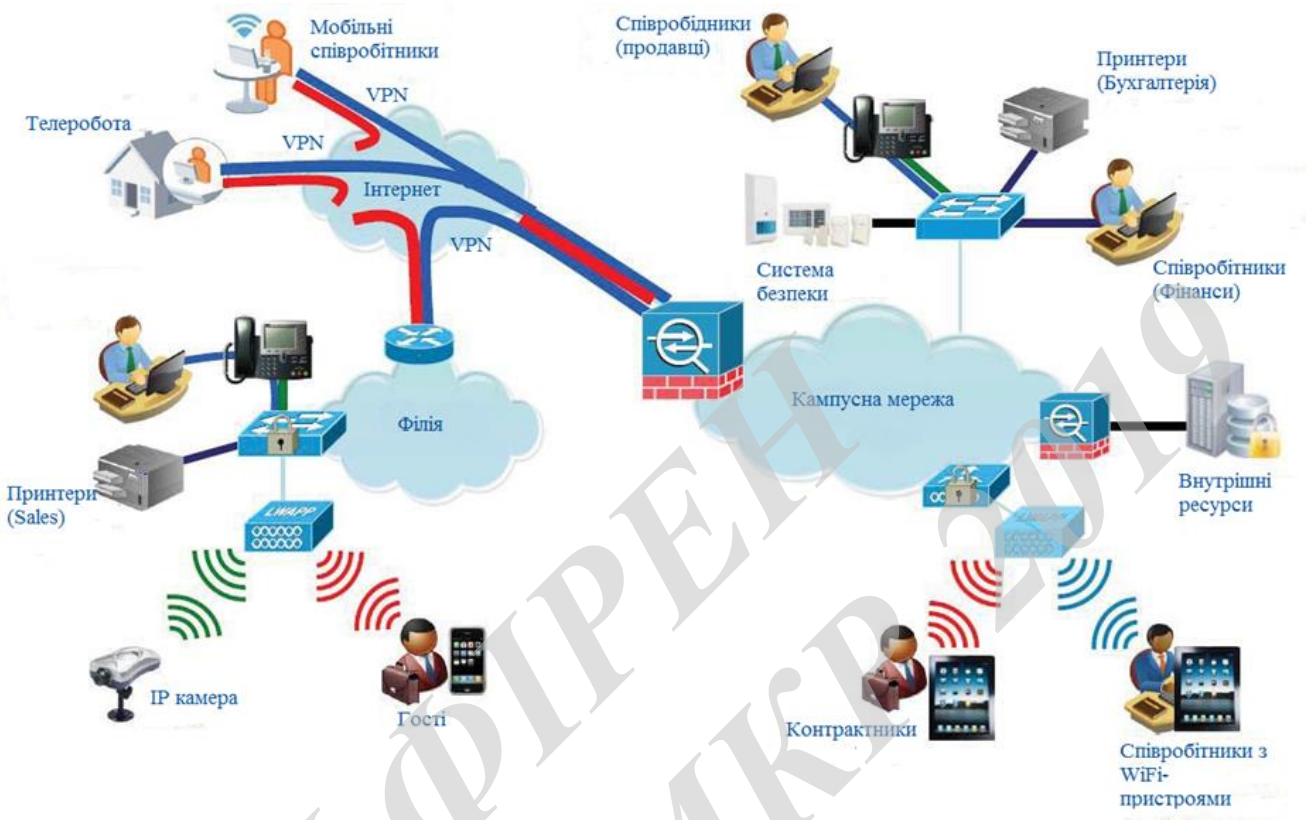
Документація, що розробляється в процесі виконання досліджень повинна містити:

- техніко-економічне обґрунтування розробки;
- структуру і топологію системи управління безпекою МАП в корпоративній мережі;
- схему технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки;
- схему витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні;
- схему доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП;
- схему доступу до інформації з використанням різних конфігурацій МАП;

- багатоагентну систему позиціонування МАП;
- схему підсистеми управління конфігурацією МАП;
- будову захищеного каналу управління на базі протоколу HTTPS;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання розробленої структурної схеми, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв.

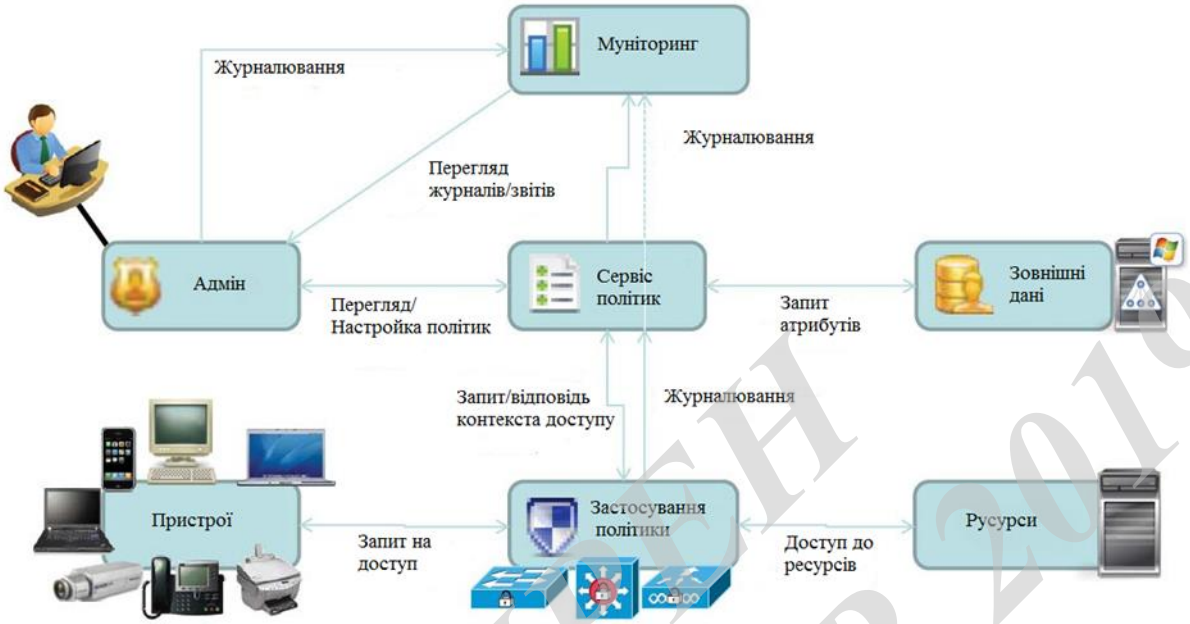
## 11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.






| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Типова структура корпоративних мереж з МАП | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |

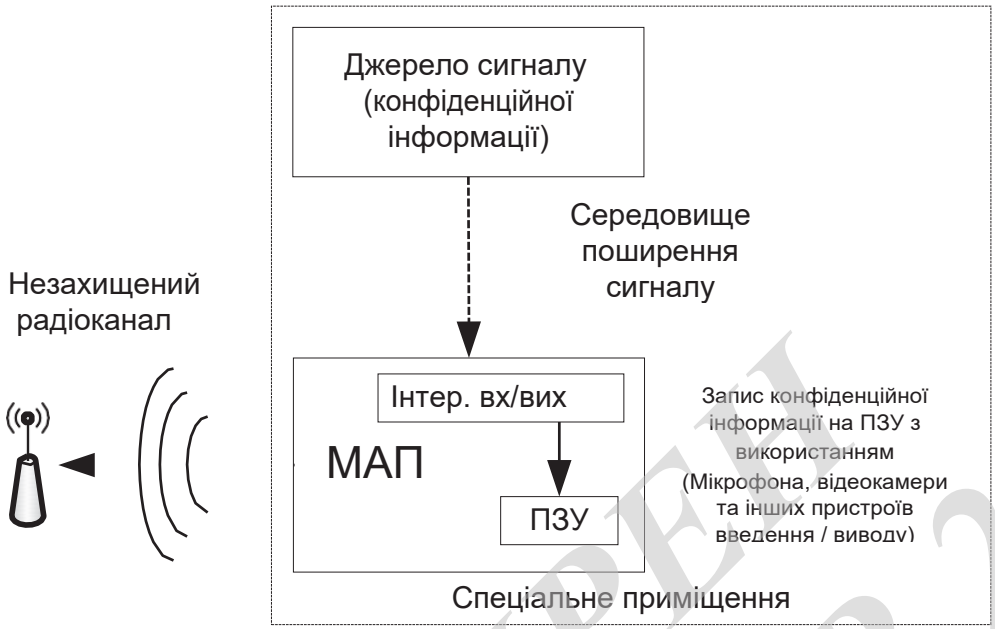





| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | |
| Змн. | Лист | № докум. | Підпис | Дата | | |
| Розроб. | | Стець Д.С. | | | Структура і топологія системи управління безпекою МАП в корпоративній мережі | Літ. / Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | |
| Реценз. | | Коваль Л.Г. | | | | |
| Н. Контр. | | Стальченко О.В. | | | | |
| Затверд. | | Бортник Г.Г. | | | | ВНТУ, гр. АРЗ-18м |

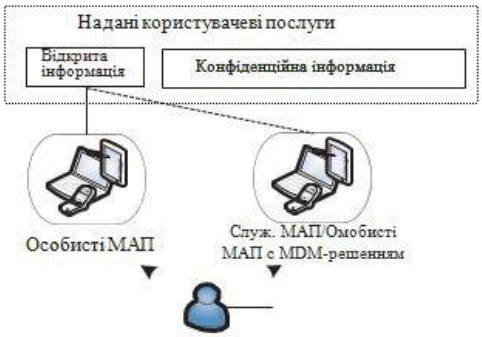



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Схема технічного каналу витоку інформації, що обробляється засобами обчислювальної техніки | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |

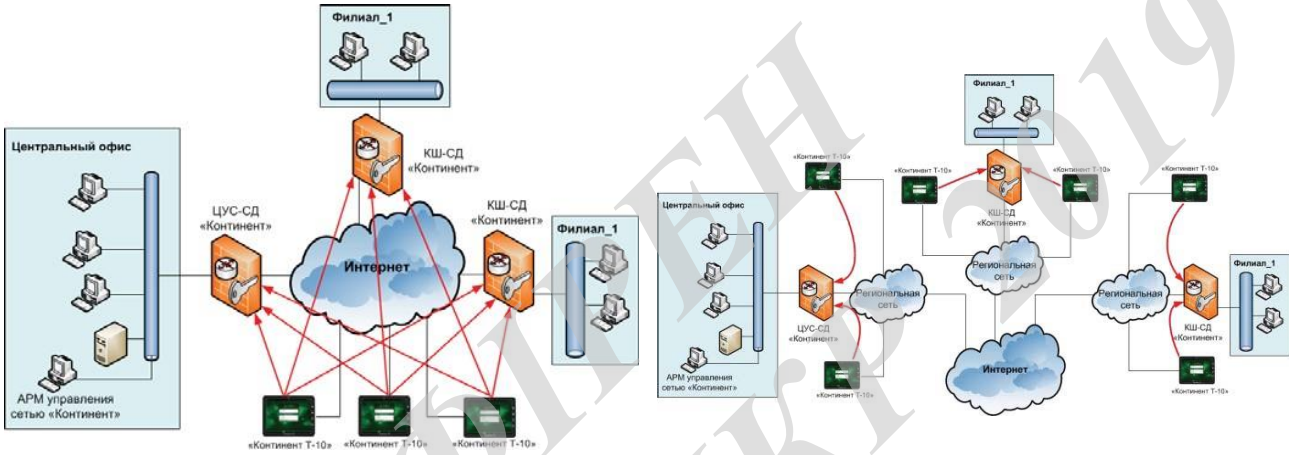




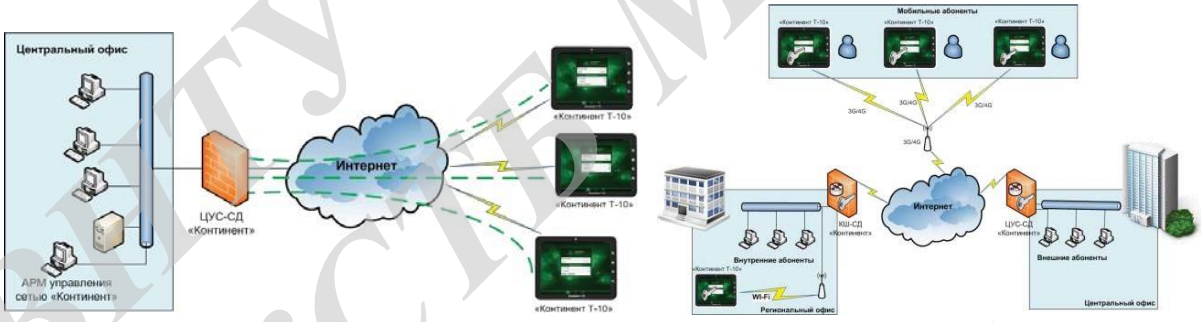

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Схема витоку інформації при несанкціонованому використанні МАП в спеціальному приміщенні | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |




а)




б) в)



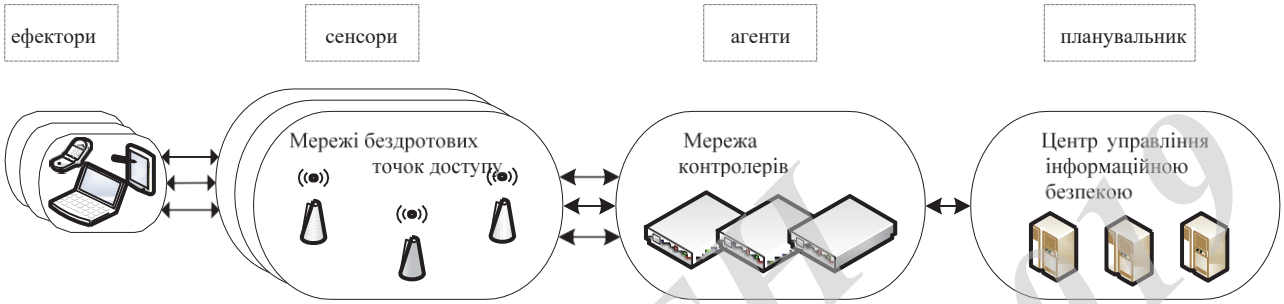

г) д)



| | | | | | 08-34. МКР.009.00.000 Е8 | | |
|---|---|---|---|---|---|---|---|
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Схема доступу в ЗКС до інформації з різним рівнем захищеності при використанні МАП | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Схема доступу до інформації з використанням різних конфігурацій МАП | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |

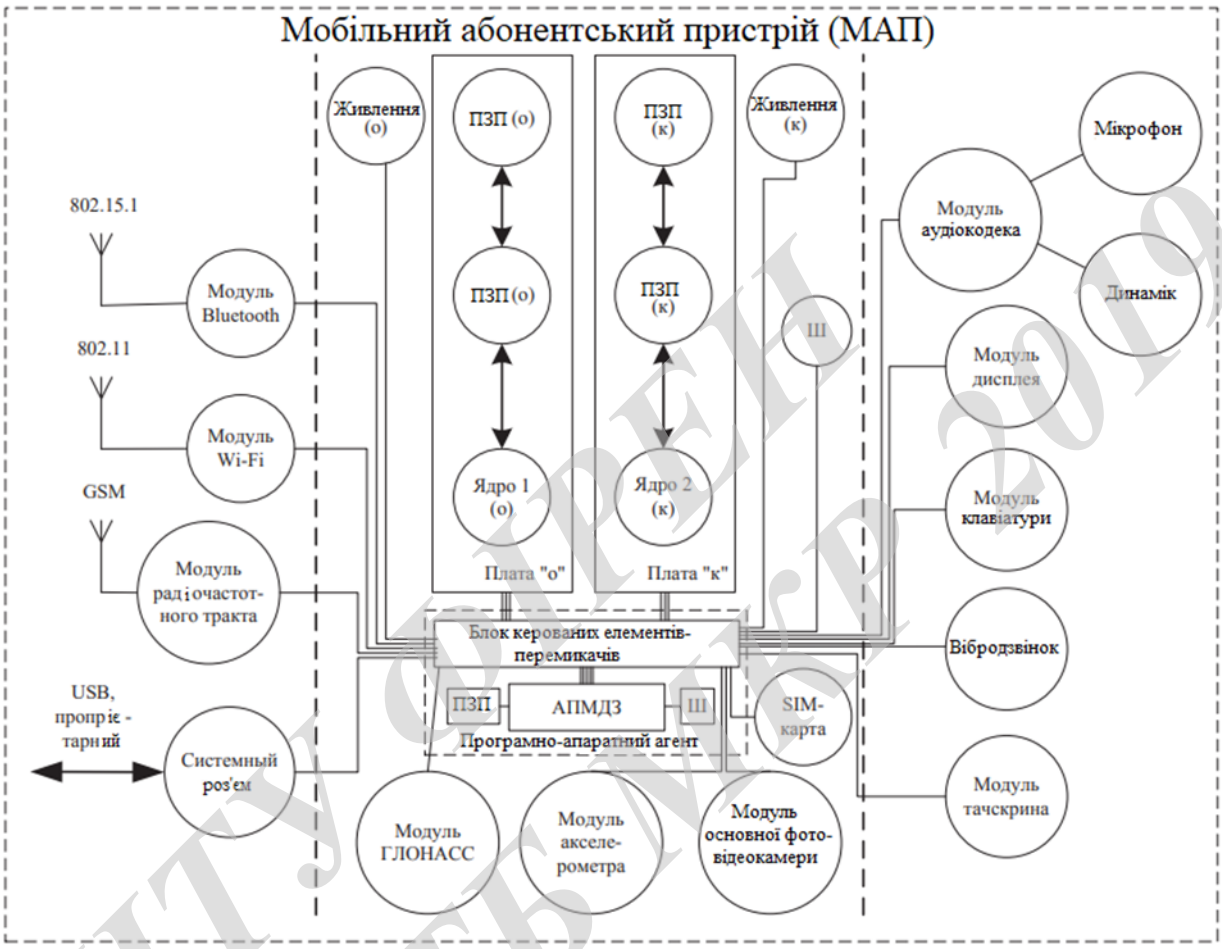





| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Багатоагентна система позиціонування МАП | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |

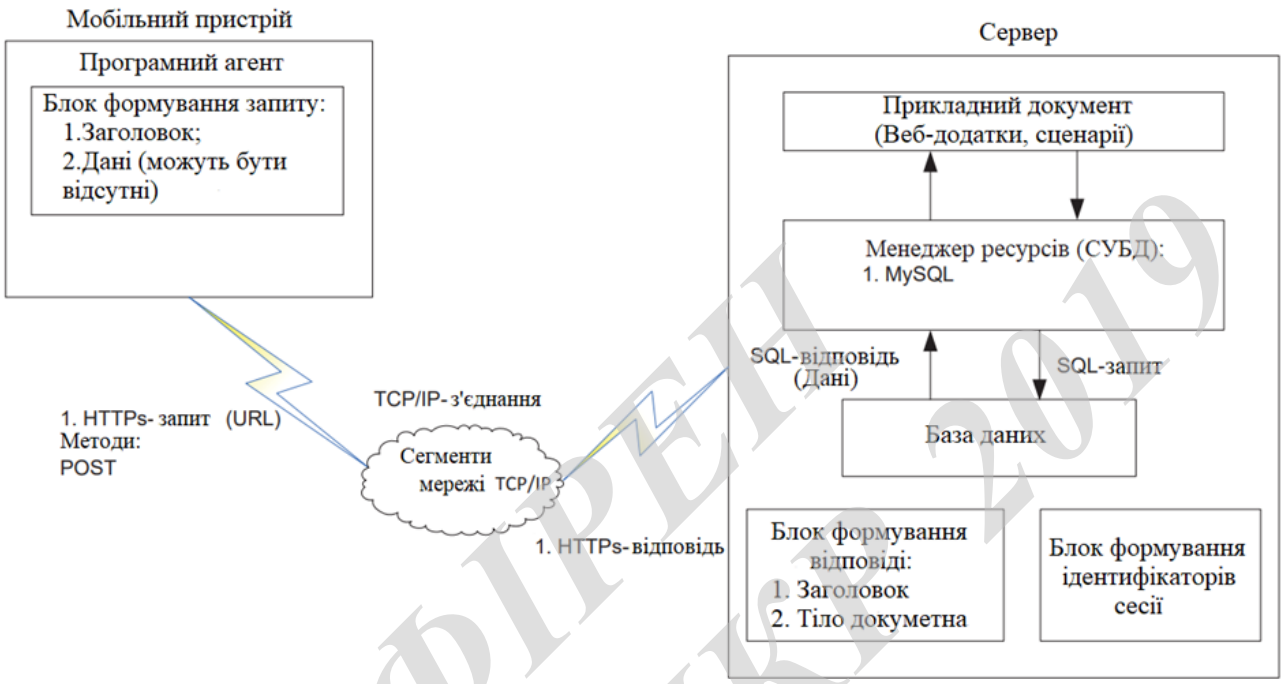



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Схема підсистеми управління конфігурацією МАП | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |



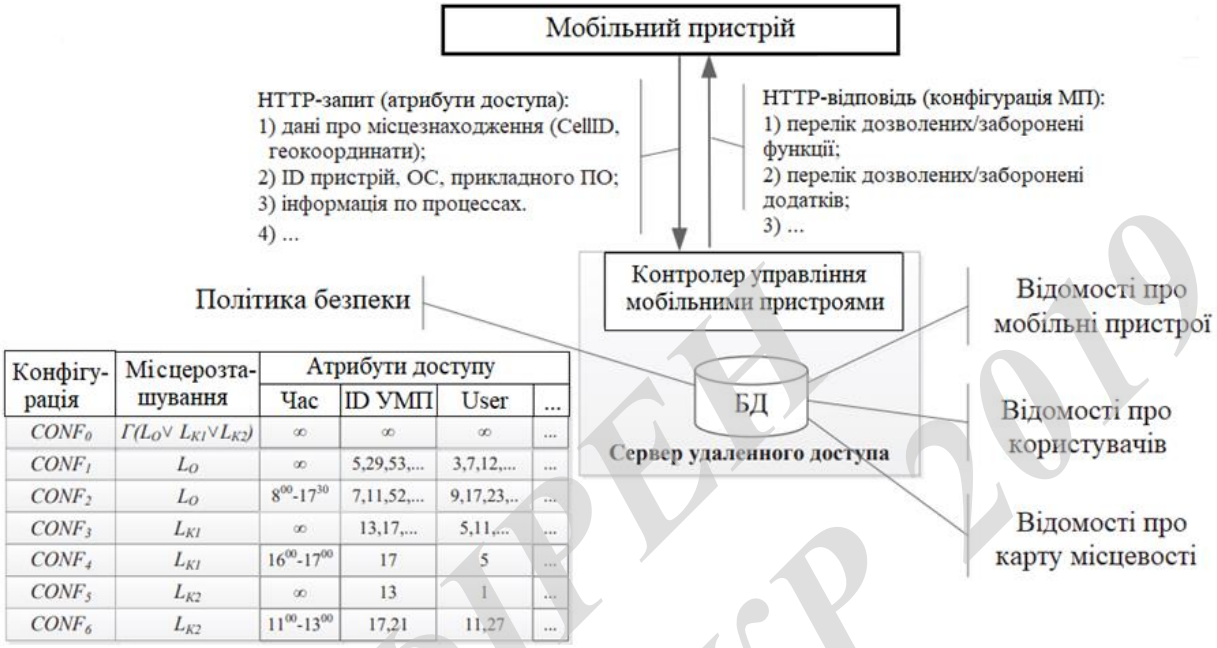



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | | |
| Змн. | Лист | № докум. | Підпис | Дата | | | |
| Розроб. | | Стець Д.С. | | | Склад і структура МАП з дублюванням функціональних блоків, що відповідають за обробку інформації в мережах з різними вимогами по захищеності | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |






| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 08-34. МКР.009.00.000 Е8 | |
| Змн. | Лист | № докум. | Підпис | Дата | | |
| Розроб. | | Стець Д.С. | | | Будова захищеного каналу управління на базі протоколу HTTPS | Літ. / Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м |
| Н. Контр. | | Стальченко О.В. | | | | |
| Затверд. | | Бортник Г.Г. | | | | |




| Конфігу-рація | Місцерозта-шування | Атрибути доступу | | | |
|---|---|---|---|---|---|
| | | Час | ID УМП | User | ... |
| $CONF_0$ | $\Gamma(L_O \vee L_{K1} \vee L_{K2})$ | ∞ | ∞ | ∞ | ... |
| $CONF_1$ | $L_O$ | ∞ | 5,29,53,... | 3,7,12,... | ... |
| $CONF_2$ | $L_O$ | $8^{00}$-$17^{30}$ | 7,11,52,... | 9,17,23,.. | ... |
| $CONF_3$ | $L_{K1}$ | ∞ | 13,17,... | 5,11,... | ... |
| $CONF_4$ | $L_{K1}$ | $16^{00}$-$17^{00}$ | 17 | 5 | ... |
| $CONF_5$ | $L_{K2}$ | ∞ | 13 | 1 | ... |
| $CONF_6$ | $L_{K2}$ | $11^{00}$-$13^{00}$ | 17,21 | 11,27 | ... |



| Змн. | Лист | № докум. | Підпис | Дата | 08-34. МКР.009.00.000 Е8 | | |
|---|---|---|---|---|---|---|---|
| Розроб. | | Стець Д.С. | | | Структурна схема, що реалізує взаємозв'язок мобільного пристрою і віддаленого сервера доступу мобільних пристроїв | Літ. | Арк. 1 / Аркушів 1 |
| Перевір. | | Стальченко О.В. | | | | | |
| Реценз. | | Коваль Л.Г. | | | | ВНТУ, гр. АРЗ-18м | |
| Н. Контр. | | Стальченко О.В. | | | | | |
| Затверд. | | Бортник Г.Г. | | | | | |