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

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Забезпечення інформаційної безпеки сенсорних мереж»

Виконав: студент 2-го курсу,
групи ТКС-20м
спеціальності 172 – Телекомунікації та радіотехніка

_____ Замрій О.В.

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

«____» _____ 2021 р.

Опонент: д.т.н., професор, зав.каф.РТ
Осадчук О.В.
_____

«____» _____ 2021 р.

Допущено до захисту
Завідувач кафедри ТКСТБ
_____ д.т.н., проф. Кичак В.М.
«____» _____ 2021 р.

Вінниця ВНТУ - 2021 рік

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
д.т.н., проф В.М. Кичак

"___" _____2021 року

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

Замрію Олегу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Забезпечення інформаційної безпеки сенсорних мереж

керівник роботи Семенова Олена Олександрівна, к. т. н, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "24" 09 2021 року № 277
2. Строк подання студентом роботи 01 грудня 2021 року

3. Вихідні дані до роботи: частота 2,4 ГГц; кількість вузлів – 9; потужність передачі від 0 … –5 дБм; чутливістю приймання – 95 дБм; швидкість передавання – 250 кбіт/с; енергоспоживання вузла – не вище 60 мВт.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) вступ; огляд принципів побудови та функціонування сенсорних мереж; аналіз шляхів забезпечення інформаційної безпеки сенсорних мереж; підвищення інформаційної безпеки сенсорних мереж; економічна частина; охорона праці та безпека в надзвичайних ситуаціях; висновки; література; додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1) Класифікація сенсорних мереж. 2) Методи виявлення атак. 3) Механізм виявлення вторгнень. 4) Класифікація протоколів управління ключами. 5) Захищена передача пакетів ZigBee. 6) Вузол сенсорної мережі. 7) Функціональна схема вузла сенсорної мережі. 8) Залежність потужності сигналу від подоланої відстані. 9) Залежність якості зв'язку від розмірів охопленої території. 10) Використання прискорюючої лінзи. 11) Нейронна мережа.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Технічна частина	Семенова О.О., доцент каф. ТКСТБ		
Економічна частина			
Охорона праці та безпека в надзвичайних ситуаціях			

7. Дата видачі завдання 01 вересня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	10.09.2021р.	
2.	Техніко-економічне обґрунтування розробки	17.09.2021р.	
3.	Огляд особливостей захисту інформації	01.10.2021р.	
4.	Дослідження роботи мережі	29.10.2021р.	
5.	Розроблення методів захисту мережі	19.11.2021р.	
6.	Аналіз економічної ефективності розробки	30.11.2021р.	
7.	Аналіз безпеки життєдіяльності, цивільний захист	06.12.2021р.	
8.	Оформлення пояснювальної записки та графічної частини	13.12.2021р.	
9.	Нормоконтроль МКР	14.12.2021р.	
10.	Попередній захист МКР, рецензування МКР	17.12.2021р.	
11.	Захист МКР ДЕК	20.12.2021р.	

Студент _____ Замрій О. В.
(підпис)

Керівник роботи _____ Семенова О.О.
(підпис)

АНОТАЦІЯ

УДК 621.396

Замрій Олег Володимирович. Забезпечення інформаційної безпеки сенсорних мереж. Магістерська кваліфікаційна робота. – Вінниця: ВНТУ, 2021. – 138с.

На українській мові. Бібліогр.: 31 назв; Рис.:30; Табл.: 20.

Магістерська робота присвячена розробленню та дослідженню методів підвищення ефективності захисту інформації у сенсорних мережах. У роботі проаналізовано сучасні методи підвищення інформаційної безпеки. Обгрунтовано новітні технології інформаційної безпеки. Розраховано економічний ефект. Розглянуті питання безпеки життєдіяльності та охорони праці. Отримані результати задовольняють вимогам технічного завдання.

Ключові слова: сенсорна, мережа, захист, атака, інформація

ABSTRACT

UDK 621.396

Zamrii Oleh Volodymyrovych. Providing the information security of sensor networks. Master thesis. – Vinnytsya: VNTU, 2021. – 138pp.

In Ukrainian language. Refs.: 31 titles; figs.: 30; tables: 20.

The master thesis is dedicated to developing and researching the methods of information security efficiency increasing in sensor networks. In this thesis modern methods of information security efficiency increasing have been analyzed. The novel technologies of functional security have been substantiated. The economic gain has been calculated. Problems of industrial and occupational safety have been considered. The obtained results satisfy preliminary specifications.

Keywords: sensor, network, protection, attack, information.

ЗМІСТ

ВСТУП

Актуальність теми. Безпровідна сенсорна мережа складається з великої кількості малих пристроїв, тобто вузлів, кожен з яких має сенсор, процесор і обладнання, необхідне для комунікації. Завдання таких пристроїв полягає у моніторингу навколишнього середовища. Їх можна використовувати у таких областях, як медичний моніторинг, управління електроенергією, управління логістикою ізапасами, а також моніторинг поля боя.

Сенсорні мережі встановлюються на великих відкритих територіях, там, де людині досить складно дістатися, або де умови роботи є екстремальними для електронних пристроїв. Розроблено безліч додатків для сенсорних мереж, розгорнутих у офісах, житлових будинках, заводах, або на відкритій території.

Через значні технічні обмеження, які накладаються на вузли мережі, а також через встановлення у віддалені райони, безпровідні сенсорні мережі є дуже вразливими до великої кількості загроз інформаційній безпеці, таких як блокування доступності інформації та спотворення інформації. У випадках, коли подібні сенсорні мережі використовуються в критично важливих сферах, ця проблема може становити серйозну загрозу. Ще один приклад реальної загрози – виробничий шпіонаж, тобто коли атака спрямовується на сенсорну мережу, розгорнуту на заводі для управління виробничими процесами.

Окрім традиційних проблем безпеки, таких як безпечна маршрутизація іагрегація даних, у сенсорних мережах застосовуються механізми безпеки, що також включають комунікацію між вузлами. На практиці сенсори не можуть бути підключені до мережі лише на базі апріорної довіри. Тому наразісважливоим є створення та дослідження моделей реєстрації сенсорів у мережі, що дозволить вирішувати задачі, які неможливо розв’язати за допомогою традиційних криптографічних механізмів.

Стримкий розвиток та впровадження безпровідних технологій призвели до значного зростання кількості як пристроїв, так і користувачів. Збільшення числа різноманітних безпровідних мереж призвело до взаємного впливу їх одна

на одну, а збільшення кількості абонентів в умовах обмежених частотних діапазонах спричинило часті випадки міжканальної та просторової інтерференції. В свою чергу, це чинить вплив на пропускну здатність каналів, на їх працездатність, на захисту мереж від несанкціонованого кібернетичного впливу.

Аналіз останніх досліджень. Дослідженню проблем інформаційної безпеки мереж безпровідного зв'язку присвячено праці вчених: Д. В. Агеєва, В. М. Астапені, В. М. Богуша, В. Л. Бурячка, В. В. Домарева, А. Карлсона, О. Г. Корченка, Г. Т. Маркова, М. В. Степашкина, С. В. Толюпи, В. О. Хорошка та Я. С. Шифрина та багатьох інших [1-3].

Мета та задачі дослідження. Метою даної магістерської кваліфікаційної роботи є дослідження механізмів забезпечення інформаційної безпеки у сенсорних мережах.

Для досягнення мети потрібно розв'язати такі задачі:

- аналіз принципів забезпечення інформаційної безпеки у сенсорних мережах;
- аналіз проблемних місць у механізмах безпеки та способи їх подолання;
- синтез методів підвищення інформаційної безпеки у сенсорних мережах.

Об'єктом дослідження є сенсорні мережі безпровідного зв'язку.

Предметом дослідження є інформаційна безпека в сенсорних мережах безпровідного зв'язку.

Методи дослідження. Для рішення поставлених завдань були використані методи теорії телетрафіку, теорії інформації та передавання сигналів, апарат нейронних мереж.

Новизна одержаних результатів полягає у наступному:

- обгрунтовано механізм виявлення вторгнень;
- запропоновано метод ідентифікації пристрою;
- розроблено функціональну схему вузла сенсорної мережі.

Особистий внесок здобувача: розроблено рекомендації до підвищення інформаційної безпеки сенсорних мереж.

1 ОГЛЯД ПРИНЦИПІВ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СЕНСОРНИХ МЕРЕЖ

1.1 Архітектура сенсорних мереж

Безпровідні сенсорні мережі (англ. WSN – Wireless Sensor Network) складаються з мініатюрних обчислювальних пристроїв – мотів, забезпечених сенсорами (датчиками температури, тиску, освітленості, рівня вібрації, розташування тощо) і трансиверами, що працюють у заданому радіодіапазоні. Гнучка архітектура, зниження витрат при монтажі виділяють безпровідні мережі інтелектуальних датчиків серед інших безпровідних і провідних інтерфейсів передачі даних, особливо коли йдеться про велику кількість з'єднаних між собою пристроїв, сенсорна мережа дозволяє підключати до 65 000 пристроїв [1]. Постійне зниження вартості безпровідних рішень, підвищення їх експлуатаційних параметрів дозволяють поступово переорієнтуватися з провідних рішень у системах збору телеметричних даних, засобів дистанційної діагностики, обміну інформацією. «Сенсорна мережа» є сьогодні усталеним терміном (англ. Sensor Networks), що позначає розподілену, самоорганізовану, стійку до відмови окремих елементів мережу з пристроїв, що не обслуговуються і не вимагають спеціальної установки. Кожен вузол сенсорної мережі може містити різні датчики для контролю зовнішнього середовища, мікрокомп'ютер та радіоприймач. Це дозволяє пристрою проводити вимірювання, самостійно проводити початкову обробку даних та підтримувати зв'язок із зовнішньою інформаційною системою.

Технологія ретрансльованого ближнього радіозв'язку 802.15.4/ZigBee [2], відома як «Сенсорні мережі», є одним із сучасних напрямків розвитку самоорганізованих відмовностійких розподілених систем спостереження та управління ресурсами та процесами. Сьогодні технологія безпровідних сенсорних мереж є єдиною безпровідною технологією, за допомогою якої можна вирішити завдання моніторингу та контролю, які критичні до часу роботи датчиків. Об'єднані в

безпровідну сенсорну мережу датчики утворюють територіально-розподілену систему збору, обробки і передачі інформації, що самоорганізується. Основною сферою застосування є контроль та моніторинг вимірюваних параметрів фізичних середовищ та об’єктів.

Прийнятий стандарт IEEE 802.15.4 [3] описує контроль доступу до безпровідного каналу та фізичний рівень для низькошвидкісних безпровідних персональних мереж, тобто два нижні рівні відповідно до мережної моделі OSI. «Класична» архітектура сенсорної мережі заснована на типовому вузлі, який включає:

• радіотракт;

• процесорний модуль;

• елемент живлення;

• різні датчики.

Архітектура типової сенсорної мережі подана на рис.1.1.

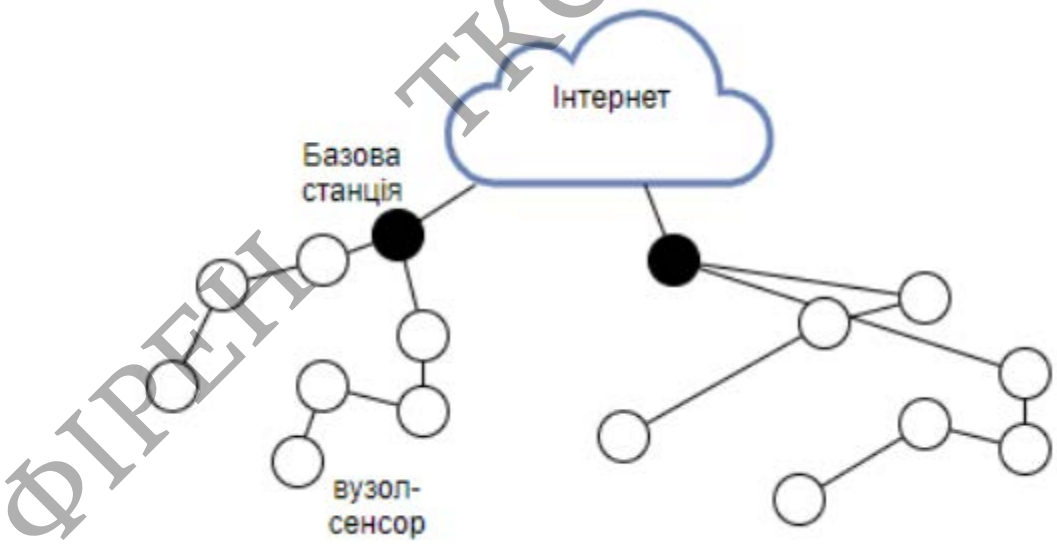


Рисунок 1.1 – Архітектура типової сенсорної мережі

Використання в типовому вузлі сенсорної мережі як датчика другого трансивера, відповідного стандарту ISO 24730-5, дозволяє використовувати сенсорну мережу не тільки для моніторингу параметрів середовищ і об’єктів, але і для визначення місцезнаходження та моніторингу пересувань об’єктів, забезпе-

чених спеціальними радіочастотними мітками. Створена з таких вузлів сенсорна мережа утворює безпровідну інфраструктуру RTLS.

Типовий вузол може бути представлений трьома типами пристроїв:

• мережевий координатор (FFD – Fully Function Device);

• здійснює глобальну координацію, організацію та встановлення параметрів мережі;

• найбільш складний із трьох типів пристроїв, що потребує найбільшого обсягу пам’яті та джерела живлення;

• пристрій з повним набором функцій (FFD – Fully Function Device);

• підтримка 802.15.4;

• додаткова пам’ять та енергоспоживання дозволяє виконувати роль координатора мережі;

• підтримка всіх типів топологій («точка-точка», «зірка», «дерево», «чарункова мережа»);

• здатність виконувати роль координатора мережі;

• здатність звертатися до інших пристроїв у мережі;

• пристрій з обмеженим набором функцій (RFD – Reduced Function Device);

• підтримує обмежений набір функцій 802.15.4;

• підтримка топологій «точка-точка», «зірка»;

• не виконує функції координатора;

• звертається до координатора мережі та маршрутизатора;

1.2 Платформи сенсорних мереж

Через відсутність чіткої стандартизації у сенсорних мережах, існує кілька різних платформ. Всі платформи відповідають основним базовим вимогам до сенсорних мереж: мала споживана потужність, тривалий час роботи, малопотужні приймачі та наявність сенсорів. До основних платформ можна віднести MicaZ, TelosB, Intel Mote 2.

Рисунок 1.2 – Типовий вузол MicaZ

Характеристики типового вузла MicaZ:

• мікропроцесор: Atmel ATmega128L;

• 7,3728 МГц частота;

• 128 Кб флеш-пам’яті для програм;

• 4 Кб SRAM для даних;

• 2 UART’s;

• SPI шини;

• I2C шина;

• радіо: ChipCon CC2420;

• зовнішня флеш-пам’ять: 512 Кб;

• 51-pin додатковий конектор;

• вісім 10-бітових аналогових I/O;

• 21 цифрових I/O;

• три програмованих LEDs;

• JTAG порт;

• живлення від двох батарей AA

• мікропроцесор: MSP430 F1611;

• 8 МГц частота;

• 48 Кб флеш-пам’яті для програм;

• 10 Кб RAM для даних;

• UART;

• SPI шини;

• вбудований 12-бітовий ADC/DAC;

• DMA контролер;

• радіо: ChipCon CC2420;

• зовнішня флеш-пам’ять: 1024 Кб;

• 16-pin додатковий конектор;

• три програмованих LEDs;

• JTAG порт;

• опціонально: Сенсори освітленості, вологості, температури;

• живлення від двох батарей AA.Mote 2;

• 320/416/520 МГц PXA271 XScale мікропроцесор;

• 32 Мбайта Флеш-пам’яті;

• 32 Мбайт ОЗУ;

• mini-USB інтерфейс;

• I-Mote2 конектор для зовнішніх пристроїв (31+21 pin);

• радіо: ChipCon CC2420;

• світлодіодні індикатори;

• живлення від трьох батарей AAA.

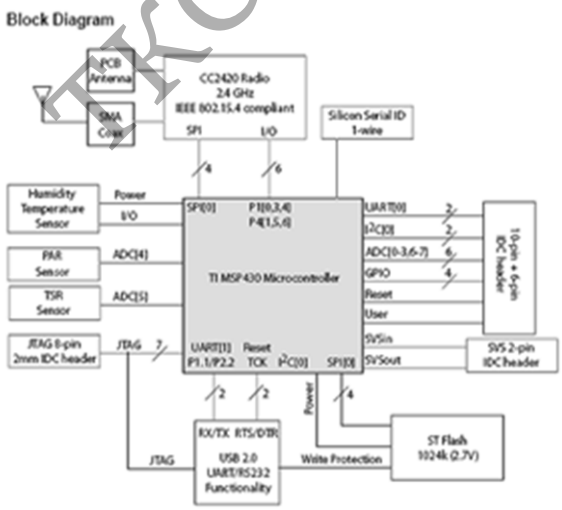


Рисунок 1.3 – Типова схема вузла TelosB

Рисунок 1.4 – Плата Intel Mote 2

Основним стандартом передачі даних у сенсорних мережах є IEE802.15.4, які спеціально було розроблено для безпровідних мереж з малопотужними приймачами.

Жодних стандартів у галузі програмного забезпечення в сенсорних мережах немає. Існує кілька сотень різних протоколів обробки та передачі даних, а також систем керування вузлами. Найбільш поширеною операційною системою є система з відкритим кодом – TinyOs. Багато розробників часто пишуть свою систему управління, часто мовою Java. Програма керування сенсорного вузла під керуванням операційної системи TinyOs пишеться мовою nesC.

1.3 Алгоритми сенсорних мереж

Будь-яке середовище передачі (радіоефір, Ethernet тощо) обмежене через те, що одночасно ним може скористатися лише один або обмежена кількість користувачів.

Протоколи канального рівня (MAC – Medium Access Control) займаються управлінням доступу до єдиного середовища передачі даних.

Класифікація MAC протоколів [3,7]:

• Протоколи на основі конкуренції

• Вузли конкурують за доступ до середовища передачі

• Приклади: ALOHA (Pure and Slotted), CSMA

• Протоколи за розкладом

• Вузли передають у різних підканалах

• Приклади: FDMA, TDMA, CDMA

Властивості MAC протоколів:

• Уникнення колізій – основне завдання MAC протоколів;

• Енергетична ефективність – важлива властивість у сенсорних мережах. MAC контролює трансивер;

• Масштабованість та адаптивність – MAC протоколи повинні вміти адаптуватися;

• Ефективність використання каналу – це важливо в сенсорних мережах.

• Затримка – важливість залежить від конкретної програми;

• Пропускна здатність – залежить від програм-додатків;

• Справедливість – сенсорні мережі можуть мати неоднорідний розподіл трафіку.

Найбільш важливими факторами в сенсорних мережах є енергетична ефективність, уникнення колізій та адаптивність.

Енергетична ефективність – один із найголовніших факторів у сенсорних мережах. Основні джерела втрат енергії:

• Колізії – атрибут «конкурентних» протоколів;

• Пасивне прослуховування каналу – для малопотужних трансиверів, витрати енергії на прийом повідомлення можуть бути більшими ніж на його передачу;

• Overhearing – може бути домінуючим фактором при великому навантаженні та щільності вузлів;

• Control Packet Overhead – зменшують ефективну goodput.

• Розглянемо найбільш популярні. MAC: Co-ordinated Adaptive Sleeping. Комбінування основних переваг протоколів «за розкладом» (TDMA) та «конкурентних» протоколів (CSMA). Синхронізований розклад. Розклад підібрано таким чином, що коли вузли хочуть передати інформацію, вони прокидаються синхронно. Несинхронізована передача. Коли вузол прокинувся та хоче передати інформацію, він робить це за допомогою алгоритму CSMA/CA.

Основний компроміс: жертвуючи затримками/справедливістю, покращуємо енергетичну ефективність. S-MAC намагається зменшити витрати енергії за рахунок:

• Пасивний прийом – періодичне засипання.

• Колізії – використання RTS/CTS

• Overhearing – вимкнення радіо, коли передача не призначається для цього вузла.

• Службові пакети – надсилання повідомлень

Переваги:

• Значно ефективніший за звичайний CSMA/CA;

• Планує час сну та час активності для забезпечення енергетично ефективної передачі задовільних затримок.

Недоліки:

• Алгоритмічно складніше;

• Істотні витрати на організацію (розклад);

• Комбінує виявлення несучої, RTS/CTS та засипання за розкладом в один MAC протокол, що може перешкодити при оптимізації під конкретні програми.

B-MAC: Versatile Low-power medium access for sensor networks.

Поділ канального рівня та контролю доступу до середовища, дає кращу оптимізацію під конкретні програми. Сон без розкладу (Unscheduled sleep). Зменшує кількість службової інформації. Але на передачу потрібно більше зусиль, щоб пробудити приймач від сну. Пробудження без розкладу (Unscheduled wakeup). Часові інтервали між пробудженнями дуже короткі. Може бути використаний CSMA/CA або інші app-specific алгоритми.

2 АНАЛІЗ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕНСОРНИХ МЕРЕЖ

2.1 Забезпечення інформаційної безпеки у сенсорних мережах

2.1.1 Вимоги до забезпечення інформаційної безпеки у сенсорних мережах

Мета служб безпеки сенсорних мереж полягає у захисті даних та ресурсів вузлів від кібератак і некоректного функціонування. Вимоги до інформаційної безпеки сенсорної мережі наступні:

• Доступність інформації, яка гарантує працездатність необхідних мережевих сервісів навіть при відмові в обслуговуванні (DoS – атака) [12];

• Авторизація, яка гарантує, що лише авторизовані та довірені вузли мережі можуть отримувати інформацію про надання мережевих послуг;

• Аутентифікація, яка гарантує, що повідомлення, які передаються від одного вузла до іншого є справжньою – вузол «зловмисник» не може замаскуватися під довірений вузол мережі;

• Конфіденційність, яка гарантує, що кожне повідомлення в мережі буде прочитане лише тим користувачем, якому воно призначалося;

• Цілісність інформації, яка гарантує, що надіслане повідомлення не було змінено проміжним вузлом «зловмисником»;

• Суворе виконання зобов’язань, що означає, що вузол-передавач не може заперечувати надсилання повідомлення;

• Принцип новизни даних, який передбачає, що всі отримані дані є актуальними, гарантуючи невідтворюваність застарілих даних зловмисником.

Більш того, у рамках припущення про впровадження нових вузлів у мережу, а також виходу з ладу старих, припускаємо, що має виконуватися збереження прямої та зворотної секретності:

• Пряма секретність – сенсорний вузол не може прочитати будь-які наступні повідомлення, після того, як він перестане бути користувачем цієї мережі.

• Зворотна секретність – сенсорний вузол, що впроваджується в мережу, не повинен мати можливості прочитати будь-які раніше передані повідомлення в мережі.

Служби забезпечення інформаційної безпеки в сенсорних мережах, як правило, зосереджені навколо криптографічних методів. Тим не менш, через обмеження розглянутої технології, багато вже існуючих надійних алгоритмів забезпечення інформаційної безпеки не практичні для використання. Основні вимоги інформаційної безпеки у сенсорних мережах подано на рис.2.1.

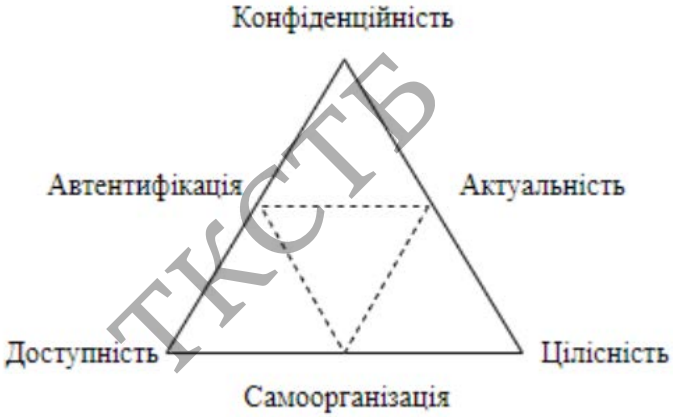


Рисунок 2.1 – Вимоги інформаційної безпеки у сенсорних мережах

2.1.2 Модель загроз у сенсорній мережі

Модель загроз сенсорної мережі передбачає наявність відомостей у зловмисника щодо механізмів захисту інформаційної безпеки, що використовуються у розгорнутій сенсорній мережі;

Розглянуті умови можуть поставити під загрозу як кібербезпеку вузла, так і його фізичне захоплення зловмисником. Через високу вартість розгортання стійких до несанкціонованого втручання сенсорних вузлів, більшість пристроїв розглядаються як нестійкі до злому. Важливо відзначити, що як тільки зловмисник отримує контроль над вузлом мережі – він отримує доступ до кри-

тично важливої інформації, що зберігається в цьому пристрої, для подальшого використання в корисливих цілях.

Базові станції в сенсорній мережі вважаються заслуговують на довіру, оскільки є більш потужними пристроями і в більшості випадків не схильні до проблематики простих сенсорних вузлів.

На сьогоднішній день, більшість наукових досліджень та розробок зосереджені на безпечній маршрутизації між датчиками та базовою станцією. Так у роботі [5], розглянуті загрози, які можуть призвести до виведення з ладу базової станції мережі.

Атаки в сенсорній мережі можуть бути класифіковані на наступні категорії:

• Зовнішні та внутрішні атаки: зовнішні атаки ініційовані шкідливими вузлами, які не належать до сенсорної мережі; внутрішні атаки відбуваються через некоректну і неавторизовану роботу легітимних вузлів сенсорної мережі;

• Пасивні та активні атаки: пасивні атаки включають дії зловмисника, пов’язані з підслуховуванням або моніторингом пакетів даних, що передаються в сенсорній мережі; активні атаки включають перехоплення і модифікацію даних або створення помилкового інформаційного потоку;

• Атаки mote та laptop класів: у класі mote-атак зловмисник використовує кілька вузлів, можливості яких аналогічні використовуваним сенсорним вузлам, щодо атаки; атаки laptop класу мають на увазі використання більш потужних пристроїв, наприклад, ноутбуків, для організації шкідливих дій у сенсорній мережі. Ці пристрої мають більш потужну передачу даних, обчислювальну потужністю, а також великі енергоресурси порівняно із сенсорними вузлами.

2.1.3 Основні групи та типи загроз в сенсорних мережах

Сенсорні мережі є уразливими для більшості різних типів атак. Спираючись на вимоги щодо забезпечення інформаційної безпеки в сенсорних мережах, ці атаки можуть бути класифіковані наступним чином:

• Атаки на секретність та аутентифікацію: стандартні криптографічні методи можуть забезпечити секретність та справжність каналів зв'язку мережі від зовнішніх атак, таких як, підслуховування, атаки відтворення та модифікації або заміни пакетів даних;

• Атаки на доступність мережі: атаки на доступність мережі часто визначаються як атаки відмови в обслуговування (DOS-атаки), які можуть бути спрямовані в будь-який шар сенсорної мережі;

• Приховані атаки на порушення цілісності інформації: у розглянутому типі атак метою зловмисника є впровадження в мережу хибних потоків даних. Наприклад, зловмисник компрометує вузол мережі та змінює або додає до потоку даних хибну інформацію.

Для більшості розглянутих атак (рис. 2.1), збереження працездатності мережі для проведення подальших маніпуляцій із даними має ключове значення. DOS-атаки в сенсорній мережі, при використання цієї технології в галузі охорони здоров'я, можуть призвести до шкоди здоров'ю та безпеки людей [2].

2.1.4 Показники для оцінювання методів забезпечення безпеки

Класифікація атак на безпеку сенсорних мереж подана на рис.2.2. Згідно з розглянутим, пропонується використовувати такі показники з метою оцінки доцільних методів забезпечення інформаційної безпеки в сенсорних мережах.

• Інформаційна безпека: механізм забезпечення інформаційної безпеки має відповідати вимогам, описаним раніше;

• Відмовостійкість: якщо кілька вузлів мережі є скомпрометованими, то робота системи безпеки має, як і раніше, функціонувати;

• Енергоефективність: механізм забезпечення інформаційної безпеки повинен мати низьке енергоспоживання, щоб максимізувати термін служби сенсорного вузла та мережі в цілому;

• Гнучкість: використання механізму забезпечення інформаційної безпеки не повинно перешкоджати використанню різних методів розгортання мережі, наприклад, випадкове розсіювання чи фіксоване розташування вузлів;

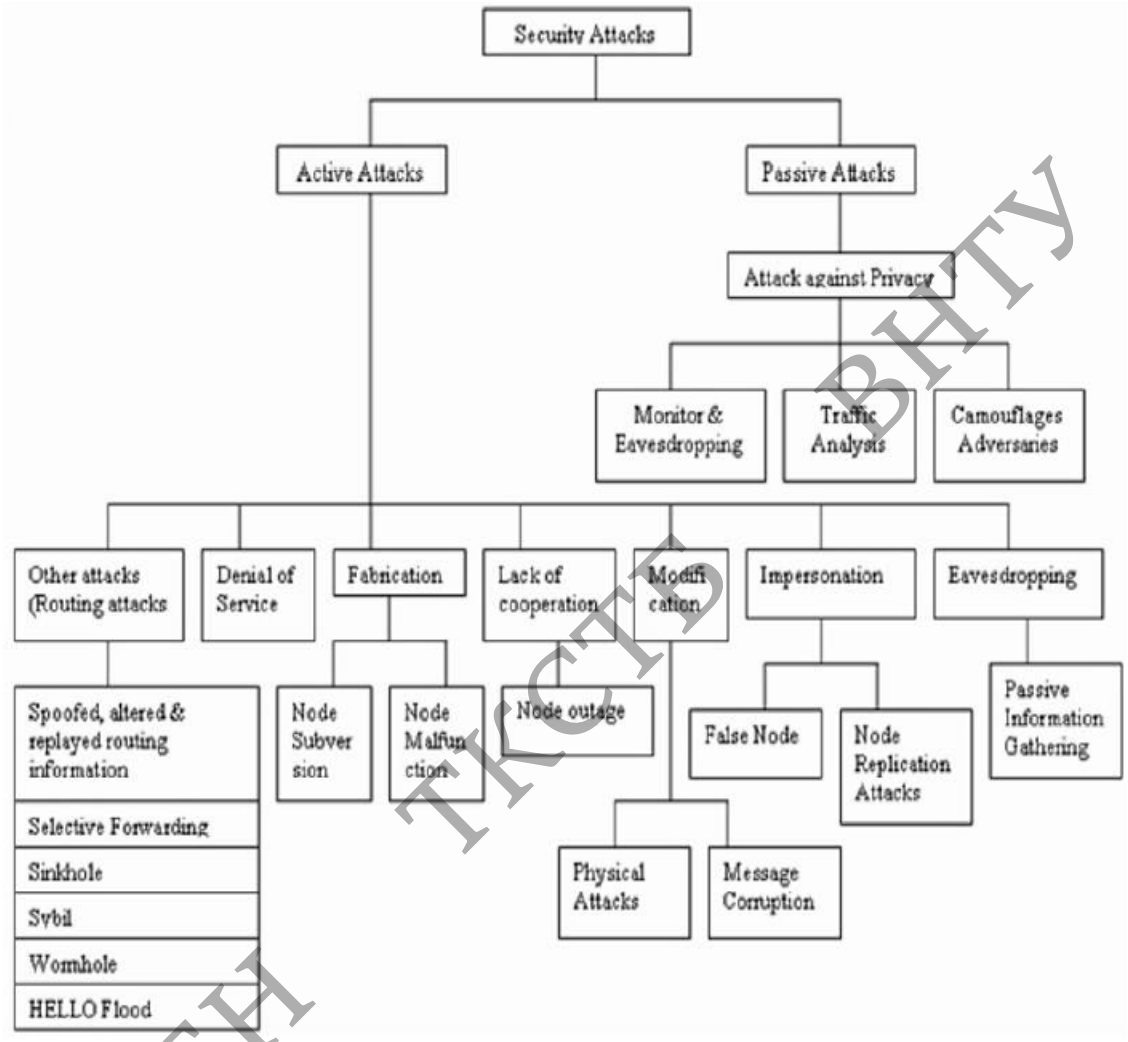


Рисунок 2.2 – Класифікація кібератак у сенсорних мережах

• Масштабованість: механізм забезпечення інформаційної безпеки має підтримувати можливість масштабування мережі без ушкодження або зміни вимог до безпеки;

• Відмовостійкість: механізм забезпечення інформаційної безпеки продовжує функціонувати за наявності несправностей у мережі, таких як пошкоджені або вузли, що вийшли з ладу;

• Самовідновлення: періодично в сенсорних вузлах можуть виникати збої або закінчуватися енергоресурси. Справні датчики повинні мати можливість реорганізації для підтримки встановленого рівня безпеки;

• Достовірність та ефективність: цей пункт має на увазі забезпечення кінцевих користувачів інформацією на різних рівнях. Механізм забезпечення інформаційної безпеки повинен запропонувати користувачеві вибір щодо бажаної надійності, затримки повідомлень і т.д.

На сьогоднішній день існує безліч приватних рішень розглянутої проблеми, проте близько 70% пристроїв сенсорних мереж є слабозахищеними. На цьому етапі розвитку технології, інформаційна безпека є ключовим параметром у подальшій верифікації «розумних датчиків» у діяльність людини, яка в свою чергу сильно обмежена можливостями технології (низькі енергоресурси пристроїв). Крім усіх перерахованих раніше перспектив – основа концепції Інтернету речей приваблює своєю низькою вартістю та простотою компонентів, що негативно впливає на варіанти усунення загроз інформаційній безпеці. Таким чином, ми отримуємо пряму залежність проблеми забезпечення інформаційної безпеки Інтернету речей від простоти самої технології. Очевидним рішенням є усунення недоліків технології щодо питання інформаційної безпеки, що, однак, призведе до різкого зростання вартості пристроїв.

2.2 Захист інформаційної безпеки сенсорної мережі

2.2.1 Особливості кластерної архітектури

Безпровідна сенсорна мережа – це розподілена мережа необслуговуваних мініатюрних сенсорних вузлів, які здійснюють контроль та збір даних. Існує багато додатків, для яких виробники випускають різні вузли для створення сенсорних мереж. За областю застосування програми сенсорних мереж можна поділити на такі категорії [1]: метеорологічні дані (температура, тиск), телемедицина, надзвичайні ситуації (пожежі, катастрофи та ін.), військові операції (визна-

чення місцезнаходження рухомих цілей, територіальне поширення хімічної зброї) та ін. Ці дані переносяться по безпровідному каналу до базової станції (БС). На рис. 2.3 наведено приклад архітектури сенсорної мережі [2].

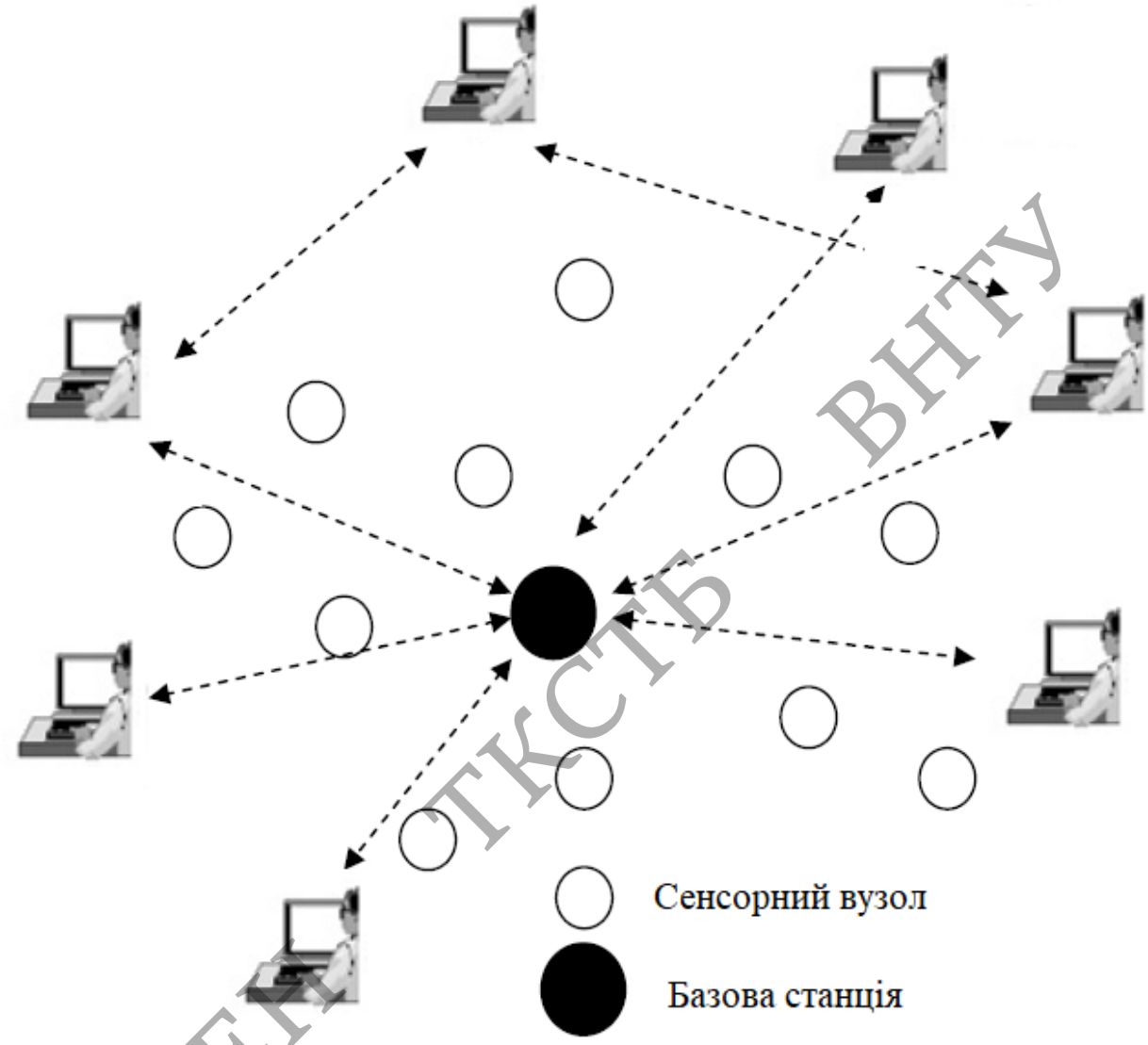


Рисунок 2.3 – Схема архітектури сенсорної мережі для практичного застосування

Вузол мережі, який називається сенсором, містить датчик, що зчитує дає дані від зовнішнього середовища (сенсор), мікроконтролер, пам'ять, радіопередавач, автономне джерело живлення і іноді виконуючі механізми. Для сенсорної мережі характерні наступні фактори, котрі впливають на забезпечення інформаційної безпеки: обмеження сенсорних вузлів у енергоресурсах; продук-

тивність процесора, пам’яті; схильність до видалення вузла з мережі або його заміни; використання вразливих до порушення інформаційної безпеки безпровідних каналів зв’язку. Одна з особливостей сенсорних мереж полягає в тому, що для виконання функцій сенсорні вузли розташовують часто в тих місцях, куди людина не може дістатися.

Обмеження в енергоресурсах для вузлів сенсорної мережі є одним із важливих факторів, що впливають на час функціонування всієї мережі чи її частини. Основне енергоспоживання сенсорних вузлів припадає на обчислювальні процеси та обмін повідомленнями між вузлами.

Тому одним із способів зниження енергоспоживання є скорочення споживаної потужності за рахунок зменшення відстані стояння між вузлами, що взаємодіють. З цією метою використовують кластерну архітектуру побудови сенсорних мереж. У цьому випадку вузли групують у кластери (групи), обмін даними з БС проводиться через виділений головний вузол кластера, який збирає дані (концентратор навантаження) для їх подальшої передачі. На рис. 2 наведено схему сенсорної мережі кластерної архітектури (два кластери), що концентрує інформацію від сенсорних вузлів до БС. Групуванням сенсорних вузлів у кластерні області досягається масштабованість сенсорної мережі. Часто для сенсорної мережі характерно велике число сенсорних вузлів, розташованих з високою щільністю [4], для чого потрібна побудова багаторівневої ієрархічної архітектури головних вузлів кластерних областей.

Наведена на рис. 2.4 архітектура відноситься до однорангової, коли всі вузли сенсорної мережі взаємодіють з базовою станцією напряму.

2.2.2 Ризик загрози виконання функцій головного вузла нелегітимним сенсорним вузлом

До висувають головного вузла висувають високі вимоги з енергоспоживання, оскільки через нього проходять всі повідомлення сенсорних вузлів кластерної області. Застосовують такі стратегії визначення головного вузла класте-

ра – призначення при проектуванні або вибір одного із сенсорних вузлів кластерної області як головного. Вибір може бути фіксованим або змінним, будь-якого вузла або вузла з найбільшими збереженими ресурсами (енергозабезпечення, пам'яті). Високі вимоги до інформаційної безпеки головного вузла є причиною періодичної зміни головного вузла кластерної області [5]. Аналізу у цій роботі підлягає забезпечення інформаційної безпеки кластерної області при реалізації однієї з загроз, що призводить до високого ризику інформаційної безпеки.

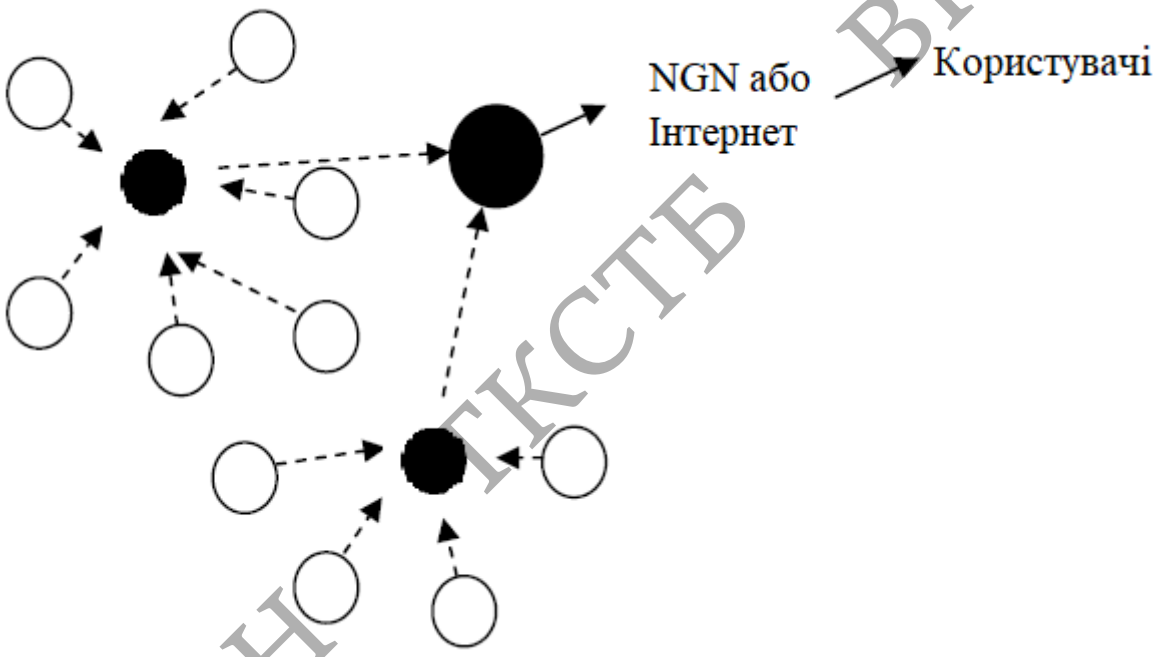


Рисунок 2.4 – Схема сенсорної мережі кластерної архітектури

Згідно з Рекомендацією МСЕ-Т Е.408 [6] за вимогами до безпеки мереж електрозв'язку, характеристика ризику інформаційної безпеки визначається двома показниками – ймовірністю загрози безпеки та наслідком її впливу при атаці зловмисника (реалізації цієї загрози).

Для сенсорних мереж характерна висока ймовірність реалізації загрози інформаційної безпеки – вкидання в мережу (в даному випадку в кластерну область) зловмисником нелегітимного сенсорного вузла.

Високий ризик інформаційної безпеки щодо наслідку буде мати місце в тому випадку, якщо цей вузол буде виконувати функцію головного сенсорного вузла. Це може виражатися у різних формах наслідків атаки «відмова в обслуговуванні» (DoS) маршрутизації, виражених у припиненні функціонування частини або всієї мережі [7]:

- Виснаження мережевих ресурсів сенсорних вузлів;

- головний вузол знищує всі пакети або вибірково ті, які він отримує для наступної передачі;

- сфальсифікована, змінена або нелегітимно повторена інформація отриманого пакета для подальшої передачі та ін.

Способи забезпечення інформаційної безпеки багатьох мереж зв'язку включають як традиційні механізми захисту (криптографія, автентифікація та ін), так і механізми виявлення вторгнення (Intrusion Detection System – IDS). Незалежно від того, які засоби захисту передбачені, зловмисник у такій вразливій до загроз інформаційної безпеки мережі, як сенсорна, за допомогою спеціальних протоколів може знайти способи, щоб порушити безпеку. Відповідно до роботи [7], це є причиною того, що захист від загроз інформаційної безпеки в сенсорних мережах починається з роботи механізмів IDS. Це саме стосується і випадку розглянутої атаки (вкидання зловмисником у кластерну область нелегітимного вузла з виконання ним функцій головного вузла).

Виявлення вторгнень у загальному випадку – це процес моніторингу та визначення спроб реалізації загроз інформаційної безпеки. В даній роботі це визначення спроб вкидання нелегітимного сенсорного вузла в кластерну область сенсорної мережі та використання його як головного вузла кластера.

2.2.3 Механізми виявлення вторгнення у кластерну область

Прийнято класифікувати механізми виявлення вторгнень на три типи [4]:

- Виявлення на основі сигнатур. Під сигнатурою розуміють характеристики (профілі) відомих атак зловмисника: IDS порівнює поточну роботу з кож-

ним із профілів, що зберігаються. При збігу з одним з них механізм виявлення вторгнення оповістить про це. Недоліком такого механізму є те, що він не дозволяє виявити новий (невідомий) вид атаки;

- Виявлення на основі аномалій. Суть роботи такого механізму полягає в установці профілів при нормальній поведінці системи (зазвичай це встановлюється автоматизованим чином) та виявлення відхилення від нього при поточній роботі. Основний недолік такого механізму полягає в тому, що він помилково оповіщає багато атак зловмисника, яких насправді не було;

- Виявлення, засноване на специфікаціях. Цей тип поєднує обидва попередні.

Використання одночасно обох типів механізмів дозволяє зменшити зазначені недоліки та підвищити інформаційну безпеку сенсорної мережі.

Далі розглянемо деякі механізми виявлення вторгнень на основі аномалій при вкиданні зловмисником нелегітимного сенсорного вузла. Моніторинг здійснюється для запобігання цим нелегітимним вузлом виконання функцій головного вузла. На рис. 2.5 наведена структура потоків даних в сенсорній мережі, що включає пакети даних від сенсорів і пакети механізму виявлення вторгнень IDS. На рис.2.5 показано дві кластерні області на нижньому ієрархічному рівні структури сенсорної мережі. Повідомлення з головних вузлів цих кластерних областей направляються в головний вузол верхнього рівня і далі на базову станцію.

На рис. 2.5 показаний принцип роботи механізму виявлення вторгнень, в основі якого лежить постійний моніторинг кожного з сенсорних вузлів кластерної області за поведінкою їх вузлів-сусідів. Зібрані дані механізму виявлення вторгнень аналізуються кожним сенсорним вузлом і направляються для обробки головному вузлу кластера. У разі виявлення зловмисної поведінки головний вузол повідомляє про вузол-зловмислник сусіднім з ним вузлам. В результаті взаємодія з ним припиняється.

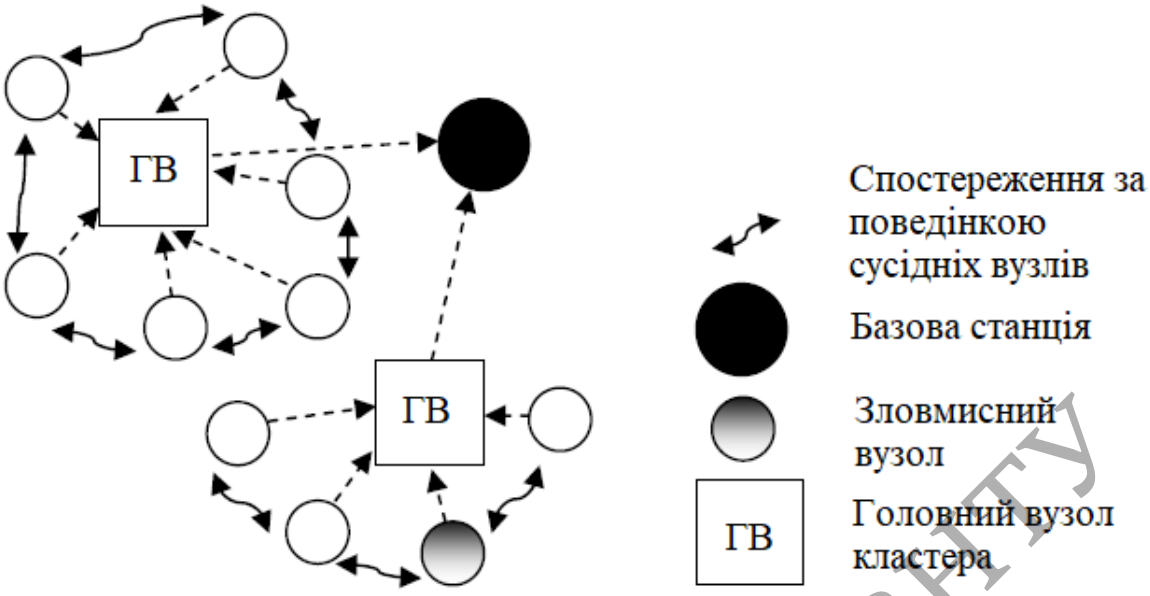


Рисунок 2.5 – Принцип роботи механізму виявлення вторгнень у сенсорних мережах

2.2.4 Механізми виявлення на основі аномалій вторгнень нелегітимного сенсорного вузла кластерної області

Розглянемо атаку в кластерній області сенсорної мережі шляхом вкидання нелегітимного сенсорного вузла при стратегії зміни під час експлуатації головних вузлів залежно від ступеня виснаження їхньої енергії. При такій зміні функції головного вузла покладаються на той кінцевий вузол, який зберіг найбільшу електроенергію. Завдання забезпечення інформаційної безпеки кластерної області розпадається на дві: виявлення нелегітимного сенсорного вузла і, у разі безуспішного вирішення цього завдання, виявлення виконання функцій головного вузла нелегітимним вкинутим зловмисником сенсорним вузлом.

Далі наведено опис механізмів системи виявлення вторгнення IDS на основі аномалій. Розглядаються фізичний та канальні рівні сенсорного вузла кластерної області [7]. При цьому робиться акцент на характеристику, що дозволяє виявити вторгнення, але не наводиться, яким чином обробляється цей сигнал.

1. Захист фізично. Проблема захисту радіоінтерфейсу (захист від прослуховування каналу передачі та зашумлення) інтенсивно досліджується для всіх

безпровідних мереж. Запропоновано багато рішень, таких як широкосмугова передача і стрибкоподібна перебудова частоти. Коли вузол приймає пакет, важко визначитити, чи надійшов пакет від заявленого відправника, якщо не застосовується аутентифікація.

На фізичному рівні сенсорного вузла використовується величина потужності сигналу RSSI (Received Signal Strength Indicator).

Сучасні операційні системи для сенсорних мереж, такі як TinyOS, надають можливість отримання RSSI. Для безпровідного середовища передачі RSSI залежить від відстані між вузлами. При розгортанні сенсорної мережі значення RSSI дозволяють визначити вузли-сусіди. При функціонуванні сенсорної мережі вузли стежать за цими значеннями, що надходять від сусідніх сенсорних вузлів. Отримання неочікуваного значення RSSI відрізняється підозрілим аномальною поведінкою від можливого вкидання нелегітимного сенсорного вузла для заміни легітимного вузла. Існує чимало факторів (фоновий шум, погодні умови), які з великою ймовірністю можуть викликати помилкові підозри. Тому цей підхід слід використовувати у комбінації з іншими (на інших рівнях).

2. Захист на канальному рівні. Якщо для управління розмежуванням доступу використовують протоколи встановлення розкладу, то для кожного з вузлів виділяється унікальний часовий слот. Для підміни легітимного вузла при вкиданні нелегітимного сенсорного вузла необхідно, щоб він використовував той самий часовий слот. Якщо вкинутий зловмисником сенсорний вузол не дотримується цього часового розкладу і намагається видати себе за легітимний вузол, в той час як для цього вузла передача не передбачається, то сусідні з ним вузли можуть визначити такий нелегітимний вузол. Нижче показано, яким чином фіксується аномальне явище при виконанні протоколу часового множинного доступу TDMA (Time Division Multiple Access) та протоколу S-MAC (Sensor MAC), виконує перемикання сплячого та робочого режимів.

Передача даних від сенсорних вузлів у головний кластерний вузол області здійснюється за схемою множинного доступу з часовим розділенням TDMA [5]. При цьому кожному сенсорному вузлу надається певний інтервал часу

(слот) однакової несучої частоти. Отримання повідомлення на непризначеному для нього слоті відзначається як підозріле аномальне явище від можливого вкидання нелегітимного додаткового сенсорного вузла або для заміни легітимного вузла.

Відповідно до протоколу S-MAC [9] для зниження споживання електроенергії сенсорний вузол сенсорної мережі працює за певним циклом, що включає крім режиму передачі та прийому повідомлень ще очікуючий і сплячий режими. Споживання енергії в кожному з цих режимів різне. Сусідні сенсорні вузли за допомогою обміну повідомленнями встановлюють узгоджений розклад часових періодів цих режимів. Отримання повідомлення на непризначеному для нього режимі відзначається як підозріле аномальне явище від можливого вкидання нелегітимного нового сенсорного вузла або для заміни легітимного вузла.

2.3 Криптографія у сенсорних мережах

При побудові надійної сенсорної мережі важливим завданням є вибір криптографічного методу шифрування даних. На даний момент не існує єдиного рішення, котре яке підходило б сенсорним мережах різних типів. Саме тому при побудові мережі потрібно оцінювати необхідні характеристики мережі такі як, очікуване число вузлів, швидкість передавання даних, енергоспоживання, вартість розгортання мережі, потрібний рівень безпеки розглянемо основні характеристики різних типів шифрування, що можна застосувати і у сенсорних мережах.

2.3.1 Шифрування

Головною проблемою використання алгоритмів шифрування із закритим ключем є великі обчислювальні витрати. Так, для виконання однієї операції множення зі 128-бітним результатом мікропроцесору потрібно буде спожити

більше 1000 нДж. В той же час, симетричні методи і алгоритми на основі хеш-функцій потребують менше ресурсів. Зокрема, при шифруванні 1024 біт інформації за алгоритмом RSA мікропроцесор MC68328 DragonBall споживає 42мДж. А от при використанні алгоритму AEC – лише 0,104мДж.

В той же час, застосувати алгоритми із відкритим клем можливо при правильному підборі як алгоритму, так і основних параметрів, що пов'язані з енергоспоживанням. Зокрема, надійність, подібну до надійності RSA можливо одержати при застосуванні ECC (Elliptic Curve Cryptography), окрім того при цьому розмір ключа є меншим, що скорочує часові витрати. Наприклад, ECC з ключем розміром 160 біт має такий же рівень безпеки як і RSA ключем 1024 біт.

Таким чином, застосування асиметричних ключів у сенсорних мережах є досить проблемним, через великі обчислювальні витрати, але при правильній оптимізації є можливим.

В алгоритмах симетричного шифрування використовується один ключ, відомий обом сторонам. При використанні алгоритмів симетричного шифрування енергозатрати є значно меншими. При цьому, необхідно забезпечити надійний механізм передачі ключа шифрування.

2.3.2 Протоколи управління ключами

Мета механізмів управління ключами – це встановлення криптографічних ключів в вузлах мережі надійно та безпечно. Окрім того, механізм підтримує приєднання і від'єднання вузлів. На рис.2.6 подано класифікацію існуючих протоколів управління ключами.

В залежності від структури мережі застосовують централізовані або розподілені протоколи управління ключами. Якщо використовується централізована схема управління, то один об'єкт, який називається Key Distribution Center (KDC), контролює, генерує та розподіляє ключі. На централізованій схемі базується протокол LKHW. В його основу покладена логічна ієрархія ключів LKH. В цій схемі ключ розподіляється по дереву мережі із KDC.

Недолік такої схеми – тільки один об’єкт відповідає за весь механізм. У випадку, якщо KDC вийде зі строю випадково чи внаслідок дій зловмисника, то безпека мережі дуже сильно знижується.

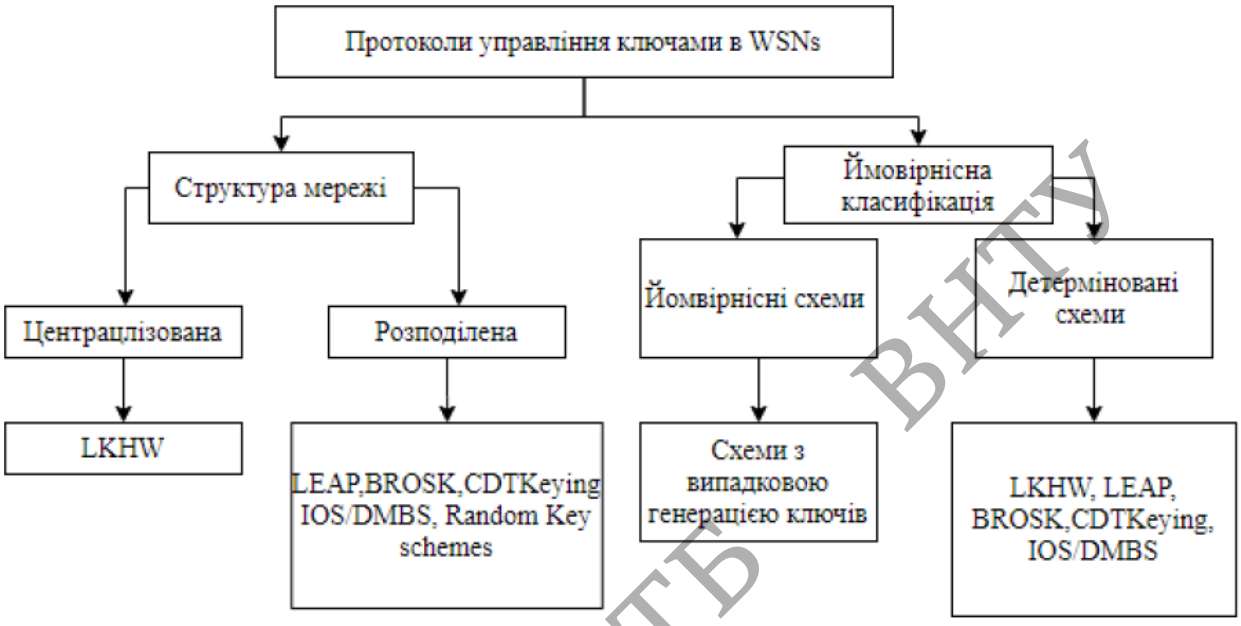


Рисунок 2.6 – Класифікація протоколів управління ключами у сенсорних мережах

При застосуванні розподіленої схеми за управління ключами відповідають різні об’єкти. Тобто протоколи не мають вразливості в одній точці мережі як у попередній схемі. Ці протоколи можуть бути або детермінованими чи ймовірнісними.

LEAP – ц еще один протокол управління ключами сенсорної мережі, він грунтується на алгоритмах симетричного шифрування. В залежності від вимог до безпеки, він застосовує різні механізми управління. Згідно цього протоколу, у вузлах мережі встановлюються таки типи ключів: 1) індивідуальний – спільний між вузлом і базовою станцією, він попередньо конфігурується, 2) груповий – для всіх вузлів, він також конфігурується попередньо, 3) парний – відомий сусіднім вузлам, 4) кластерний – розділяється між групою вузлів, призначений для локальної комунікації вузлів.

Згідно цього протоколу, час який необхідний для атаки на вузол більше ніж час ініціалізації мережі, протягом ятого вузли мережі встановляють контакт із сусідніми. Для ініціалізації мережі спільний ключ встановлюється в вузли до її розгортання. Кожен вузол обчислює головний ключ, котрий залежить від унікального ідентифікатора вузла та спільного ключа. Потім вузли обмінюються повідомлення HELLO, яке може аутентифікувати одержувач. Тоді вузли обчислюють спільний ключ знаючи свої головні ключі. По завершені ініціалізації на всіх вузлах спільний ключ видаляється і припускається, що жоден вузол не був скомпрометований до цього моменту. Так як після цього зловмисники не зможуть одержати спільний ключ, то введення даних ззовні є неможливим. Окрім того, жоден вузол не зможе підробити головні ключі інших вузлів.

Розглянемо схему поширення ключа, яки базується на теорії комбінаторного проєктування. За цією схемою генеруються симетричні ключі із параметрами n^2+n+1, $n+1$, 1. Ця схема підтримує n^2+n+1 вузлів та застосовує набір ключів розміру n^2+n+1. Генерується n^2+n+1 послідовностей ключів розміру $n+1$, причому кожна пара послідовностей має один спільний ключ, а кожен ключ з'являється рівно у $n+1$ послідовностях. Після розгортання мережі у кожної пари вузлів точно є один спільний ключ. Недолік цієї схеми –параметр n має бути відомим, тобто розмір мережі фіксований.

Розглянемо схему PIKE (peer intermediaries for key establishment), згідно із якою всі вузли мережі організовуються у двовимірний простір (рисунок 2.7). Координати кожного вузла позначаються як (x;y) причому x, y є {0, 1,.. √N – 1}. У кожного вузла є спільний ключ з 2(√N – 1) вузлами, що мають одинакові координати x або y. Для тих двох вузлів, які не мають спільних координат застосовують маршрутизатор. Але для цієї схеми потрібні високі витрати на комунікацію, так як безпечне з’єднання можна встановлене тільки з 2/√N вузлами, тобто кожен вузол має встановити ключ майже для кожного з своїх сусідніх вузлів по всьому шляху передачі.

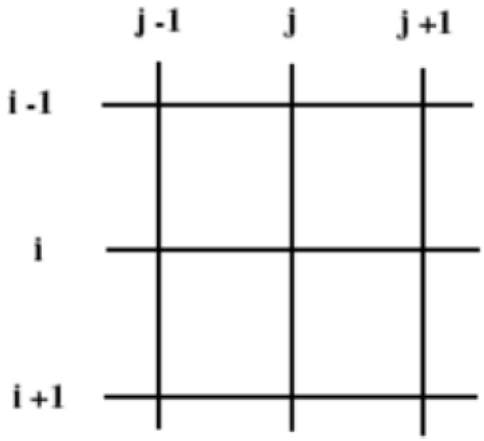


Рисунок 2.7 – Схема PIKE

2.3.3 Протоколи безпеки

Розглянемо основні протоколи, оптимізовані для сенсорних мереж. Так, протокол SPINS (Security Protocols for sensors networks) складається з двох блоків: SNEP і μTESLA. SNEP забезпечує конфіденційність даних та двосторонню аутентифікацію. μTESLA реалізує аутентифікацію для широкомовної передачі даних.

2.3.3.1 SNEP

Для виконання вимог безпеки задіюють два блоки захисту μTESLA і SNEP. SNEP забезпечує конфіденційність даних та двосторонню комунікацію вузлів A і B, що мають спільний головний ключ χAB. Використовуючи функцію псевдовипадкових чисел F отримують для кожного напрямку комунікації ключі шифрування $K_{AB}=F\chi(1)$ та $K_{BA}=F\chi(3)$ і MAC ключі $K'_{AB}=F\chi(2)$ і $K'_{BA}=F\chi(4)$. Зашифрована інформація має такий формат $E=\{D\}<K,C>$, тут D – данні, K – ключ шифрування, C – лічильник. MAC шифрування має вигляд $M=M(K',C||E)$. Повне повідомлення, яке передається з вузла A до вузла B має такий вигляд $A\rightarrow B$: $\{D\}<K_{AB},C_A>$), $MAC(K'_{AB}C_A||\{D\}<K_{AB},C_A>)$

До переваги SNEP відносять:

- Семантичну безпеку. Оскільки після кожного повідомлення лічильник інкрементується, то кожне повідомлення шифрується по різному. Число у лічильнику є достатньо довге, аби не повторюватися у рамках життєвого циклу одного вузла.
- Аутентифікація даних. Перевіривши MAC, отримувач може підтвердити той факт, що повідомлення прийшло від оригінального відправника.
- Захист від атак повторного відтворення. Лічильника в MAC, у якому є номер поточного повідомлення захищає від атак повторного відтворення.
- Слабка актуальність повідомлення. Отримувач може перевірити той факт, що повідомлення було отримане саме після попереднього повідомлення, це гарантується порядком повідомлень.
- Невеликі витрати на комунікацію. Оскільки стан лічильника зберігається на обох сторонах, саме тому він не передається з відправленням кожного повідомленням.

SNEP забезпечує слабку актуальність даних, так як він гарантує порядок повідомлень відправлених із вузла B до вузла A, але не те що повідомлення було відправлене у відповідь на запит вузла A з вузла B.

Вузол A здатен досягти строгої актуальності даних для відповіді вузла B із використанням N_A – випадкового число бітів, згенерованих вузлом A. Вузол A генерує число N_A та відправляє його до вузла B з запитом R_A. Потім, вузол B відправляє N_A разом із відповіддю R_B.

Однак, з метою оптимізації, замість явного повернення N_A, вузол B може використовувати його при обчислені MAC. Тоді обмін повідомленнями можна бути описати так $A \rightarrow B$: N_A, R_A $B \rightarrow A$: $\{RB\}<K_{BA}, C_B>$ $MAC(K_{BA}', N_A \| C_B \| \{R_B\}<K_{BA}, C_B>)$

Вузол A може бути впевненим після перевірки MAC, що відповідь була згенеровано вузлом B на запит R_A.

Розглянемо протокол обміну станом лічильника. Для досягнення малих розмірів повідомлень припустимо, що обидві сторони A і B знають стан

лічильника одна одного. Тобто, C_A та C_B можна не додавати до повідомлень. Але повідомлення можуть втрачатися під час передачі, тоді C_A та C_B матимуть не цілісний стан, необхідно буде синхронізувати їх значення. Для цього використовується такий протокол обміну значеннями C_A і C_B $A \rightarrow B$: C_A $B \rightarrow A$: C_B, $MAC(K'_{BA} C_A || C_B)$ $A \rightarrow B$: $MAC(K'_{AB} C_A || C_B)$

Значення C_A та C_B не потребують шифрування, так як не є секретними. Окрім того, що MAC не містить імен вузлів A та B. Ключі K'_{BA} та K'_{AB} неявно зв'язують повідомлення, що забезпечую правильний напрямок їх передачі. Коли вузол A виявляє, що C_B несинхронізовано, то він може зробити запит C_B до вузла B застосовуючи N_A для гарантування актуальності даних $A \rightarrow B$: N_A $B \rightarrow A$: C_B, $MAC(K'_{BA} N_A || C_B)$

З метою запобігання DoS атаками, у випадку, коли зловмисник відправляє фіктивні повідомлення для синхронізації станів лічильників без необхідності, можливе перемикання вузлів в режим передачі лічильників після кожного зашифрованого повідомлення. Ще один спосіб – виявлені таких атак шляхом додавання іншого короткого MAC до повідомлень, котрий не залежить від лічильника.

2.3.3.2 µTESLA

Протокол µTESLA представляє собою модифікацію протоколу TESLA. Через високі обчислювальні затрати, використання самого протоколу TESLA у сенсорних мережах неможливе. Окрім того, за протоколом TESLA кожен пакет містить приблизно додаткових 24 байти робочих даних. У сенсорних мережах вузли відправляють невеликі повідомлення розмірами біля 30байт, тому це є не практичним, так як з 64 бітним ключем та MAC частина пакета, що пов'язана з TESLA, буде складати лише 50%.

Із урахуванням наведених недоліків протоколу TESLA, було розроблено протокол µTESLA в якому були вирішені такі проблеми протоколу TESLA:

- TESLA здійснює аутентифікацію початкового пакета за цифровим підписом, що вимагає занадто потужних обчислювальних ресурсів порівняно із можливостями вузлів.
- Протокол TESLA шифрує повідомлення використовуючи асиметричні алгоритми із відкритим ключем, що також вимагає суттєвих затрат на обчислення.

Протокол μTESLA вимагає синхронізації між вузлами та базовою станцією. Перед відправленням пакету, базова станція обчислює MAC із секретним ключем, відомим в даний момент тільки базовій станції. Після того, як вузол отримав пакет, він може перевірити, чи не розкрила базова станція секретний ключ. Це можливо завдяки строгій синхронізації за часом та графіку, за яким ключ буде розкритий. Оскільки ключ, ще не розкритий, то вузол може бути впевненим у тому, що пакет не було пошкоджено або змінено зловмисником під час передачі. Вузол зберігає цей пакет у буфері. Потім базова станція передає секретний ключ вузлам, що можуть його перевірити. Якщо ключ пройшов перевірку, то вузли можуть його використовувати для аутентифікації пакету, збереженого в буфері.

Кожен MAC ключ представляє собою ключ із ланцюга ключів, що був згенерований односторонньою функцією *F*. Для генерації ланцюга односторонніх ключів, відправник випадково обирає з ланцюга останній K_n та повторно застосовує функцію *F* з метою обчислення $K_i=F(K_i+1)$. Використовуючи SNEP протокол, кожен вузол може просто отримати ключ аутентифікації із ланцюга ключів.

Розглянемо такий приклад. На рис. 2.8 подано зображено ланцюг ключів μTESLA у часових інтервалах, та послідовність пакетів, відправлених з базової станції. Кожен ключ із цього ланцюга знаходиться у деякому часовому інтервалі. Усі пакети, відправлені протягом цього інтервалу, зашифровано за допомогою одного ключа.

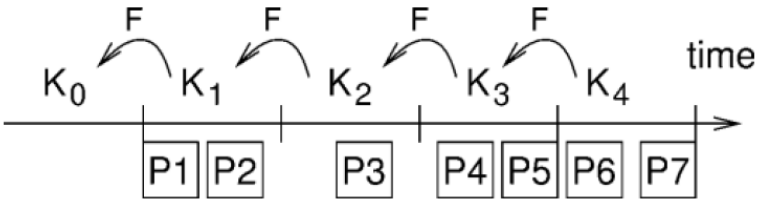


Рисунок 2.8 – Ланцюг ключів μTESLA

У цьому випадку відправник розкриває секретний ключ, це відбувається через один часовий інтервал після його використання для обчислення MAC. Вважається, що отримувачі є синхронізованими за часом із відправником і вони знають ключ K_0. Пакети P_1 та P_2 було відправлено у перший часовий інтервал та зашифровано ключем K_1. У пакета P_3 MAC обчислений за допомогою ключа K_2. Вважаємо, що пакети P_4, P_5, P_6 втрачено при передачі, так як отримувач не може виконати аутентифікацію пакетів P_1, P_2, P_3. Базова станція відправляє ключ K_2 в інтервал 4, який перевіряють шляхом порівняння відомого значення ключа K_0 та його обчисленого значення ключа двічі застосувавши функцію F, тобто $K_0=F(F((K_2))$.

Потім сенсорні вузли можуть обчислити значення першого ключа $K_1=F(K_2)$, здійснити аутентифікацію пакетів P_1, P_2 ключем K_1 та пакету P_3 ключем $K2$.

Розкриття ключів здійснюється незалежно від широкомовної передачі пакетів та залежить від часових інтервалів. Окрім того, в протоколі μTESLA відправник періодично відправляє в спеціальному пакеті поточний ключ.

Протокол μTESLA має декілька етапів: налаштування відправника, відправлення аутентифікованих пакетів, налаштування отримувача, аутентифікація пакетів.

Налаштування відправника відбуваєтсья таким чином. Відправник (базова станція) початку генерує послідовність секретних ключів. За допомогою генератора випадкових чисел він створює останній ключ послідовності K_n, та застосовує до нього односторонню функцію F таким чином: $K_j=F(K_j+1)$. Так як F є односторонньою функцією, неможливо обчислити наступні ключі, наприклад

$K_0 \ldots K_j$, знаючи ключ K_{j+1}. Окрім того, еможна знайти знайти K_{j+1} знаючи ключі $K_0 \ldots K_j$. Подібний підхід використовує система одноразових паролів S/Key.

Відправлення автентифікованих пакетів відбувається таким чином. Час розділяється на уніфіковані інтервали, а відправник асоціює одному часовому інтервалу один ключ. У часовому інтервалі i відправник застосовує для обчислення MAC поточний ключ K_i. Відправник розкриває ключ K_i у часовому інтервал (i+δ). Зокрема, час затримки розкриття ключа має бути більшим за час передачі пакета до найбільш віддаленого вузла.

Налаштування отримувача здіснютсья таким чином. У протоколі μTESLA отримувач, маючи один ключ, може перевірити підпослідовність ключів у ланцюзі ключів. Якщо отримувач має ключ K_i, то він може здійснити аутентифікацію ключа Ki+1 за допомогою функції F, тобто $K_{i+1}=F(K_i)$. Для того, щоб налаштувати протокол μTESLA, кожний має мінімум один ключ із послідовності ключів. Відправник і отримувач мають бути синхронізовані за часом. Графік розкриття ключів повинен бути відомий отримувачу. З цією метою до відправника S отримувач відправляє запит з N_R. Відправник, тобто базова станція, S відповідає повідомленням, у котрому міститься поточний час T_s, ключ K_i, використаний у пройденому часовому інтервалі i, час початку цього часового інтервалу T_i, тривалість часового інтервалу T_{int}, час затримки δ. Процес описується виразами:

$$M \rightarrow S: N_M$$

$$S \rightarrow M: T_s | K_i | T_i | T_{int} \mid \delta \text{ MAC}(K_{MS}, N_M | T_s | K_i | T_i | T_{int} \mid \delta)$$

MAC застосовує спільний ключ, відомий як вузлам, так і базовій станції, а N_M призначено для забезпечення свіжості даних.

Аутентифікація широкомовних пакетів реалізується у такий спосіб. Після одержання пакету отримувач має перевірити, чи не були вони під час передачі пошкоджені зловмисником. У випаду, коли зловмиснику відомий ключ якогось часового інтервалу, він здатен пошкодити пакети, так як йому відомий ключ, використаний при обчислення MAC. Зокрема, отримувач має знати, що пакет не було пошкоджено, а відправник не розкрив ключа, який було використано у

MAC цього пакету. У ому випадку, коли пакет не пошкоджено, отримувач має його зберегти у буфері, інакше пакет повинен бути відкинуто.

Одразу після одержання ключа, отримувач перевіряє його на рівність з останнім ключем, який йому відомий. Це виконується шляхом застосування односторонньої функції F протягом декількох разів: $K_u=F_{i-u}(K_i)$

Якщо перевірка була успішною, то виконується аутентифікація усіх пакетів, відправлених у часових інтервалів з u до i. Отримувач заміняє збережений ключ K_i на ключ K_u.

Широкомовна передачі з вузла реалізується таким чином. Так як сенсор-вузол має обмежену пам'ять, він не здатен зберігати всю послідовність ключів односторонньої функції. Крім того, обчислення кожного ключа починаючи із початкового K_n є довгим процесом. Нарешті, досить складно для вузла мати спільний ключ із кожним отримувачем. Ще однією проблемою є те, що розкриття ключа є дороговартісним, якщо батареї вузлів мають невелику ємність. Існують такі рішення вищенаведених проблем:

- Здійснювати широкомовну передачу із базових станцій. Вузол передає повідомлення на базову станцію за протоколом SNEP, базова станція здійснює широкомовну передачу.
- Вузол здійснює широкомовну передачу, але для зберігання послідовності ключів використовується базова станція. Вона при необхідності передає ключі до вузла. З метою заощадження енергії вузла, розкриття ключів може також виконуватися базовою станцією, як і налаштування нового отримувача.

Перший варіант є більш прийнятним, так як при широкомовній передачі всі отримувачі повинні бути додатково синхронізовані ще і з цим вузлом, я також знати його графік розкриття ключів. Це обмежує число тих вузлів, які можуть виконувати широкомовну передачу.

Таким чином, основним шляхом забезпечення інформаційної безпеки сенсорних мереж є застосування криптографічних методів шифрування даних. Можливо застосовувати асиметричне шифрування, але воно не є оптимальним

в умовах оптимізації енергетичних витрат. Симетричні алгоритми добре підходять для вузлів-сенсорів, що суттєво обмежені в ресурсах. В той же час, симетричні методи шифрування потребують застосування надійних протоколів управління ключами, вибір визначається структурою мережі та способом генерації і поширення ключів. Однак, саме протоколи управління ключами є слабким місцем сенсорних мереж.

Комбінація протоколів SNEP та μTESLA забезпечує високий рівень відповідності сенсорних мереж вимогам та надає можливість здійснювати захищене широкомовне мовлення у межах мережі.

2.4 Особливості безпеки у різних технологіях сенсорних мереж

2.4.1 Безпека в Short-Range Low Power мережах

Як відомо, низькошвидкісні безпровідні мережі близької зони дії в основному засновані на стандарті IEEE 802.15.4. Цей стандарт використовують такі технології як 6LoWPAN, ZigBee, Z-Wave, EnOcean, SNAP. Стандарт 6LoWPAN представляє собою комбінацію IPv6 із IEEE 802.15.4. Стандарт LoWPAN також використовує IPv6 поверх IEEE 802.15.4. Протоколи для пристроїв типу «розумний дім» працюють на технологіях 6LoWPAN та EnOcean.

Мережа стандарту 6LoWPAN складається з одної або декількох мереж. За допомогою маршрутизатора що контролює вхідний та вихідний потік даних, вони підключаються до інтернету. В мережі 6LoWPAN механізми забезпечення безпеки дозволяють доступ до даних лише авторизованим користувачам, зберігають цілісність даних та виявляють вторгнення несанкціонованого користувача. Окрім того, потрібно аналізувати трафік з обох сторін мережі – як з IPv6 так і з LoWPAN.

Механізм фрагментації пакетів є досить вразливим через авторизації на рівні LoWPAN і застосування пристроїв із обмеженою пам’яттю. Наприклад, зловмисник може зупинити процес коректного збору пакета на приймальному

вузлі або здійснити атаку шляхом відправлення одного protocol-complaint 6LoWPAN фрагменту.

Для маршрутизації трафіку IPv6 у малопотужних мережах, які реалізують поверх 6LoWPAN і у яких можливі великі або непередбачувані втрати пакетів можна використовувати протокол маршрутизації IPv6 для LLN (RPL).

Для захисту RPL використовує поле "Захист", яке розташоване після заголовка повідомлення ICMPv6, що має розмір 4 байти. В цьому полі інформація вказує на рівень захисту та на криптографічний алгоритм, що застосовується для шифрування даних. RPL забезпечує семантичну безпеку, підтримку автентичності даних, конфіденційність, захист від атак повторного відтворення, керування ключами. На RPL здійснюються такі атаки, як селективна переадресацію, Сибіл, sinkhole, Hello flooding, відмовау в обслуговуванні та чорна дірка.

3.2 Безпека в Bluetooth Low Energy

Протокол BLE представляє собою малопотужну версія технології Bluetooth. У BLE швидкість передачі даних та радіодіапазон даних є нижчими, ніж у звичайному Bluetooth. BLE розроблено для додатків з низькою потужністю, котрі працюють на акумуляторах з невеликою ємністю. Завдяки малій потужності та тривалому час роботи акумуляторів, BLE пристрої можуть працювати довгі роки без заміни акумулятора. До найбільш популярних атак на BLE відносять пасивне підслуховування та атаку типу «людина в середині».

Захистити мережу від пасивного підслуховування можна шляхом шифрування комунікації за допомогою ключа. У ранніх версіях BLE пристрої використовували тимчасові ключі, які легко було вгадати. У версії BLE 4.2 для генерації ключів Diffie-Hellman Key застосовують Federal Information Processing Standard (FIPS), який є сумісним з стандартом Elliptic Curve Diffie-Hellman (ECDH), що загалом суттєво ускладнює реалізацію атаки підслуховування.

Захист від атак "людина в середині" означає, що потрібно забезпечити, аби пристрій розпочав комунікацію з призначеним пристроєм, а не в жодному випадку із неавторизованим пристроєм, або ж пристроєм, що видає себе за при-

значеного. Із цією метою BLE Secure Connections використовує числовий метод порівняння.

2.4.2 ZigBee протокол

Захист мережі ZigBee базується на симетричній криптографії, тобто на обох сторонах для шифрування і дешифрування використовується спільний ключ. Для шифрування використовується алгоритм AEC. захист мережі При цьому засновано на відкритій моделі довіри, це означає, що стек рівнів протоколу довіряють один одному і один спільний ключ шифрування. Цей ключ зберігається на самому пристрої для шифрування даних від різних рівнів. Таким чином, можна забезпечення захист даних тільки при передаванні між кінцевими пристроями, але не між окремими рівнями. ZigBee використовує один рівень безпеки як для всіх пристроїв у мережі та і для всіх рівнів пристрою, що дозволяє спростити забезпечення сумісності кінцевих пристроїв у безпровідній мережі.

Окрім того, для забезпечення захисту від атак повторного відтворення вмикається лічильник кадрів. Пристрій, котрий одержує кінцеве повідомлення перевіряє лічильник кадрів і відкидає повторні повідомлення. Для захисту від глушіння сигналу у ZigBee використовується гнучка зміна частоти.

У ZigBee передбачено дві архітектурні моделі захисту – централізована модель та розподілена. Це дозволяє забезпечити вимоги багатьох кінцевих пристроїв. Різниця між цими двома моделями полягає в тому, як саме вони приймають нові пристрої у мережу та захищають передані повідомлення.

Хоча розподілена схема забезпечує менший захист, вона є більш простою. Для побудови розподіленої схеми застосовують маршрутизатор. Він забезпечує захист та передавання ключів шифрування. Після приєднання до мережі нового маршрутизатора з кінцевими пристроями, попередній маршрутизатор передає їм мережевий ключ, котрий шифрується так званим ключем приєд-

нання (link-key). При цьому усі пристрої мають ключ приєднання, тобто вони попередньо сконфігуровані.

Більш надійною є централізована схема. Вона містить так званий центр довіри (Trust Center), котрий розташовується у координаторі. Центр довіри конфігурує мережу, відповідає за приєднання нових пристроїв та за аутентифікацію всіх маршрутизаторів. Центр довіри встановлює ключі приєднання для пристрою при його приєднанні та для пари пристроїв за запиту. Також центр довіри генерує і передає так званий мережевий ключ (network-key). У цій моделі також всі пристрої мають бути попередньо сконфігурованими з ключем приєднання, котрий використовується для шифрування передачі мережевого ключа для тих пристроїв, котрі приєднуються до мережі. Ці схеми подано на рис. 2.9.

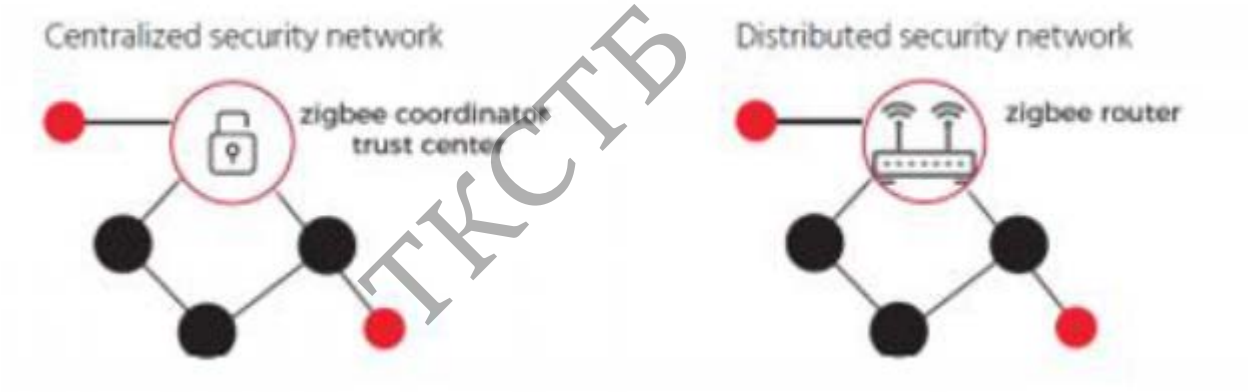


Рисунок 2.9 – Централізована та розподілена схема захисту

Безпека мережі, побудованої на відкритій моделі довіри, залежить від таких припущень.

- Безпечне зберігання симетричних ключів. У стандарті ZigBee припускається, що симетричні ключі не доступні ззовні, а всі передачі ключів шифруються. Виключенням може бути короткий момент часу, не більше 8мс, при ініціалізації мережі. У цей момент передається один ключ, який може бути не шифрованим. Тобто є короткий момент вразливості мережі.

- Реалізовано усі схеми безпеки. Це означає, що і централізована та розподілена схема захисту імплементуються у кінцевих пристроях і будуть використовується залежно від тієї схеми, яку використовує вся мережа
- Всі криптографічні механізми імплементовані правильно, пристрій дотримується усіх правил безпеки.
- Протокол захисту на кінцевих пристроях реалізований повністю.
- Генератор випадкових чисел, що використовується, є надійним.

Пристрої мережі ZigBee для комунікації використовують мережевий ключ та ключ приєднання. Та сторона, яка отримує повідомлення, знає який саме ключ призначений для його розшифровування.

Мережевий ключ є спільним 128-бітним ключем і використовується для широкомовного мовлення. Всього є два типи мережевих ключів – стандартний ключ та ключ підвищеної безпеки. Останній потребує шифрування коли передається мережею – при ініціалізації мережі або при приєднанні до мережі нових пристроїв. З цією метою використовується ключ приєднання, відомий всім пристроям у випадку застосування розподіленої схеми. У випадку централізованої схеми він використовується між центром довіри і одним вузлом.

Ключ приєднання також є 128-бітним ключем. У розподіленій схемі використовуються два типи ключів приєднання – глобальний та унікальний. У централізованій схемі використовуються три типи ключі приєднання: глобальний (який використовується центром довіри та усіма вузлами мережі), унікальний (відомий тільки центру довіри та одному вузлу), ключ прикладного рівня (використовується між однією парою вузлів). Ключем приєднання, пов’язані з центром довіри є попередньо сконфігурованими поза межами мережі ZigBee. З цією метою можна застосувати QR-код на пристрої. Ключі приєднання між вузлами генеруються центром довіри і шифруються за допомогою мережевим ключем.

При використанні централізованої схеми центр довіри періодично генерує, пересилає та переключає мережеві ключі, що дозволяє мінімізувати час, протягом якого зловмисники змогли б заволодіти мережевим ключем. Потім

новий мережевий ключ шифрується та передається до вузлів. У випадку, коли вузол одержує новий мережевий ключ, то він не замінює старий ключ на новий, а зберігає його. Вузол може зберігати декілька мережевих ключів, а центр довіри ідентифікує поточний мережевий ключ шляхом застосування унікальної послідовності чисел. Подібним чином центр довіри замінює ключ прикладного рівня.

Окрім того, технологія ZigBee передбачає так зване оновлення через повітря OTA (over-the-air updates). Це дає змогу виробникам як оновлювати пристрої, так і після виявлення нових загроз застосовувати нові методи забезпечення безпеки. У технології ZigBee захист OTA є багаторівневим, так як пакет оновлення шифрується унікальним ключем, підписується іншим унікальним ключем, а потім шифрується протягом процесу виготовлення. Це дозволяє розшифрувати пакет оновлення лише кінцевому пристрою. Коли пристрій одержує новий пакет оновлення, то завантажувач операційної системи розшифровує підписи пакету оновлення, валідує їх і лише тоді запускає сам процес оновлення.

Архітектура ZigBee (рис.2.10) включає механізми захисту на таких трьох рівнях: MAC, NWK, APL. На MAC рівні механізм захисту засновано на стандарті IEEE 802.15.4. Ключ для шифрування даних на MAC-рівні базується на відкритій моделі довіри, відповідає активному ключі мережі та встановлюється рівнем вище. На рис. 2.11 подано вихідний MAC-кадр після шифрування.

Аналогічно до MAC-рівня функціонує рівень NWK, який відповідає за маршрутизацію та безпечну передачу пакетів. На рис. 2.12 подано вихідний кадр рівня NWK.

Механізми безпеки прикладного рівня (APL) реалізуються на підрівні APS. Виконання інструкцій із забезпечення безпечної передачі пакетів APS передбачає встановлення ключів та управління ними. На рис. 2.13 подано вихідний кадр рівня APL.

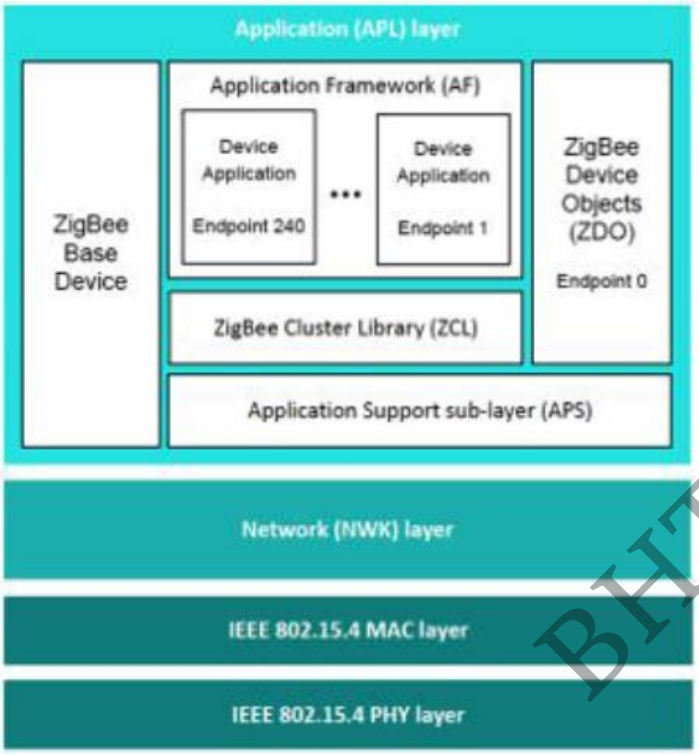


Рисунок 2.10 – Стек архітектури ZigBee

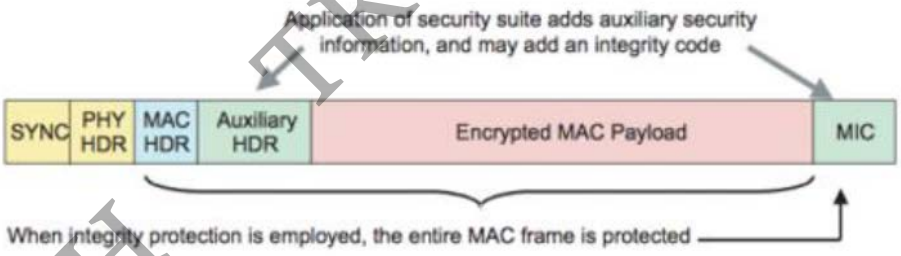


Рисунок 2.11 – Пакет ZigBee з захистом на MAC-рівні

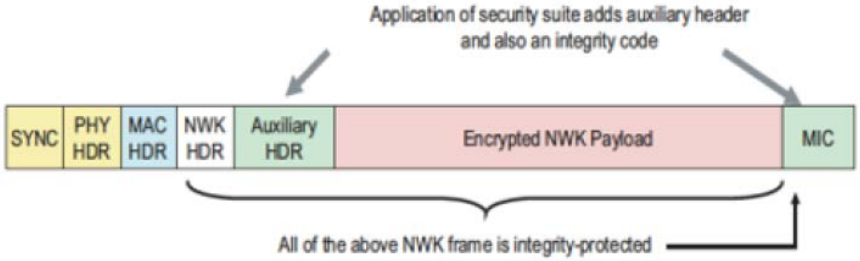


Рисунок 2.12 – Пакет ZigBee з захистом на рівні NWK

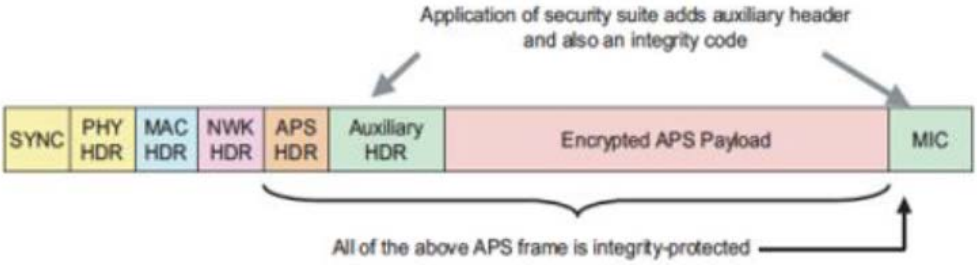


Рисунок 2.13 – Пакет ZigBee із захистом на рівні APL

Для підвищення рівня безпеки окремих вузлів у версії ZigBee 3.0 додано захищений канал на прикладному рівні між парою вузлів мережі, де використовується набір AEC-ключів. Його можна використовувати у домашні сенсорній мережі, де вузлами мережі є замки. Також між цими вузлами можна встановити додатковий рівень захисту за допомогою ключа захищеного каналу на прикладному рівні, що має запобігти відкриванню замків зловмисником після захоплення мережного ключа.

Найбільш очевидною загрозою безпеки мережі ZigBee процес передавання мережевого ключа під час ініціалізації. Розглянемо протестову мережа, яка складається трьох пристроїв: Samsung SmartThings Hub v2, маршрутизатора Centralite Smart Outlet, та магнітного сенсора, який відправляє повідомлення при відкритті/закритті замки Iris Contact Sensor. У процесі перевірки для перехоплення та ін'єкції даних було застосовано модуль Atmel Raven RZUSB 802.15.4, та спеціальне програмне забезпечення: для конвертації перехоплених пакетів у файли libpcap чи Daintree SNA застосовано zbdump; для знаходження мереж ZigBee та IEEE 802.15.4 – zbstumbler; для аналізу перехоплених пакетів – Wireshark.

Протягом тестування було перехоплено перехопити мережевий ключ, що означає повний контроль зловмисника над мережею.

На рис.2.14 зображений перехоплений пакет команди APS в програмі Wireshark. В пакеті було передано зашифрований мережевий ключ. Його було зашифровано із використанням Default Link Key, який публічно відомий. Саме

тому його можна розшифрувати з використанням AEC дешифрування. Результат дешифрування подано на рис.2.15.

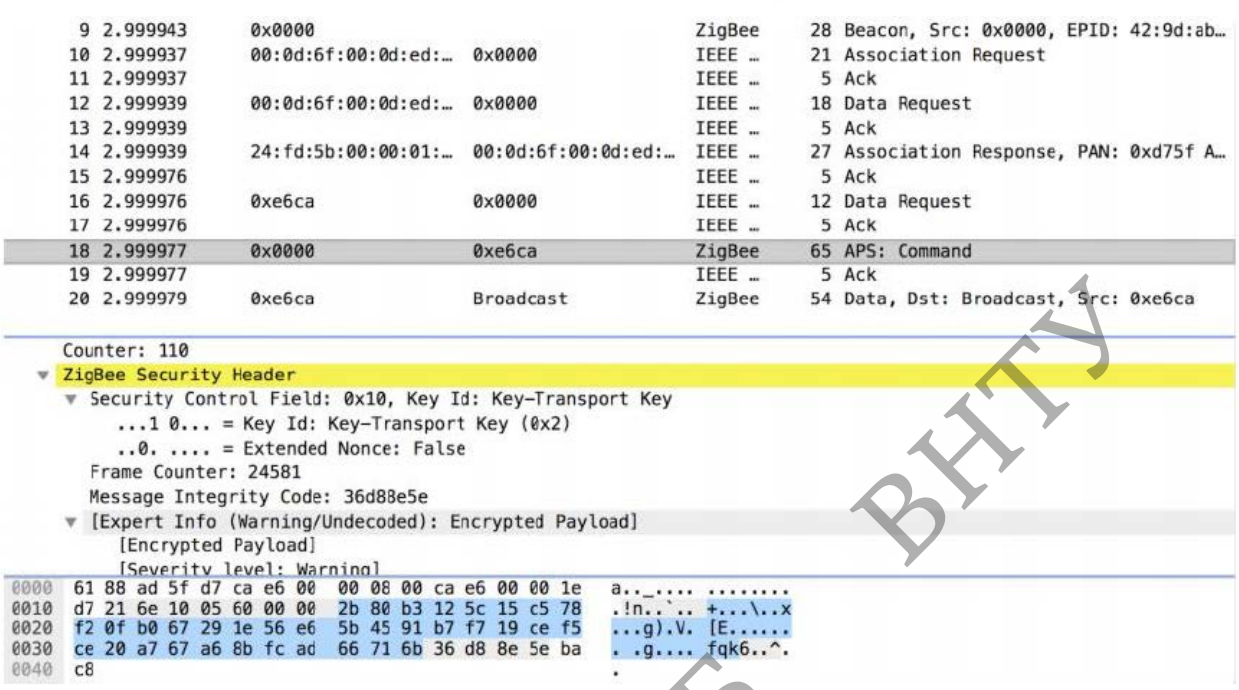


Рисунок 2.14 – Перехоплений пакет команди APS в програмі Wireshark

```
ef bf bd ef bf bd ef bf bd 7d 11 29 23 ef bf bd 3b 44 ef bf bd 0c ef bf bd 45 ef bf
bd 79 ef bf bd 70 30 ef bf bd 1b ef bf bd 3f 44 ef bf bd ef bf bd 5e 49 ef bf bd ef
bf bd ef bf bd e5 bc a3 ef bf bd 1c ef bf bd ef bf bd ef bf bd ef bf bd ef bf bd 75
                                  5f 65 0a
```

Рисунок 2.15 – Дешифрований Default Link Key

Не вдалося реалізувати атаку відтворення, оскільки при використанні лічильника повідомлень, кінцевий пристрій відкидав спеціально надіслані повідомлення від Atmel Raven RZUSB. Однак, можливим є прослідковуваннння номеру останнього повідомлення, а скоригувавши відповідно пакет можна відтворити цей тип атаки.

Мета атаки на підміну пристрою полягала у підкоригувані Association Request. При цьому замінюється MAC адрес на зовнішньому пристрої. Через технічні обмеження, процес відповідь на Association Request і передавання мережевого ключа тривав менше 0,00004 сек. За такий короткий період Atmel Raven RZUSB не було переключено з режиму прослуховування в режим пере-

давання для відправлення пакету про підтвердження приєднання. В той же час, такий тип атаки можна просто легко реалізувати на двох пристроїв Atmel Raven RZUSB, один з яких буде використано для прослуховування, інший – для передачі.

Таким чином, технологія ZigBee характеризується досить строгим режимом безпеки, для шифрування використовуються алгоритми AES. Однак, серйозною проблемою є передача мережевого ключа при ініціалізації мережі та при приєднанні до неї нового пристрою. Окрім того, імплементація протоколу є ненадійною.

Було проведено огляд та аналіз технології ZigBee, яка заснована на стандарті IEEE 802.15.4, що здатен надати надійні та гнучкі механізми безпеки. Було проаналізовано спроби атак на мережу, яка функціонує згідно цього протоколу. Виявлено, що слабким місце у протоколі є момент ініціалізації мережі, так як протягом нього поширюється спільний ключ, і саме в цей момент зловмисники можуть реалізувати атаки прослуховування та підміни вузла. Окрім того, зловмисники можуть ініціювати повторну ініціалізацію мережі та провести атаку.

2.5 Дослідження сенсорної мережі

Розробку сенсорної мережі необхідно розпочинати із з розроблення окремого вузла мережі. За основу візьмемо типовий вузол, який складається з кількох основних елементів (рис. 2.16): блоку збору даних, блоку оброблення даних, передавача, блоку живлення.

В залежності від прикладної задачі сенсорної мережі використовують додаткові модулі. Це можуть система визначення місцезнаходження або силовий генератор. Модуль збору даних складається з двох частин – АЦП та сенсора. Після перетворення в АЦП, сигнал від сенсора передається у блок оброблення. Для під'єднання вузла до мережі слугує передавач.

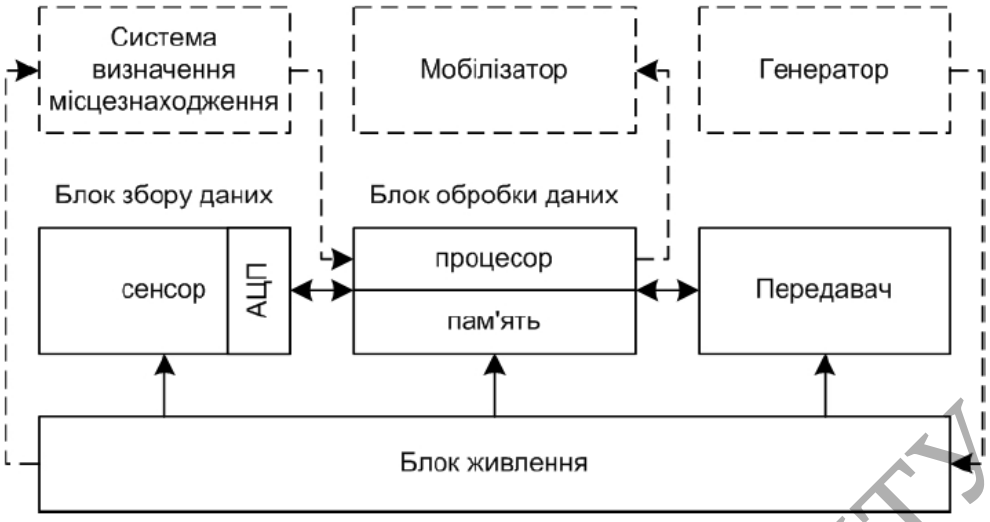


Рисунок 2.16 – Вузол сенсорної мережі

Пропонована функціональна схему вузла сенсорної мережі показана на рис. 2.17. Основним елементом цієї схеми є мікроконтролер, він керує роботою вузла і його елементами. Від сенсора до мікроконтролера через АЦП передаються результати вимірювання. Мікроконтролер обробляє дані, які потім зберігаються у пам'яті або надходять у модуль передавача для передачі. USB-інтерфейс призначений для налаштування мікроконтролера. Живлення модулів здійснюється від автономних джерел живлення. Допоміжними модулями вузла є джерела опорних напруги та частоти.

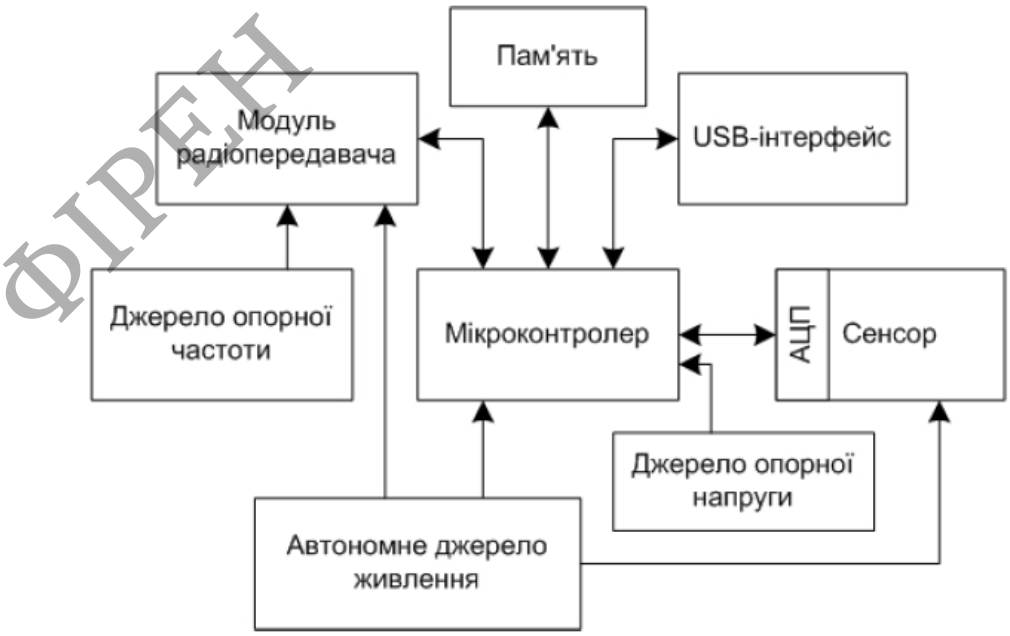


Рисунок 2.17 – Функціональна схема вузла сенсорної мережі

Розглянемо сенсорну мережу, яка працює на частоті 2,4 ГГц і містить малопотужні вузли зі змінною потужністю передавання 0…–5 дБм і чутливістю приймання рівною – 95 дБм. Швидкість передавання даних – 250 кбіт/с. Енергоспоживання вузлів не вище 60 мВт.

Розрахунок залежності потужності сигналу від відстані обчислюється так:

$$P_r = 10\lg\left(\frac{P_t \cdot G_r \cdot G_t \cdot \lambda^2}{(4\pi)^2 \cdot d^2} \cdot 10^3\right),$$

де P_r – потужність сигналу на відстані від передавача, дбм;

P_t – потужність передавача, дБм;

G_r – коефіцієнт підсилення приймача;

G_t – коефіцієнт підсилення передавача;

d – відстань між передавачем і точкою приймання сигналу, м;

λ – довжина хвилі сигналу.

Коефіцієнти підсилення передавача і приймача приймаємо рівними 1.

Звичайно в умовах реального оточення сигнал буде послаблюватися значно сильніше. У такому випадку використовують коефіцієнт послаблення сигналу для різних умов поширення – *n*. Для середовища без перешкод цей коефіцієнт рівний 2 [11], а його максимальне значення – 6.

З урахуванням вище зазначеного і того, що коефіцієнт *n* приймаємо рівним 3 і переписуємо рівняння для приблизного врахування впливу реального середовища на поширення сигналу у такому вигляді:

$$P_r = 10\lg\left(\frac{P_t \cdot G_r \cdot G_t \cdot \lambda^2}{(4\pi)^2 \cdot d^3} \cdot 10^3\right)$$

На рис. 2.18 подано отримані за формулами залежності. Як видно з рис. , у вільному середовищі сигнал послаблюється до рівня чутливості приймача на відстані 300 метрів.

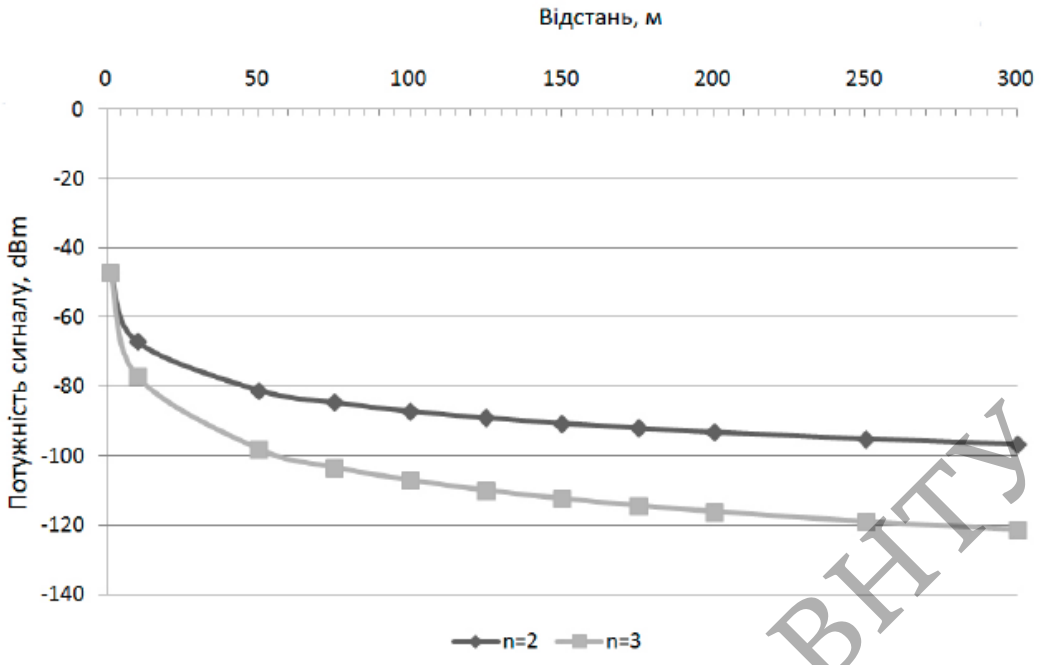


Рисунок 2.18 – Залежність потужності сигналу від подоланої відстані

Результати моделювання якості зв’язку між вузлами, що рівномірно покривають територію подано на рис. 2.19. Так як вузли малопотужними, то досліджувані ділянки можна представити як квадрати. Дев’ять вузлів розташовані приблизно на рівній відстані квадратами 3×3 вузлів. Час моделювання – 100 секунд, протягом цього часу кожен вузол передав 100 повідомлень.

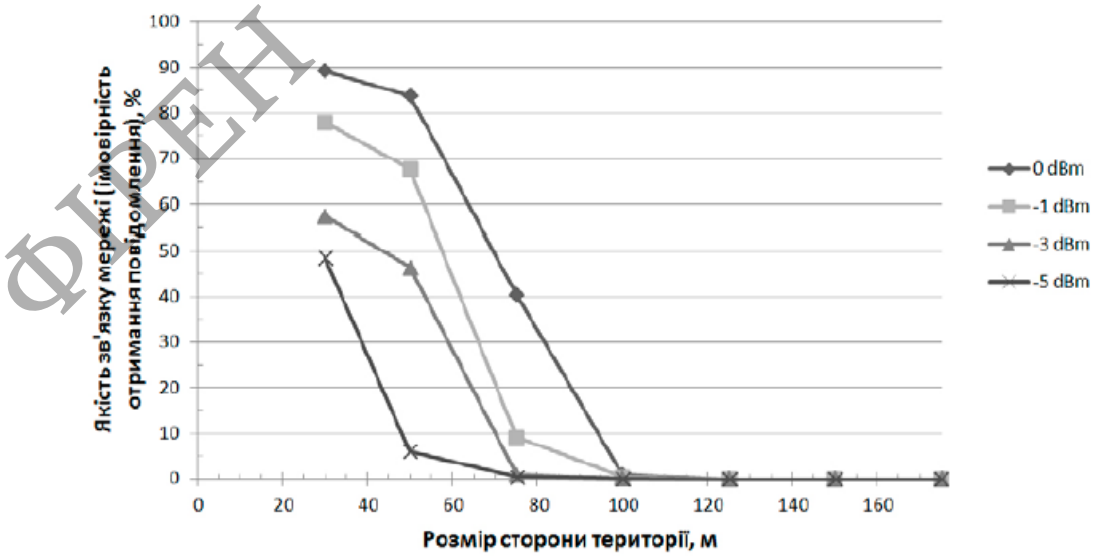


Рисунок 2.19 – Залежність якості зв'язку від розмірів охопленої території

3 ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕНСОРНИХ МЕРЕЖ

На стан безпеки мереж безпроводового зв'язку різних типів впливає суттєве збільшення кількості мобільних пристроїв, сенсорних вузлів та точок безпровідного доступу (ТДБ). Це чинить вплив на розподіл та використання частотного ресурсу, який досить важко зменшити такими методами як централізоване планування безпроводової інфраструктури, регуляторний моніторинг, адаптивні системи налаштування, автокорегування, додаткові пристрої для збору інформації про стан системи.

3.1 Метод модифікованої прямокутної квадратурної амплітудної модуляції

Одним із широко застосованих та простих методів кодування цифрових послідовностей є прямокутна квадратурна амплітудна модуляція. Існує декілька способів знизити впливу широкосмугових каналів, які розташовані в одній смузі частот. До них відносяться рознесення носійних або мереж, застосування направлених антен та згорткових кодів. В той же час, вказані методи не вирішують основну проблему невірно переданих даних, а тільки дозволяють зменшити число помилок.

Для підвищення ефективності використання смуги частот можна застосовувати модифікацію стандартної прямокутної квадратурної амплітудної модуляцію. Завдяки цьому можливо досягнення найбільшої евклідової відстані між базовим і модифікованим векторам (довжини вектору помилки).

Для синхронізації роботи передавача і приймача застосовують службові підканали. На цих підканалах передається інформація стосовно виду вектору – базовий вектор чи модифікований. Зокрема, кожен вид має бути занесений до стандарту, лише після цього можливо використовувати модифікований вектор-

ний простір у промислових масштабах.

Розглянемо варіанти модифікації базового простору комплексних векторів безпровідних підканалів. Основними параметрами є евклідова відстань між векторами у векторному базовому просторі і у векторному модифікованому просторі. Вектор задаємо таким чином:

$$R = Q + i \cdot I ,$$

де Q , I – дійсна і уявна координати відповідно.

Для векторних просторів, призначених для модуляції 2k-QAM, мінімальна відстань між векторами для базового векторного простору – 2000, а зовнішня відстань – 0,000. Віддалення обчислюється так:

$$\Delta_{ном} = r_{вн} - r_{зовн} = 2,000 .$$

У випадку, коли застосовано дві системи з базовим векторним простором, це означає максимальне перекриття. Чим меншим є віддалення, тим більш стабільною буде робота цих систем.

Для нормалізації середньої енергії до одиниці для векторного простору визначають коефіцієнт нормування. Вказаний коефіцієнт відображає енергетичну оптимальність векторного простору. Це означає, чим меншим є коефіцієнт нормування, тим більш оптимального використовується енергія сигналу. Порівнюють можна лише коефіцієнти, котрі відносяться до модуляції одного виду.

Базовий векторний простір описується за допомогою такого виразу:

$$R = \{\pm(2m-1) \pm (2m-1)i\} .$$

При обертанні базового простору на 45° отримується найпростіше перетворення, як показано на рис. 3.1,а.

У першому випадку в кожному із квадрантів збережена симетрія. Якщо ж

нею знехтувати, можливо одержати два перетворення, а саме зміщення проти годинникової стрілки і за годинниковою стрілкою.

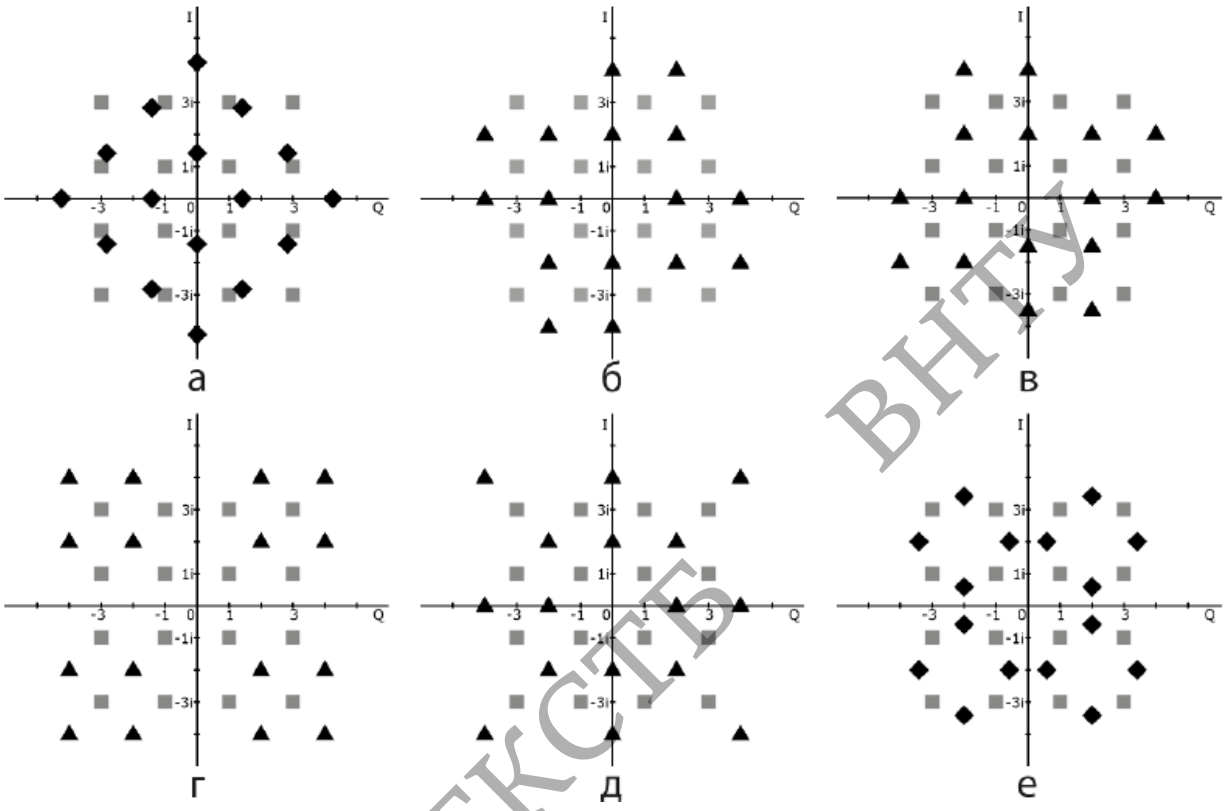


Рисунок 3.1 – Модифікація векторного простору: а) обертання на 45°; б) зміщення проти годинникової стрілки; в) зміщення за годинниковою стрілкою; г) нормальне віддалення від початку координат; д) компактне віддалення від початку координат; е) обертання групи на 45°

Замість простого зміщення застосовують складні більш при реалізації компактні модифікації зміщення, рис. 3.1, д.

У кожному із розглянутих випадків необхідно збільшувати максимальну амплітуду окремих векторів. Базовий векторний простір складається із квадратних елементів, це означає, що кожен елемент може обертатися окремо від інших елементів на 45°.

Якщо замінити дві системи на базовому векторі на системи на базовому і модифікованому векторах, то виграш буде рівний:

$$\delta = \frac{\Delta_б - \Delta_м}{\Delta_б} \cdot 100\%$$

де $\Delta_б$ і $\Delta_м$ – віддалення для базового й модифікованого векторних просторів відповідно.

Підвищення рівня завад призводить до збільшення числа помилок під час приймання сигналу. Селективність фільтра можливо зменшити для кожного вектору. Таке зменшення призводить до зростання кількості помилок, які мають місце у модифікованому просторі векторів. Саме тому, у більшості випадків здійснюють переналаштування на модуляцію з меншим коефіцієнтом *k*. Обидві системи одночасно не потребують переналаштування, так як простори двох векторів – як базового 16-QAM так і модифікованого 64-QAM – не перетинаються.

Найкраща модифікація – це обертання групи. У такому випадку, симетрія буде збережена, а максимальна амплітуда майже не змінюєтьс. Окрім того, при цьому реалізується просте перетворення, котре розподіляється у просторі рівномірно і лишає місце для здійснення третьої модифікації базового векторного простору. Так як енергетична ефективність обертання групи дуже подібна до базового векторного простору, на практиці для вхідних ланок не змінюють коефіцієнти підсилення.

Побудова простору векторів третього та вищих порядків є ще одним етапом оптимізації смуги частот. Ця схема використовується також і для модуляцій типу 256-QAM і 1024-QAM.

3.2 Адаптивний підбор вільних каналів

Адаптивний підбір вільних каналів – це один із методів вирішення проблеми інформаційної безпеки у мережах безпровідного зв’язку. Зазвичай, для цього використовують вбудовані алгоритми автоматичного вибору вільних каналів. Це дозволяє сканувати спектр частот тільки в області розташування то-

чок безпровідного доступу. Особливості розташування клієнтів при цьому не враховуються. Вузол починає працювати на самому вільному каналі, що покращує роботу усієї мережі, хоча і не робить її оптимальною через те, що неможливо врахувати усі параметри сучасних сенсорних мереж, до яких відноссяться висота розташування, поляризація, екранування, перевідбиття. У табл. 3.1 наведено рівні якості сигналу для вузлів.

Таблиця 3.1 – Рівні якості сигналу для пристроїв

Рівень сигналу, дБмВт	Якість	Технічні характеристики
менше -90	Дуже низька	Робота мережі малоймовірна.
від -0 до -81	Низька	Мінімальний рівень сигналу для роботи мережі.
від -80 до -71	Задовільна	Мінімально необхідний рівень сигналу для передачі пакетів.
від -70 до -67	Хороша	Достатній рівень сигналу.
більше -67	Відмінна	Максимально досяжний рівень сигналу.

Для вибору оптимального частотного каналу передачі даних використовують додаткові незалежні пристрої – аналізатори спектру. Ці пристрої утворюють схему, яка складається з вузлів, пристроїв та аналізаторів спектру. Власне аналізатори спектру підключаються до контролера або до користувача (рис.3.2).

Розглянута схема складається із контролера (розподіляє канали й навантаження в мережі, керує інфраструктурою зв’язку), вузла (перемикається у тихий режим), пристрою (збирає дані зі своєї мережевої карти чи з вбудованого аналізатора спектру), аналізатора спектру (передає дані до контролера).

На контролер передається інформація від мережевих карт та від аналіза-

торів спектру. В принципі, формат даних може відрізняється, але можна передати їх до списку каналів з мінімальним рівнем сигналу. Кожен аналізатор спектру характеризується ваговим коефіцієнтом в залежності від важливості свого розташування.

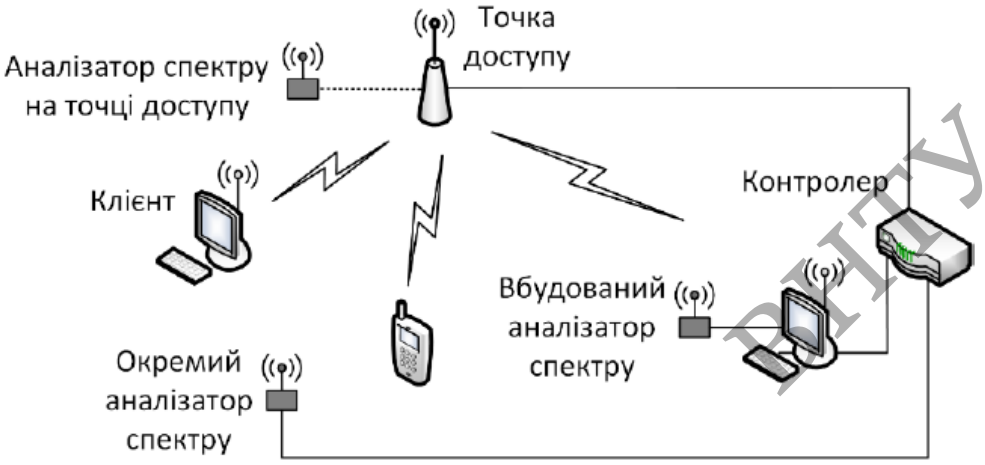


Рисунок 3.2 – Схема з аналізаторами спектру

Контролер обирає вільний канал для кожного вузла, а потім ініціює передачу по новому каналу. Надалі, процес сканування повторюється. На рис. 3.3 зображено алгоритм збору даних.

Рівень сигналу у каналі розраховують таким чином:

$$L_j^{ch} = \frac{1}{N}\sum_{i=1}^{N} L_{ij}$$

де ch –номер каналу передачі;

N – число вузлів, що належать одному каналу;

L_{ij} – це вимірювання в i-му вузлі j-го каналу.

За один цикл вимірювання опитування у кожній точці здійснюється приблизно 100 разів. Замість L_i бажано використовувати середнє виміряне значення.

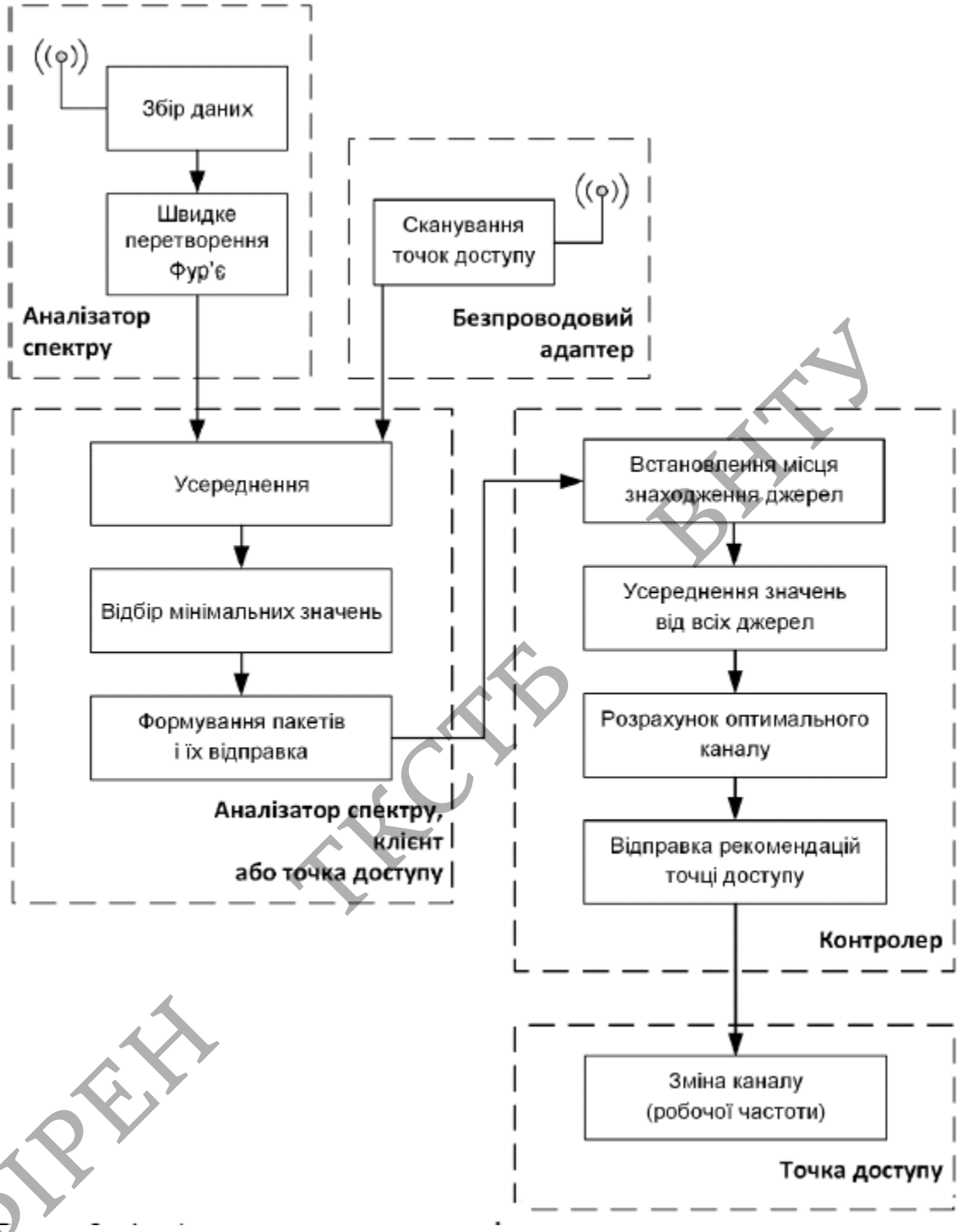


Рисунок 3.3 – Алгоритм динамічного розподілу каналів

Середній рівень сигналу від усіх зовнішніх пристроїв складає:

$$L_{зовн}^{ch} = \frac{1}{M}\sum_{j=1}^{M}\mu_j L_j^{ch},$$

де M – кількість аналізаторів спектра;

μ_j – вага пристрою;

L_j^{ch} –середній рівень сигналу одного пристрою.

Середній рівень сигналів від вбудованих безпровідних адаптерів:

$$L_{вн}^{ch} = \frac{1}{H}\sum_{j=1}^{H}\mu_j \sum_{k=1}^{K} v_k^{ch} L_k ,$$

де H –кількість адаптерів;

K – це число сканованих вузлів;

v_k^{ch} – це коефіцієнт перетинання каналів;

L_k – це рівні сигналу до k-ї мережі.

Існують три варіанти портативних аналізаторів спектру:

1. Приймач і блок керування відокремлені на окремому чіпі.

2. Приймач із визначеним рівнем сигналу на двох станах і блоці керування.

3. Інтегровані безпровідні карти.

Перші два типи аналізаторів спектра працюють разом із пристроями, з вузлом або окремо. Третій тип використовується окремо. Так як у сенсорній мережі можуть бути застосовані різні типи обладнання з різними швидкостями та з різною точністю вимірювання, на етапі збору інформації потрібно проводити уніфікацію.

Підсистема аналізу даних подана на рис. 3.4.

Безпровідна сенсорна мережа може перебувати в одному з трьох станів:

- режим регулярної роботи;
- критичний режимі;
- режим відмови у обслуговуванні.

У випадку, коли у мережу додано підсистему із аналізаторами спектрів, настання критичного режиму є ймовірним, оскільки пристрої на перевантаже-

них вузлах перенаправляються на сусідні вузли не лише за максимальним рівнем сигналу, але й згідно алгоритмів розподілу навантаження.

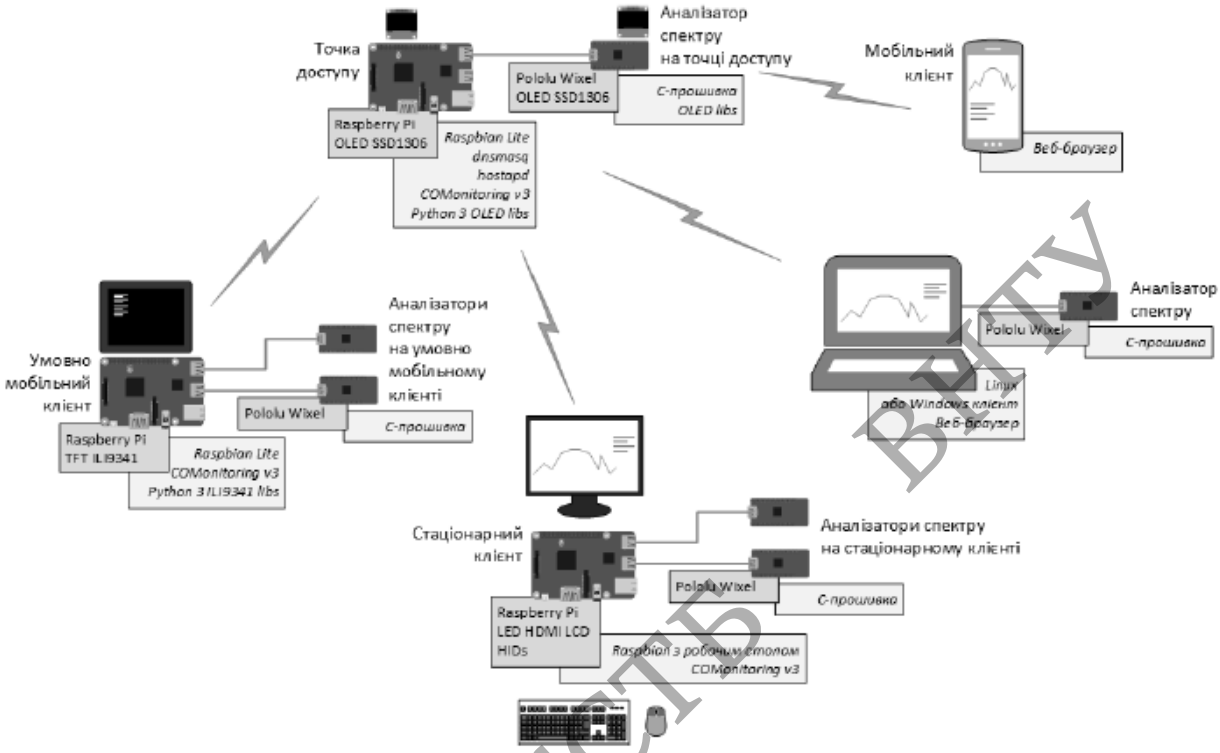


Рисунок 3.4 – Підсистема аналізу даних

Коефіцієнт ефективності визначається так:

$$K = \frac{E}{C},$$

де E – це ефективність,

C – це вартість.

Визначимо вартість сенсорної мережі:

$$C = P_{інф} + P_{обсл},$$

де $P_{інф}$ –вартість інфраструктури;

$P_{обсл}$ –вартість обслуговування.

Вартість системи із аналізаторами спектру:

$$C_{sa} = P_{інф} + P_{обсл} + P_{AC} = C + P_{AC},$$

тут P_{AC} –вартість підсистеми із аналізаторами спектру.

Пристрої можна поділити на три категорії: рухомі; умовно рухомі та нерухомі. Позначимо число рухомих пристрої як $N_{рух}$, умовно рухомих –$N_{умов}$ і нерухомих пристроїв – $N_{нерух}$. Число рухомих пристроїв приблизно дорівнює загальному числу умовно рухомих та нерухомих пристроїв:

$$N_{рух} \approx N_{умов} + N_{нерух}.$$

Вартість підсистеми із аналізаторами спектру:

$$P_{AC} = (N_{умов} + N_{нерух})P_{AC0} + P_{конт},$$

де P_{AC} –вартість аналізатора спектру,

$P_{конт}$ – це вартість контролера, відповідального за збір та аналіз даних з аналізаторів спектру, він надсилає рекомендації на основний контролер.

Вартість інфраструктури залежить від числа пристроїв:

$$P_{інф} \sim N_{рух} + N_{умов} + N_{нерух} + N_{гост},$$

де $N_{гост}$ – кількість гостьових пристроїв.

Позначимо показник відкритості безпровідної мережі через σ

$$N_{гост} = \sigma N_{рух}.$$

Тоді повна кількість пристроїв:

$$N \approx (2+\sigma)(N_{умов} + N_{нерух}).$$

Ефективність сенсорної мережі прямо пропорційна мінімальному часу доступу пристрою до ресурсів вузла:

$$E \sim T_{amin} = \Delta T N_{max},$$

де ΔT – розмір часового вікна передачі,

$N_{\max}$ – це максимально можливе число пристроїв на один вузов.

Ефективність сенсорної мережі із аналізаторами спектру:

$$E_{AC} \sim N_{ТБД} N_{\Delta T},$$

де $N_{\text{ТБД}}$ – це число вузлів.

Якість роботи оцінюється за співвідношенням коефіцієнтів ефективності:

$$\frac{K}{K_{AC}} = \frac{E \cdot C_{AC}}{E_{AC} \cdot C} = \frac{N}{N_{ТБД}} \cdot \frac{1}{N_{max}} \cdot \left(1 + \frac{P_{AC}}{P_{інф} + P_{обсл}}\right).$$

3.3 Метод підвищення функціональної безпеки

Як відомо, поляризаційні параметри електромагнітних хвиль є інформативними. Також, вони можуть проявлятися як мультипликативні завади.

Забезпечення ортогональності сигналів від різних пристроїв обумовлює можливість функціонування багатоканальних систем зв'язку. Це можна виконати за допомогою частотного, часового та кодового розділення каналів або їх комбінації. Застосування просторового рознесення із використанням фазованих антенних граток має досить обмежені можливості. В той же час, стрімке під-

вищення числа пристроїв у сенсорних мережах та їх щільне розташування у приміщенні вимагає пошуку нових шляхів вирішення проблеми перевантаження шляхом розділення одночасно працюючих пристроїв, а також запобігання зниження швидкості передачі інформації та її якості.

Для ортогоналізації сигналів застосовують поляризацію електромагнітної хвилі. Для підвищення інформаційних можливостей мереж зв'язку відомо два напрямки використання поляризаційних властивостей хвиль. Перший напрямок – ущільнення каналу шляхом поляризаційного розділення сигналів, це призведе до підвищення пропускної здатності всієї мережі. Другий напрямок – підвищення пропускної здатності каналу шляхом поляризаційного розділення сигналів при невизначеності поляризаційної структури електричного поля.

На рис. 3.5 наведено приклад розташування циліндричної прискорюючої лінзи. Така лінза працює разом із вертикальним несиметричним вібратором, причому розташування пластин паралельно площині поляризації хвилі.

Як відомо, для стандарту IEEE 802.11b/ g передбачена робота у частотному діапазоні 2,4000…2,4835ГГц, при цому середня довжина хвилі становить $\lambda_{сер}$ 0,123 м.

Рисунок 3.5 – Розташування антени і прискорюючої лінзи

На рис. 3.5 фокусна відстань позначена як *F*,– це максимальна довжина профілю становить $t = t' + t''$, ширина – *d*, – це відстань між окремими пластинами – *a*.

Відстань між пластинами розраховуємо таким чином:

$$a = \frac{\lambda_{сер}}{2\sqrt{1-n^2}} \approx 0,077\,(м),$$

де n –коефіцієнт заломлення прискорюючої лінзи, приймаємо рівним 0,6.

Відстань має відповідати такій умові $\lambda/2 < a < \lambda$. Ширина прискорюючої лінзи для кожного каналу розраховується так:

$$d_5 = 7a_5 = 0,539м,$$
$$d_{12} = 7a_{12} = 0,532м.$$

Фокусна відстань прискорюючої лінзи для кожного каналу визначається так:

$$F_5 \approx d_5 = 0,539м$$

$$F_{12} \approx d_{12} = 0,532м.$$

Приймаємо, що $F \approx d$. Глибина елементів обчислюється таким чином:

$$t'_n = a_n \left| \frac{1}{n+1} - \sqrt{\frac{1}{(n+1)^2} + \frac{1}{4(1-n^2)}} \right|.$$

Максимальний радіус першої зони Френеля знаходимо за формулою:

$$R_{ЗФ} = \sqrt{\frac{r_{пер} \cdot r_{пр}}{r_{пер} + r_{пр}} \lambda_{\max}} = \frac{1}{2}\sqrt{L \cdot \lambda_{\max}} = \frac{1}{2}\sqrt{\frac{c \cdot L}{f_{\min}}},$$

де $r_{пер}$, $r_{пр}$ – це відстані від передавача і приймача до можливої перешкоди відповідно,

λ_{max} – максимальна довжина хвилі.

Приймаємо, що повна відстань між приймачем і передавачем рівна $L = r_{пр} + r_{пер} = 2r$. Перешкода створить максимальний вплив у діапазоні робочих частот при мінімальній частоті і рівновіддаленості від приймача і передавача, тобто за умови $r = r_{пр} = r_{пер} = \frac{1}{2}L$.

Для дослідження впливу прискорюючої лінзи, розташованої на стороні приймача необхідно дослідити експериментальний канал зв'язку між передавачем і приймачем (рис. 3.6). У якості передавач застосуємо Asus RT-N16. Приймач представляє собою пристрій Wifly-city IDU-2850UG-G2000. Для дослідження спектру сигналу застосовано аналізатор спектру Ubiquiti AirView2.

Досліджуваний сигнал має ширину спектру 10 МГц, а модуляція здійснюється за допомогою додаткового коду із однією носійною.

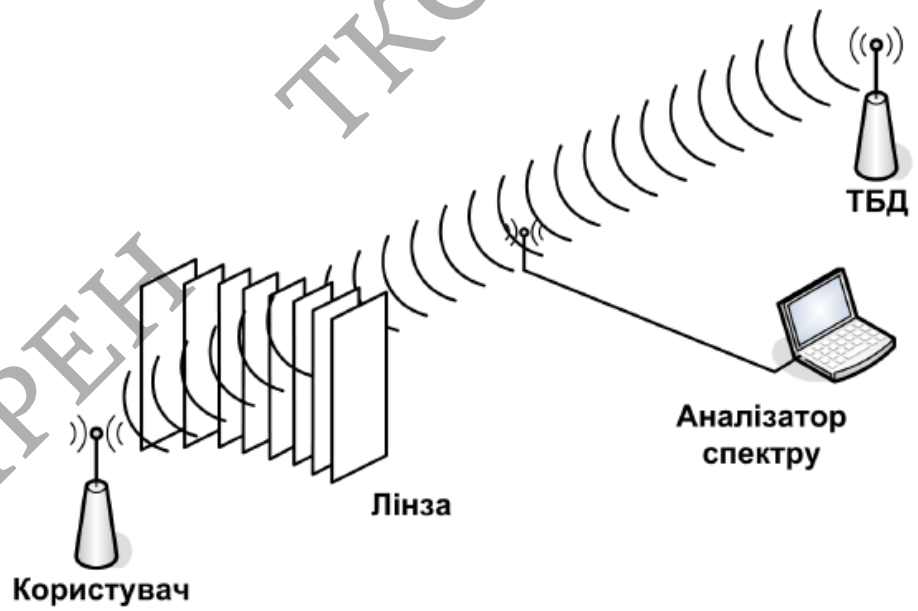


Рисунок 3.6 – Дослідження прискорюючої лінзи (сторона приймача)

Можна розрахувати максимальний радіус першої зони Френеля для відстані $R_{зв}$ = 11 м. Він становить $R_{зФ}1$ = 0,586 м. Прискорююча лінза встановлюється зі стороні приймача. Дані про рівень сигналу наведено на рис. 3.7.

Як показано на рис. 3.7, у сигналах можуть бути нестаціонарні завади. Найбільших значень ці завади набувають на частотах 2,417 та 2,452 ГГц. Стаціонарні завади будуть найбільшими на частотах 2,400 та 2,448 ГГц.

Як можна побачити з кривої із медіанними значеннями, в смузі передачі середнє підсилення сигналу складає 5-7 дБ. Це дозволяє покрити важкодоступні ділянки, віддалені від основної зони покриття приблизно в два рази. При передачі потоку даних з прискорюючої лінзи і без неї швидкість передавання даних була різна. Середній рівень сигналу у випадку без прискорюючої лінзи був рівний -85 дБмВт, а середня швидкість передавання – 680 кбіт/с. При застосуванні прискорюючої лінзи середній рівень сигналу дорівнює -78 дБмВт, а середня швидкість передавання – 710 кбіт/с.

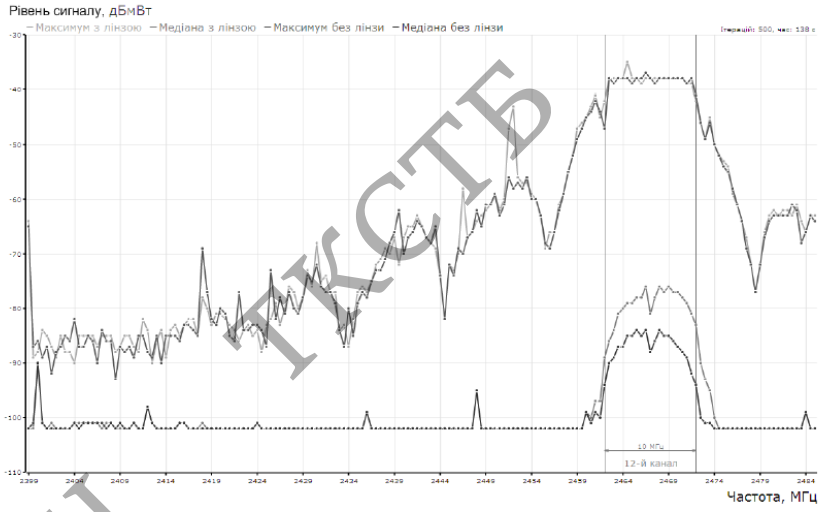


Рисунок 3.7 – Спектр сигналів з прискорюючою лінзою та без прискорюючої лінзи

Отже, застосавання прискорюючої лінзи дозволило покращити швидкісні показники системи на 4%.

Також було вивчено вплив прискорюючої лінзи на дальність прийому при граничній відстані між передавачем і приймачем. На передавальній стороні було встановлено неспрямовану антену, яка має підсилення 5 дБ. На приймальній стороні спрямована антена має підсилення 10 дБ (рис. 3.8).

Передавач розташовано на висоті $h_1 = 8$ м, а приймач – на висоті $h_2 = 2$ м.

Довжина хвилі для 5-го каналу дорівнює λ = 0,123 м. Відстань обирається за такою формулою:

$$P'_{пр} = -175 + 20\lg R_{зв} + P'_{пер} + G'_{пр} + G'_{пер} + \Delta'_{max},$$

де $P'_{пр}$ –чутливість приймача,

$P'_{пер}$ –потужність передавача,

$G'_{пр}$ – підсилення антени приймача,

$G'_{пер}$ – підсилення антени передавача,

Δ'_{max} – максимальна похибка при виготовленні антени.

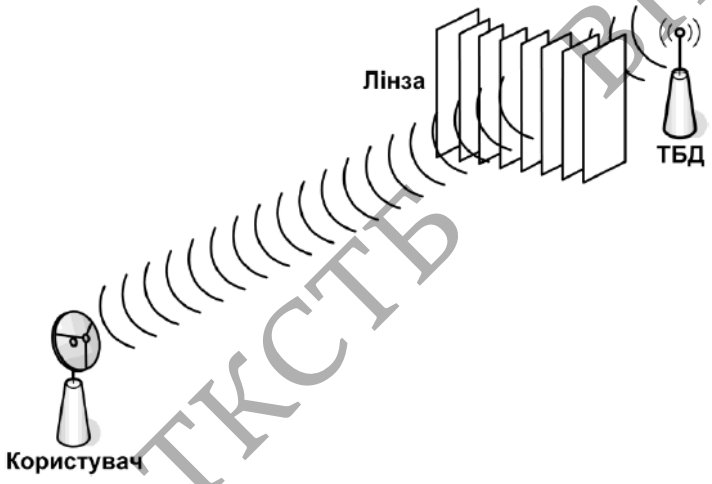


Рисунок 3.8 – Дослідження прискорюючої лінзи (сторона передавача)

Інтервал відстаней, на яких можливий зрив зв'язку, становить від 168 до 188 м. Приймаємо відстань в середині інтервалу $R_{зв}$ = 175 м. Номінальна потужність передавача Asus RT-N16 – 19,5 дБмВт, підсилення стаціонарної антени – 5 дБ, підсилення прискорюючої лінзи – 6 дБ. Потужність випромінювання на приймачі згідно формули Введенського:

$$P'_{пр} = P'_{пер} + G'_{пр} + G'_{пер} - K'_{сер} =$$

$$= P'_{пер} + G'_{пр} + G'_{пер} - 20lg\frac{V}{R_{зв}} - 20\lg f_{сер} - 93 =$$

$$= P'_{пер} + G'_{пр} + G'_{пер} - 20lg\,4\pi\frac{h_1 \cdot h_2}{\lambda \cdot R_{зв}^2} - 160,75,$$

де $K'_{сер}$ – це зниження потужності випромінювання за рахунок впливу Землі т відстані між передавачем і приймачем;

$f_{сер}$ – середня частота, рівна 2,442 ГГц ;

V– це коефіцієнт Введенського,

λ –довжина хвилі, на якій були здійснені вимірювання.

Із попередньої формули отримуємо потужність без прискорюючої лінзи та з прискорюючою лінзою:

$$P'_{пр} = (-96,8 \pm 0,2)\,дБмВт;$$

$$P'_{пр.лін} = (-90,8 \pm 0,2)\,дБмВт.$$

Максимальна чутливість приймача $P'_{пр.max} = -91$ дБмВт. Розрахований максимальний коефіцієнт підсилення склав 14 дБ. Без прискорюючої лінзи маємо $P'_{пр} < P'_{пр.max}$, це означає, що зв'язок неможливий. За наявності прискорюючої лінзи $P'_{пр.лін} < P'_{пр.max}$, тобто – зв'язок є можливим.

Графік зриву передавання даних було побудовано за результатами вимірювання для трьох випадків (рис. 3.9):

1) спрямована антена з коефіцієнтом підсилення у 10 дБ без прискорюючої лінзи;
2) спрямована антена з коефіцієнтом підсилення у10 дБ із прискорюючою лінзою;
3) неспрямована антена із коефіцієнтом підсилення у 5 дБ з прискорюючою лінзою.

Якість зв'язку можна виразити як відношення числа прийнятих пакетів до числа відправлених пакетів. Недосконаліть виготовлення прискорюючої лінзи призводить до появи ефекту часткового екранування та розсіювання (рис. 2.9). Передавання зі спрямованою антеною, що має коефіцієнт підсилення у 10 дБ, демонструє кращі результати, ніж передавання із неспрямованою антени,

що має коефіцієнт підсилення 5 дБ.

Зрив передавання при спрямовані антени з прискорюючою лінзою починається раніше, ніж при неспрямованій антені (рис. 3.10). Цей ефект можна пояснити екрануванням, розсіюванням та нерівномірністю розподілу амплітуд струмів у розкриві лінзи.

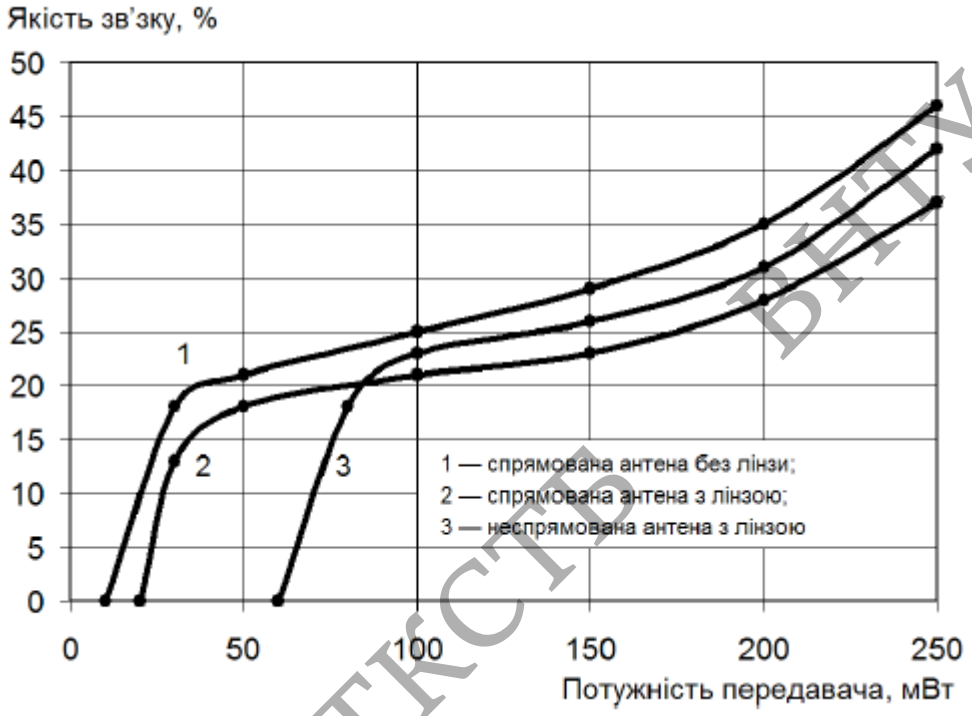


Рисунок 3.9 – Графіки залежності якості зв'язку від потужності передавача

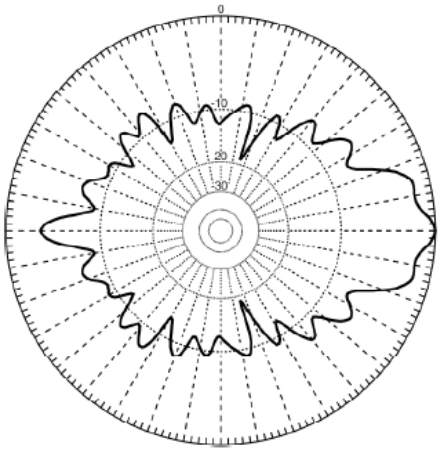


Рисунок 3.10 – Діаграма спрямованості лінзової антени

3.4 Безпечна ідентифікація пристрою

Система ідентифікації як хеш-значення застосовує вектор вагових коефіцієнтів нейронної мережі. Структура системи ідентифікації пристрою наведена на рис.4.1.

Рисунок 3.11 – Структурна схема системи ідентифікації

Так, у блоці перетворення пароля здійснюється формування вхідних даних для нейронної мережі. Основною умовою коректного фукнціонування нейронної мережі є вірно обрана початкова навчальна вибірка. Вона представляє собою деяку множина $\{P_n\}$. Елементи множини є парами вхідних і вихідних векторів $P_i = (X_i, Y_i)$, одержаних з початкових даних. У розглянутій системі ідентифікації початковими даними для навчальної вибірки пароль S^0 заданий користувачем. Для одержання необхідної навчальної вибірку можна застосувати алгоритми перетворення бінарної послідовності у множину навчальних прикладів. Такі алгоритми відповідають слідуючим вимогам:

1) Створена множина $\{P_n^i\}$ має бути унікальною для будь-якого пароля S^i, який представляється як умова:

$$\{P_n^i\} \neq \{P_n^j\} \text{ якщо } S^i \neq S^j, i \neq j, S^i, S^j \in \{S^k\}.$$

2) Однакові елементи P_i повинні бути відсутні, немає бути елементів з однаковими складовими; тобто, всі елементи навчальної вибірки мають відповідати умові функціональності.

Таким вимогам задовільняє алгоритм А1, він забезпечує перетворення бінарної послідовності $\{U_m\}$ в множину дійсних чисел $\{P_n\}$:

1) Розширена бінарна послідовність $\{U_m^*\}$ утворюється шляхом додавання N-1 перших біт до послідовності $\{U_m\}$. Тут N відповідає довжині пароля.
2) Для створення послідовності дійсних чисел $\{V_m\}$ можна використати метод, згідно якого застосовується вікно 16 біт, яке пересувається вздовж розширеної бінарної послідовності із певним кроком. Біти всередині вікна подаються як N-розрядне бінарне число a_i, тут i – поточна позиція вікна. i-й елемент послідовності дійсних чисел $\{V_m\}$ визначається таким чином:

$$v_i = \frac{a_i}{2^N - 1},$$

де $i = 0,...,m-1$.

3) З послідовності $\{V_m\}$ одержують N вхідних векторів, що позначаються як X* .
4) Вихідні значення Y_j^* визначаються за таким виразом:

$$Y_j^* = \frac{\sum_{i=0}^{j} b_i}{\sum_{k=0}^{N-1} c_k},$$

де $j = 0,...,N-1,$

b_i – вікно розміру N, пересувається по бінарній послідовності із кроком N-1;

c_k – вікно розміру N, пересувається по бінарній послідовності із кроком N.

Основний елемент системи ідентифікації – блок ідентифікації. Він будується на базі штучної нейронної мережі прямого поширення (рис.3.12).

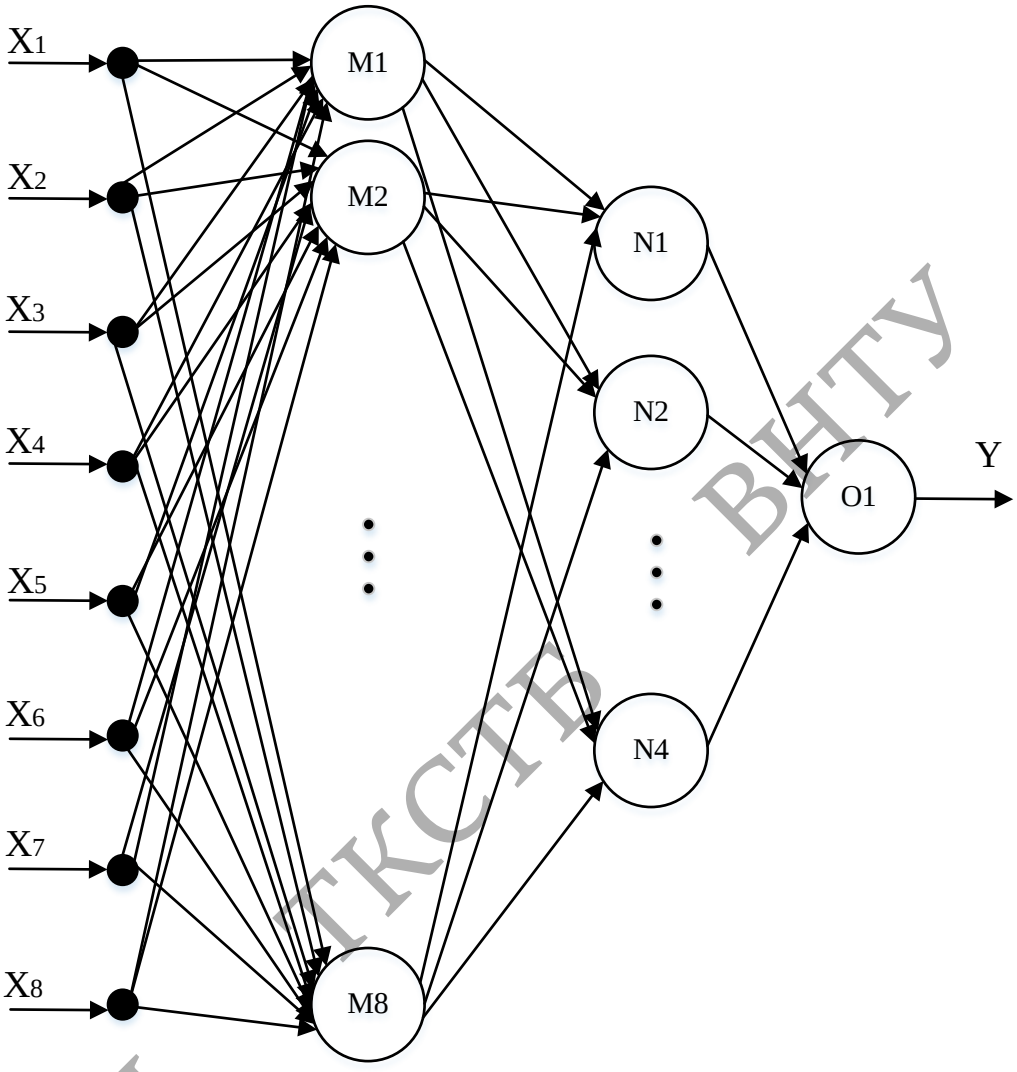


Рисунок 3.12 – Структура нейронної мережі

Використана нейронна мережа є тришаровою, нейрони в ній утворюють пірамідальну структуру. Вихідний шар складається із одного нейрона. Число нейронів вхідного шару дорівнює числу бітів, призначених для визначення однієї літери пароля. Така нейронна мережа може забезпечити як мінімум 100 змінних параметрів. Така розмірність хеш-значень є достатньою.

У процесі функціонування штучної нейронної мережі вхідний вектор X перетворюється у вихідний вектор Y. Вихідний вектор для М-шарової нейронної мережі описується таким рівнянням [7]:

$$Y = \psi^{(M)}(\omega_0^{(M)} + W^{(M)}\psi^{(M-1)}(\omega_0^{(M-1)} + W^{(M-1)}\psi^{(M-2)} \times$$

$$\times(...(\omega_0^{(2)} + W^{(2)}\psi^{(1)}(\omega_0^{(1)} + W^{(1)}X))...))),$$

тут $\psi^{(M)}$ – оператор, який перетворює вхідний вектор згідно функції активації,

$\omega_0^{(M)}$ – вектор порогових вагових коефіцієнтів,

$W^{(M)}$ – матриця вагових коефіцієнтів.

Нейронна мережа реалізує функцію вектора X, яка залежить від вектора вагових коефіцієнтів W. Для знаходження вектора вагових коефіцієнтів W застосовують алгоритми навчання, які відображають процес знаходження тих значень вагових коефіцієнтів, при яких нейронна мережа відображає навчальну вибірку з похибкою ξ. Ця похибка відповідає мірі наближення отриманих вихідних значень до очікуваних вихідних значень [6]. Як алгоритми навчання нейроннної мережі можливо застосовувати детерміновані ітераційні алгоритми, так як вони можуть забезпечити потрібну швидкість роботи.

З метою підвищення надійності роботи системи ідентифікації застосовується алгоритм перемішування вагових коефіцієнтів на базі генератора випадкових чисел. Генератор ініціюється значенням, сформованим на основі пароля – таким чином забезпечуються унікальні перестановки для різних паролей.

Надійність системи ідентифікації визначається хеш-функцією. При цьому, якість хеш-функції визначається стійкістю до криптографічних атак. Такі атаки здійснюються для розкриття пароля, у тому випадку, коли хеш-значення є відомим. До найбільш ефективних видів атак відносять наступні:

1) Атака на однобічність – знаходження вхідного значення x за значеннями h(x) та h;
2) Атака на колізії – знаходження таких значень x', при яких h(x')=h(x).

Атаки на однобічність бувають двох видів – прямі та непрямі [9]. У випадку прямої атаки потрібно знайти алгоритм одержання невідомого вхідного значення або визначити обернену залежність. Пряма атака може бути успішною

лише у деяких випадках, в той час як непряма атака є успішною набагато частіше. Непряма атака представляє собою огляд множини вхідних значень, їх обирають або випадковим чином або згідно визначеного алгоритму. Потім здійснюється порівняння значень хеш-функції, обчислених для кожного із елементів, з шуканими значеннями.

Хеш-значення – це невпорядкований вектор вагових коефіцієнтів. Вектор одержує після процесу навчання штучної нейронної мережі, який здійснюється за допомогою навчальної вибірки. Тобто, за допомогою прямої атаки на однобічність розв'язуються задачі:

1) відновлення вірного розташування вагових коефіцієнтів;
2) визначення входів мережі, задіяних при її навчанні.

При розв'язанні першої задачі необхідно переглянути множини всіх можливих векторів вагових коефіцієнтів. Застосувавши наступні правила, цю множину можна зменшити:

1) значення вагових коефіцієнтів у наступних шарам є вище за відповідні значення у попередніх шарах.
2) сума значень вагових коефіцієнтів для одного нейрона прямує до нуля.

Для перевірки достовірності вектору вагових коефіцієнтів розв'язується друга задача. Для цього слід:

1) визначити для всіх вхідних значень X_i відповідні вихідні значення Y_i.
2) визначити елементи одержаної множини, які можна використати у процесі навчання враховуючи особливості алгоритму.

Пряма атака є простішою за реалізацією, але вона досить рідко успішно завершується. Це пояснити тим фактом, що для кожного елементу множини векторів вагових коефіцієнтів переглядається множина вхідних значень із розмірністю 2^{8N}.

Непряма атака на однобічність хеш-функції, яка будується на основі нейронної мережі, ускладняється через великий час, необхідний для обчислення хеш-значення. Також, для атаки на колізії необхідна велика кількість обчислень хеш-значень та великий обсяг пам'яті для зберігання усіх отриманих значень.

На стійкість мережі до криптографічної атаки впливають наступні особливості хеш-функції на основі нейронної мережі:

1) Розмірність хеш-значення значно більша за розмірність пароля.
2) Хеш-значення має досить високу варіативність.
3) Кореляція відсутня між паролем та отриманим хеш-значенням.

Навчання нейронної мережі є дуже тривалим ітераційним процесом, в ході якого можлива непередбачена зміна вагових коефіцієнтів. Так, при зміні одного біта пароля можлива поява різних вагових коефіцієнтів, що суттєво знижує ймовірність виникнення колізії.

4 ЕКОНОМІЧНА ЧАСТИНА

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Забезпечення інформаційної безпеки сенсорних мереж» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов'язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

4.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Забезпечення інформаційної безпеки сенсорних мереж» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 4.1 та 4.2.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	-	-	-
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	-	55	58

Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв'язок (або знайдено новий зв'язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об'єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	40	-	-
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	-	-	-
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	-	-	-
Середнє значення балів експертів		51,0		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту) та

проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	-	-	-
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	-	-	-
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	55	57	50
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	-	-	-
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	-	-	-
Середнє значення балів експертів	54,0		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як розробка способу (алгоритму, програми), пристрою, отримання нової речовини.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [23]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \quad (4.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 51,0, k_{теор} = 54,0$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 51,0 + 0,4 \cdot 54,00 = 52,20 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж», даний рівень становить 52,20 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж», під час планування, об-

ліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

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

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [23]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

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

t_i – число днів роботи конкретного дослідника, дн.;

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

$$З_о = 11560{,}00 \cdot 21 / 21 = 11560{,}00 \; грн.$$

Проведені розрахунки зведемо до табл. 4.4.

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Забезпечення інформаційної безпеки сенсорних мереж» розраховуємо за формулою:

$$З_p = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (4.3)$$

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

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

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник	11560,00	550,48	21	11560,00
Інженер-дослідник	10105,00	481,19	21	10105,00
Асистент	7860,00	374,29	10	3742,86
Лаборант	6200,00	295,24	5	1476,19
Всього				26884,05

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

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} , \qquad (4.4)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=2379,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [23];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і

підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$T_р$ – середнє число робочих днів в місяці, приблизно $T_р$ = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 2379{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 25{,}70 \text{ грн.}$$

$$З_{р1} = 25{,}70 \cdot 3{,}50 = 89{,}96 \text{ грн.}$$

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Монтаж обладнання	3,50	2	1,10	25,70	89,96
Інсталяція програмних модулів	6,20	4	1,50	35,05	217,30
Моделювання безпровідних сенсорних мереж	12,00	5	1,70	39,72	476,65
Підготовка приміщення	4,00	2	1,10	25,70	102,81
Налаштування обладнання	2,50	4	1,50	35,05	87,62
Демонтаж обладнання	4,00	2	1,10	25,70	102,81
Всього					1077,13

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

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

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 10%.

$$З_{дод} = (26884,05 + 1077,13) \cdot 10 / 100\% = 2796,12 \text{ грн.}$$

4.2.2 Відрахування на соціальні заходи

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

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.6)$$

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

$$Зн = (26884,05 + 1077,13 + 2796,12) \cdot 22 / 100\% = 6766,61 \text{ грн.}$$

4.2.3 Сировина та матеріали

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

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних

математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

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

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \qquad (4.7)$$

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

n – кількість видів матеріалів;

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

K_j – коефіцієнт транспортних витрат, (K_j = *1,1 … 1,15*);

B_j – маса відходів *j*-го найменування, кг;

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

$$M_1 = 3{,}00 \cdot 48{,}00 \cdot 1{,}1 - 0{,}000 \cdot 0{,}00 = 158{,}40 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці 4.6.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір для записів	48,00	3,00	0,000	0,00	158,40
Папір офісний 80 (500) А4	102,00	3,00	0,000	0,00	336,60
Папка Office-iper K8-500	97,00	3,00	0,000	0,00	320,10
Органайзер офісний DATA 5R-XZH	172,00	5,00	0,000	0,00	946,00

Канцелярські товари	203,00	4,00	0,000	0,00	893,20
Картридж ZOFI-F2012	256,00	2,00	0,000	0,00	563,20
Всього					3217,50

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Забезпечення інформаційної безпеки сенсорних мереж», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.8)$$

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

$Ц_j$ – покупна ціна комплектуючих j-го виду, грн;

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

$$К_в = 1 \cdot 104{,}00 \cdot 1{,}1 = 114{,}40 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці 4.7.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Сенсор	1	104,00	114,40
Актор	1	65,00	71,50
АЦП	1	152,00	167,20
Обчислювальна система	1	130,00	143,00

Прийомопередавач	1	111,00	122,10
Пристрій позиціонування	1	67,00	73,70
Пристрій здійснення переміщення	1	110,00	121,00
Блок пам'яті	1	162,00	178,20
Всього			991,10

4.2.5 Спецустаткування для наукових (експериментальних) робіт

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

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.9)$$

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

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

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

k – кількість найменувань устаткування.

$$B_{спец} = 240{,}00 \cdot 1 \cdot 1{,}11 = 266{,}40 \text{ грн.}$$

Отримані результати зведемо до таблиці 4.8:

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Виконавчий ZigBee пристрій	1	240,00	266,40
Виконавчий Wi-Fi пристрій	1	1375,00	1526,25
Виконавчий Bluetooth пристрій	1	2650,00	2941,50
Всього			4734,15

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.10)$$

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

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

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

k – кількість найменувань програмних засобів.

$$B_{прг} = 7360{,}00 \cdot 1 \cdot 1{,}1 = 8096{,}00 \text{ грн.}$$

Отримані результати зведемо до табл.4.9:

Таблиця 4.9 – Витрати на придбання програмних засобів

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
ОС Windows	1	7360,00	8096,00
Пакет Microsoft Office	1	5860,00	6446,00
Пакет моделювання бездротових мереж	1	9402,00	10342,20
Всього			24884,20

4.2.7 Амортизація обладнання, програмних засобів та приміщень

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

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

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

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

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

$$A_{обл} = (19200{,}00 \cdot 1) / (3 \cdot 12) = 533{,}33 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці 4.10.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Персональний комп'ютер	19200,00	3	1	533,33
Прийстрій виводу інформації	6450,00	3	1	179,17
Блок реалізації безпровідної сенсорної мережі	7245,00	3	1	201,25
Місце оператора	6350,00	5	1	105,83
Оргтехніка	7100,00	4	1	147,92
Приміщення лабораторії	240000,00	20	1	1000,00
Всього				2167,50

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \qquad (4.12)$$

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

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е$ = 4,10 грн;

$К_{вп і}$ – коефіцієнт, що враховує використання потужності, $К_{вп і} < 1$;

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

$$В_е = 0,20 \cdot 160,0 \cdot 4,10 \cdot 0,95 / 0,97 = 131,20 \text{ грн.}$$

Проведені розрахунки зведемо до таблиці 4.11.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Персональний комп'ютер	0,20	160,0	131,20
Прийстрій виводу інформації	0,56	3,0	6,89
Блок реалізації бездротової сенсорної мережі	0,04	80,0	13,12
Місце оператора	0,15	80,0	49,20
Оргтехніка	0,42	15,0	25,83
Всього			226,24

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а

також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

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

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

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

$$B_{св} = (26884,05 + 1077,13) \cdot 20 / 100\% = 5592,24 \text{ грн.}$$

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

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

$$B_{сп} = (З_о + З_р) \cdot \frac{H_{сп}}{100\%}, \quad (4.14)$$

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

$$B_{сп} = (26884,05 + 1077,13) \cdot 30 / 100\% = 8388,35 \text{ грн.}$$

4.2.11 Інші витрати

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

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

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \qquad (4.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 60%.

$I_в$ = (26884,05 + 1077,13) · 60 / 100% = 16776,71 грн.

4.2.12 Накладні (загальновиробничі) витрати

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

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

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \qquad (4.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$$В_{нзв} = (26884,05 + 1077,13) \cdot 100 / 100\% = 27961,18 \text{ грн.}$$

Витрати на проведення науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_{о} + З_{р} + З_{дод} + З_{н} + М + К_{в} + В_{спец} + В_{прг} + А_{обл} + В_{е} + В_{св} + В_{сп} + І_{в} + В_{нзв}. \quad (4.17)$$

$В_{заг}$= 26884,05 +1077,13 +2796,12 +6766,606129 +3217,50 +991,10 +4734,15 + 24884,20 + 2167,50 +226,24 +5592,24 +8388,35 +16776,71 +27961,18 = 132463,08 грн.

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

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (4.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

$$ЗВ = 132463,08 / 0,95 = 139434,82 \text{ грн.}$$

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (4.19)$$

де I – коефіцієнт важливості роботи. Приймемо $I = 3$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=3;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 2$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 1$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =139434,82 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів [23].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 3^3 \cdot 2 \cdot 1 \,/\, 139 \cdot 0{,}08 = 4{,}65.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Забезпечення інформаційної безпеки сенсорних мереж» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

4.4 Висновки до розділу

Витрати на проведення науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж» складають 139434,82 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Забезпечення інформаційної безпеки сенсорних мереж» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Розробка спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів. буде відбуватися в приміщені, яке обладнане комп'ютеризованими робочими місцями. На розробника, згідно ГОСТ 12.0.003-74 [25], можуть мати вплив такі небезпечні та шкідливі виробничі фактори:

1. Фізичні: підвищена запиленість та загазованість повітря робочої зони; підвищений рівень шуму на робочому місці; підвищена чи понижена вологість повітря; підвищений рівень статичної електрики; підвищений рівень електромагнітного випромінювання; недостатня освітленість робочої зони.

2. Психофізіологічні: розумове перевантаження; перенапруга аналізаторів; статичне перевантаження.

Відповідно до визначених факторів формуємо рішення щодо безпечного виконання роботи.

5.1 Технічні рішення щодо безпечного виконання дослідження спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів

5.1.1 Обладнання приміщення та робочого місця

Кожен має право на належні, безпечні і здорові умови праці. Це гарантує Конституція України (ч. 4 ст. 43). Більш детальні вимоги щодо охорони праці, зокрема охорони праці під час роботи із використанням ПК, містять Кодекс законів про працю, Закон України «Про охорону праці», а також інші підзаконні нормативно-правові акти. У відповідності до вимог ст. 153 Кодексу законів про працю України та ст. 6 Закону України «Про охорону праці» на всіх підприємствах, в установах, організаціях створюються безпечні і нешкідливі умови праці [31]. Забезпечення безпечних і нешкідливих умов праці покладається на влас-

ника або уповноважений ним орган. Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Власник або уповноважений ним орган повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизму, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників.

Організація робочого місця розробника спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів. передавання повинна забезпечувати відповідність всіх його елементів і їхнього розташування ергономічним вимогам та особливостям трудової діяльності [26].

Робочі місця працівників, обладнані ПК, повинні відповідати вимогам НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. [29]. Правила поширюються на всіх суб’єктів господарювання незалежно від форм власності, які у своїй діяльності здійснюють роботу, пов’язану з персональними комп’ютерами, у тому числі на тих, які мають робочі місця, обладнані персональними комп’ютерами і периферійними пристроями. Зазначені нормативно-правові акти встановлюють санітарно-гігієнічні вимоги до приміщення, в якому розташоване робоче місце, власне до робочого місця, освітлення, рівнів вібрації і шуму, мікроклімату в приміщенні тощо.

5.1.2 Електробезпека приміщення

В приміщенні лінія електромережі для живлення ПК, периферійних пристроїв ПК й устаткування для обслуговування, ремонту й налагодження ПК виконана як окрема групова трипровідна мережа, шляхом прокладання фазових, нульових робочих і нульового захисного провідників. Нульовий захисний провідник використається для заземлення електроприймачів.

Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники. Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники відповідають номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту.

Персональні комп'ютери, периферійні пристрої, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники), електропроводи та кабелі за виконанням і ступенем захисту відповідають класу зони, мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, застосовувати негорючу ізоляцію.

Приміщення, в якому відбуватиметься дослідження за класом електробезпеки – це приміщення без підвищеної небезпеки, оскільки фактори підвищеної та особливої небезпеки на робочому місці відсутні [28].

Покриття плит підлоги гладке, міцне, антистатичне, зручним для очищення пилососом та для проведення вологого прибирання. Необхідно забезпечувати відвід статичних зарядів з покриття підлоги. Для протирання підлоги застосовують рідини, пари яких не утворить вибухо- та пожеженебезпечних сумішей з повітрям і не викликає корозії контактів електричних сполук [29].

Тимчасова електропроводка від переносних приладів до джерел живлення виконується найкоротшим шляхом таким чином, щоб уникнути заплутування проводів у конструкціях машин, приладів і меблів.

5.2 Технічні рішення з гігієни праці та виробничої санітарії

5.2.1 Мікроклімат

Робота розробника спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів передавання згідно за енерговитратами відноситься до категорії 1а [24].

Допустимі параметри мікроклімату для категорії 1а наведені в табл.5.1.

Таблиця 5.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	55	0,1-0,2
Холодний	21-25	75	0,1

Для підтримки оптимального рівня мікроклімату в приміщенні передбачено систему кондиціонування повітря з індивідуальним регулюванням температури, систему центрального опалення та систематичне вологе прибирання приміщення.

5.2.2 Склад повітря робочої зони

В приміщенні, де здійснюється розробка спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів., можливими шкідливими речовинами у повітрі є фенол, пил, озон та вуглекислий газ. Джерелами цих речовин є офісна техніка. Пил потрапляє у приміщення ззовні. ГДК шкідливих речовин, згідно ДСН 3.3.6.042-99 [31] які знаходяться в досліджуваному приміщені, наведені в таблиці 5.2.

Таблиця 5.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Фенол	0,01	0,01	3
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	4
Вуглекислий газ	3	1	4

Параметри іонного складу повітря на робочому місці, що обладнане ПК, повинні відповідати допустимим нормам (табл.5.3).

Таблиця 5.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 см^3	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Забезпечення складу повітря робочої зони здійснюється за допомогою системи кондиціювання, регулярного провітрювання, та вологого прибирання.

5.3 Виробниче освітлення

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2006 [27].

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні (згідно ДБН В.2.5-28-2006 [27]) зазначені у таблиці 5.4:

Таблиця 5.4 – Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$, %			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

Штучне освітлення в приміщенні здійснюється системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення). Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати відблисків на поверхні екрана, а освітленість екрана має не перевищувати 300лк. Як джерела світла в разі штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ.

Для забезпечення достатнього освітлення слід максимально використовувати бічне природного освітлення, систематично очищувати скло від бруду та систематично замінювати перегорілі лампи.

5.4 Виробничий шум

Джерелами шуму під час розробки методів підвищення пропускної здатності телекомунікаційних систем передавання є працююча техніка та транспорт, який рухається ззовні приміщення.

Нормативним документом, який регламентує рівні шуму для різних категорій робочих місць службових приміщень, є ДСН 3.3.6.037-99 [30].

Таблиця 5.5 - Рівень звукового тиску

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньогеометричними частинами (Гц)									Допустимий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Для зниження шуму в приміщенні, необхідно:

– безпосередньо біля джерел шуму використовувати звукопоглинаючі матеріали для покриття стелі та стін;

– для боротьби з вентиляційним шумом потрібно застосовувати мало шумові вентилятори;

– встановити металопластикові вікна, які мають достатню звукоізоляцію.

5.5 Виробничі випромінювання

Робоче місце розробника спектрально-просторових методів виявлення та оцінювання параметрів радіосигналів. передавання обладнане ПК, який є джерелом електромагнітного випромінювання.

Ступінь впливу електромагнітних випромінювань від ПК на організм працівника залежить від діапазону частот, тривалості опромінення, характеру

опромінення, режиму опромінення, розмірів поверхні тіла, яке опромінюється, та індивідуальних особливостей організму.

Електромагнітні випромінювання, випромінювані відеодисплейним терміналом, мають широкий діапазон частот. Відповідно до стандартів, електромагнітне випромінювання повинне бути виміряне в діапазоні частот від 5 Гц до 400 кГц. Гранично допустимі рівні електромагнітного поля для працівника становлять наведені в таблиці 5.6.

Таблиця 5.6 - Допустимі параметри електромагнітних неіонізуючих випромінювань і електростатистичного поля

Види поля	Допустимі параметри поля		Допустима поверхнева щільність потоку енергії, Вт/кв.м
	за електричною складовою (Е), В/м	за магнітною складовою (Н), А/м	
Напруженість електромагнітного поля 60 кГц до 3 мГц	50	5	
Напруженість електромагнітного поля 3 кГц до 30 мГц	20		
Напруженість електромагнітного поля 30 кГц до 50 мГц	10	0,3	
Напруженість електромагнітного поля 30 кГц до 300 мГц 5	5		
Напруженість електромагнітного поля 300 кГц до 300 гГц			10Вт/кв. м
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру УФ-С (220 — 280 мм)			0,001
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру УФ-В (280 — 320 мм)			0,01
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру УФ-А (320 — 400 мм)			10,0
Електромагнітне поле оптичного діапазону в видимій час-			10,0

тині спектру 400 — 760 мм			
Електромагнітне поле оптичного діапазону в інфрачервоній частині спектру 0,76 — 10,0 мкм			35,0 — 70,0
Напруженість електричного поля відеодисплейного терміналу			20кВ/м

Для обмеження впливу ЕМП на розробника слід використовувати лише якісну техніку із сертифікатом якості і дотримуватися встановленого часу роботи за ПК.

5.6. Напруженість праці

Основними показниками напруженості праці є: тривалість зосередження уваги або щільність сигналів, ступінь ризику для власного життя та життя інших осіб або ступінь відповідальності за життя інших осіб, змінність при роботі виключно в нічну зміну.

Гігієнічна оцінка важкості та напруженості праці проводиться шляхом додавання відношень виміряних або розрахованих показників до їх допустимих рівнів, помножених на коефіцієнт значимості показника (1,0 - для основних показників, 0,15 - для допоміжних).

Клас та ступінь важкості й напруженості праці визначаються відповідно до розрахованих балів (сума відношень основних та допоміжних показників до їх нормативних рівнів, помножених на відповідний коефіцієнт) згідно з таблицею 5.7

Найвищі клас та ступінь за факторами «важкість» або «напруженість» трудового процесу - 3 клас, 3 ступінь (особливо важка або особливо напружена праця).[29]

Таблиця 5.7 – Класи умов праці за показниками напруженості праці

№ з/п	Показники напруженості трудового процесу	Класи умов праці			
		оптимальний (напруженість праці легкого ступеня)	допустимий (напруженість праці середнього ступеня)	шкідливий (напружена праця)	
		1	2	3.1	3.2
1	2	3	4	5	6
1*	Інтелектуальні навантаження	-	-	-	-
1.1	Зміст роботи	Відсутня необхідність прийняття рішення	Рішення простих альтернативних завдань згідно з інструкцією	Рішення складних завдань з вибором за алгоритмом (робота за серією інструкцій)	Евристична (творча) діяльність, що вимагає вирішення складних завдань за відсутності алгоритму; особисте керівництво в складних ситуаціях
1.2	Сприймання сигналів (інформації) та їх оцінка	Сприймання сигналів, але немає потреби в корекції дій	Сприймання сигналів з наступною корекцією дій та операцій	Сприймання сигналів з наступним порівнянням фактичних значень параметрів з їх номінальними значеннями. Заключна оцінка фактичних значень параметрів	Сприймання сигналів з наступною комплексною оцінкою взаємопов`язаних параметрів. Комплексна оцінка всієї виробничої діяльності

Продовження таблиці 5.7

1	2	3	4	5	6
1.3	Розподіл функцій за ступенем складності завдання	Обробка та виконання завдання	Обробка, виконання завдання та його перевірка	Обробка, перевірка і контроль за виконанням завдання	Контроль та попередня робота з розподілу завдань іншим особам
1.4	Характер виконуваної роботи	Робота за індивідуальним планом	Робота за встановленим графіком з можливим його коригуванням під час діяльності	Робота в умовах дефіциту часу	Робота в умовах дефіциту часу та інформації з підвищеною відповідальністю за кінцевий результат
2	Сенсорні навантаження	-	-	-	-
2.1	Тривалість зосередження уваги (в % від часу зміни)	До 50	51-75	Більше 75	-
2.2	Щільність сигналів (світлових, звукових) та повідомлень в середньому за 1 годину роботи	До 150	151-300	Більше 300	-
2.3	Навантаження на зоровий аналізатор	-	-	-	-
2.3.1	Розмір об’єкта розрізнення (при відстані від очей до об’єкта розрізнення не більше 0,5 м), мм, % часу зміни	Більше 5 мм 100% часу	5,0-1,1 мм більше 50% часу; 1,0-0,3 мм до 50 % часу; менше 0,3 мм до 25% часу	1,0-0,3 мм більше 50% часу; менше 0,3 мм 25-50% часу	Менше 0,3 мм більше 50% часу, у тому числі з використанням оптичних приладів

Продовження таблиці 5.7

1	2	3	4	5	6
2.3.2	Спостереження за екранами відеотерміналів, годин на зміну	До 2	До 4	> 4,1-6	Більше 6
2.4	Навантаження на слуховий аналізатор (при виробничій необхідності сприйняття мови чи диференційованих сигналів)	Розбірливість слів та сигналів від 100% до 90%	Розбірливість слів та сигналів від 90% до 70%	Розбірливість слів та сигналів від 50% до 70%	Розбірливість слів та сигналів менше 50%
2.5	Навантаження на голосовий апарат, сумарна кількість годин, з напруженням голосового апарату протягом тижня	До 16	Від 16 до 20	Від 20 до 25	Більше 25
3	Емоційне навантаження	-	-	-	-
3.1	Ступінь відповідальності за результат своєї діяльності. Значущість помилки	Є відповідальним за виконання окремих елементів завдання. Вимагає додаткових зусиль в роботі з боку працівника	Є відповідальним за функціональну якість допоміжних робіт (завдань). Вимагає додаткових зусиль з боку керівництва (бригадира, майстра тощо)	Є відповідальним за функціональну якість основної роботи (завдання). Вимагає виправлень за рахунок додаткових зусиль всього колективу	Є відповідальним за функціональну якість кінцевої продукції, роботи, завдання. Неправильні рішення можуть призвести до пошкодження обладнання, зупинки технологічного процесу

Продовження таблиці 5.7

1	2	3	4	5	6
3.2	Ступінь ризику для власного життя та життя інших осіб	Виключений	-	-	Вірогідний
3.3	Ступінь відповідальності за безпеку інших осіб	Виключений	-	Є відповідальним за безпеку	-
4	Монотонність навантажень	-	-	-	-
4.1	Кількість елементів (прийомів), необхідних для реалізації простого завдання або в таких операціях, які повторюються багаторазово	Більше 10	10-6	5-2	-
4.2	Тривалість виконання простих виробничих завдань чи операцій, що повторюються, с	Більше 100	100-25	24-2	-
4.3	Монотонність виробничої обстановки, час пасивного спостереження за технологічним процесом в % від часу зміни	Менше 75	76-90	91-95	-

Продовження таблиці 5.7

1	2	3	4	5	6
5	Режим праці робітників	-	-	-	-
5.1	Тривалість робочого дня, год.	6 або 7	8	Більше 8	-
5.2	Змінність роботи	Однозмінна робота (без нічної зміни)	Двозмінна робота (без нічної зміни)	Тризмінна робота (з роботою в нічну зміну)	Нерегулярна змінність з роботою в нічний час, робота виключно в нічну зміну**

Згідно з наведеними даними таблиці 5.7 при плануванні розпорядку робочого дня і навантаження на працівника потрібно враховувати всі умови оптимальних умов праці.

5.7 Безпека у надзвичайних ситуаціях. Дослідження стійкості роботи сенсорних мереж в умовах дії загрозливих чинників надвичайних ситуацій

Серед потенційно небезпечних виробництв особливе місце посідають радіаційно-небезпечні об’єкти. Вони являють реальну небезпеку для людей, радіоелектронних систем, комп’ютерів тощо. Радіоактивне випромінювання діючи на на матеріали і деталі апаратури комп’ютерних систем приводить до суттєвих змін в їх роботі. Дія іонізуючих випромінювань залежить від виду випромінювання, дози радіації та природи опромінюваної речовини.

Матеріали, які використовуються в електронних елементах (метали, неорганічні матеріали, напівпровідники, діелектрики, смоли та різні органічні сполуки), з яких виготовляється елементи сенсорних мереж по різному реагують на іонізуючі випромінювання. Найбільш чутливі до радіації метали, оскільки їм властива висока концентрація вільних носіїв. Конструювання РЕА стійкої до іонізуючого опромінення передбачає вибір матеріалів та елементної бази, а також конструктивних рішень, які зменшують вплив радіації.

5.7.1 Дослідження стійкості роботи сенсорних мереж в умовах дії іонізуючих випромінювань

Критерієм стійкості роботи сенсорних мереж в умовах дії іонізуючих випромінювань приймається максимальне значення експозиційної дози ($Д_{е.гр}$), при якій можуть виникнути зворотні зміни параметрів елементів, але робота систем ще не порушується.

Вихідними даними для оцінки є максимальне значення потужності дози через одну годину після аварії $р_{1max}$ Р/год; коефіцієнт послаблення радіації виробничими приміщеннями, транспортними засобами, $К_{посл}$. Приймаємо $р_{1max}$= 4,36 Р/год, $К_{посл}$=2; $t_п$=1 год; t_{pmax}=40000 год.

Оцінка проводиться в наступній послідовності.

1. Аналізуються схема сенсорних мереж і елементи від яких залежить її робота. В нашому випадку це мікросхеми, транзистори, конденсатори, резистори. Для кожного елементу визначається максимально допустима експозиційна доза ($Д_{гр.і}$). Дані заносимо в таблицю 5.1. Аналізуємо дані і за мінімальним значенням $Д_{гр.і}$ визначається границя стійкості роботи сенсорних мереж .

2. Визначається можлива експозиційна доза опромінення мережі в заданих умовах протягом експлуатаційного терміну:

Табл. 5.1 – Граничні дози опромінення елементів сенсорних мереж

№	Блоки мережі	Елементи РЕА	$Д_{зві}$, Р	$Д_{звб}$, Р	$Д_{гр}$, Р
1	Живлення	Мікросхеми	10^5	10^4	10^4
		Діоди	10^4		
2	Прийомо-передавач	Конденсатори	10^6	10^6	
		Резистори	10^7		

$$Д_М = \frac{2 \cdot P_{1max} \cdot (\sqrt{t_к} - \sqrt{t_п})}{K_{посл}} = \frac{2 \cdot 4,36 \cdot (\sqrt{40000} - \sqrt{1})}{2} = 867,64\ Р.$$

3. Граничне значення експозиційної дози ($Д_{гр.min}$) порівнюється з $Д_м$, що очікується, і робиться висновок про стійкість роботи мережі. Оскільки $Д_{гр.min} > Д_м$ то сенсорна мережа стійка до радіації.

4. Розраховується допустимий час безпечної роботи сенсорних мереж у заданих умовах:

$$t_д = \left(\frac{Д_{гр.\min} \cdot K_{посл} + 2 \cdot p_{1.\max} \cdot \sqrt{t_п}}{2 p_{1.\max}} \right)^2 = \left(\frac{10^4 \cdot 2 + 2 \cdot 4,36\sqrt{1}}{2 \cdot 4,36} \right)^2 = 2294,578\,(год).$$

Отже, можлива доза опромінення елементної бази мережі складає 867,64 Р, а допустима – 10000 Р. Тож сенсорна мережа є стійкою в умовах дії іонізуючого випромінювання. Допустимий час роботи мережі в заданих умовах становить 2294,578 год., при рівні радіації 4,36 Р/год.

5.7. Дослідження стійкості роботи сенсорних мереж в умовах дії електромагнітного імпульсу

Початкові дані: $E_в$=11,4 кВ/м, $U_ж$=220В; 5В.

Дослідження стійкості роботи сенсорних мереж ведеться в послідовності:

1. Визначається горизонтальна складова напруженості електричного поля

$$E_Г = 10^{-3} \cdot E_В = 10^{-3} \cdot 11,4 \cdot 10^3 = 11,4\ (В/м);$$

2. Бездротова сенсорна мережа розподіляється на окремі функціональні вузли: система живлення, прийомопередавальний блок. На кожній дільниці визначається максимальна довжина вертикальної і горизонтальної струмопровідної частини $l_в$ і $l_г$

На дільниці мережі живлення максимальна довжина вертикальної і горизонтальної струмопровідної частини $l_{в.ж}$=0,13 м, $l_{г.ж}$ = 0,11 м. На дільниці приймопередавального блоку $l_{в.м}$=0,017 м, $l_{г.м}$ = 0,021 м.

3. Для кожної дільниці визначаються наведені напруги у струмопровідних частинах.

На дільниці мережі живлення:

$U_{в.ж} = E_г \cdot l_{в.ж} = 11,4 \cdot 0,13 = 1,08$ (В);

$U_{г.ж} = E_в \cdot l_{г.ж} = 11,4 \cdot 10^3\ 0,11 = 1760$ (В).

На дільниці прийомопередавального блоку:

$U_{в.м}=E_г \cdot l_{в.м}=11,4 \cdot 0,017=0,272$ (В);

$U_{г.м}= E_в \cdot l_{г.м}=11,4 \cdot 10^3\ 0,021=336$ (В).

4. Визначається допустиме коливання напруги живлення

$$U_{Д} = \mathrm{U}_{Ж} + \frac{\mathrm{U}_{Ж} \cdot \mathrm{N}}{100}\,(В),$$

На дільниці мережі живлення:

$$U_{ДЖ} = \mathrm{U}_{Ж} + \frac{\mathrm{U}_{Ж} \cdot \mathrm{N}}{100} = 220 + \frac{220}{100} \cdot 5 = 231\,(В).$$

На дільниці прийомопередавального блоку:

$$U_{ДМ} = \mathrm{U}_{М} + \frac{\mathrm{U}_{М} \cdot \mathrm{N}}{100} = 5 + \frac{5}{100} \cdot 5 = 5{,}2\,(В).$$

5. Визначаються коефіцієнти безпеки

$$K_{БВ} = 20 \cdot \lg \frac{\mathrm{U}_{Д}}{\mathrm{U}_{В}},\ K_{БГ} = 20 \cdot \lg \frac{\mathrm{U}_{Д}}{\mathrm{U}_{Г}}.$$

Для дільниці живлення:

$$K_{БВЖ} = 20 \cdot \lg \frac{\mathrm{U}_{ДЖ}}{\mathrm{U}_{ВЖ}} = 20 \cdot \lg \frac{231}{1{,}08} = 46{,}63 \geq 40\,(дБ);$$

$$K_{БГЖ} = 20 \cdot \lg \frac{\mathrm{U}_{ДЖ}}{\mathrm{U}_{ГЖ}} = 20 \cdot \lg \frac{231}{1760} = -17{,}63 \leq 40\,(дБ);$$

Для дільниці мікропроцесорного блоку:

$$K_{БВМ} = 20 \cdot \lg \frac{\mathrm{U}_{ДМ}}{\mathrm{U}_{ВМ}} = 20 \cdot \lg \frac{5{,}2}{0{,}272} = 33{,}31 \leq 40\,(дБ);$$

$$K_{БГМ} = 20 \cdot \lg \frac{\mathrm{U}_{ДМ}}{\mathrm{U}_{ГМ}} = 20 \cdot \lg \frac{5{,}2}{336} = -28{,}6 \leq 40\,(дБ);$$

6. Результати розрахунків заносимо в таблицю 5.2

Табл. 5.2 Результати розрахунків коефіцієнтів безпеки.

Дільниця мережі	$U_Д$, В	$E_В$, В/м	$E_Г$, В/м	$U_В$, В	$U_Г$, В	$К_{БВ}$, дБ	$К_{БГ}$,дБ
Живлення	231	11400	11,4	1,08	1760	46,63	-17,63
Прийомопередавач	5,2	11400	11,4	0,272	336	33,31	-28,6

7. Дані таблиці аналізуємо і робимо висновки

Коефіцієнти безпеки набагато менше 40 дБ, тому необхідно застосовувати екранування.

5.8 Розробка заходів по підвищенню стійкості роботи сенсорних мереж в умовах надзвичайних ситуацій

Тож сенсорна мережа є умовно стійкою в умовах впливу іонізуючого випромінювання. Допустимий час роботи мережі в заданих умовах становить 2294,578 год., при рівні радіації 4,36 Р/год. Для додаткового захисту можна застосувати підбір радіаційно стійкої елементної бази та перебування мережі в більш захищених приміщеннях.

Від впливу на систему ЕМІ необхідно застосувати додаткове екранування. Визначається перехідне гасіння енергії електричного поля екраном (А, дБ). Для сталевого екрану визначається за допомогою формули

$$A = 5{,}2 \cdot \mathrm{t} \cdot \sqrt{\mathrm{f}}\ ,(\text{дБ}),$$

де t - товщина стінки екрану, см;

f – частота f=15000 Гц.

Для дільниці живлення

$$\text{А}_{\text{ГЖ}}=40-(-17{,}63)=47{,}63\ (\text{дБ}),$$

$$t = \frac{A_{ГЖ}}{5{,}2\sqrt{\mathrm{f}}} = \frac{47{,}63}{5{,}2\sqrt{15000}} = 0{,}074\ (см).$$

Для дільниці мікропроцесорного блоку

$$\text{А}_{\text{ГМ}}=40-(-28{,}6)=68{,}6\ (\text{дБ}),$$

$$t = \frac{A_{ГЖ}}{5{,}2\sqrt{\mathrm{f}}} = \frac{68{,}6}{5{,}2\sqrt{15000}} = 0{,}11\ (см).$$

Отже даному підрозділі досліджувалась стійкість роботи сенсорних мереж в умовах дії в умовах дії іонізуючих випромінювань і електромагнітного імпульсу. В умовах дії іонізуючих випромінювань час роботи мережі перевищив заданий час. В умовах дії електромагнітного імпульсу коефіцієнт безпеки сенсорних мереж для вертикальних струмопровідних частин дільниці живлення

мережі був більший за 40 дБ. В цьому випадку система стійка. Для горизонтальних струмопровідних частин дільниці живлення і для прийомопередавача коефіцієнт безпеки був менший за 40 дБ. Після застосування металевих екранів коефіцієнт безпеки став не менше 40 дБ, а тому система є стійкою до EMI і може працювати без збоїв.

ВИСНОВКИ

У даній роботі було проаналізовано відомі механізми забезпечення інформаційної безпеки сенсорних мереж та проведено аналіз проблемних місць, розглянуто способи їх подолання.

Було розглянуто основні вимоги до механізмів забезпеченя інформаційної безпеки в сенсорних мережах, таких як аутентифікація, актуальність, цілісність, доступність та конфіденційність даних, самоорганізація вузлів мережі. Описано обмеження, які накладаються на розробників сенсорних мереж при реалізації процедур з0абезпечення безпеки.

Було проведено огляд та аналіз технології ZigBee, яка заснована на стандарті IEEE 802.15.4, що здатен надати надійні та гнучкі механізми безпеки. Було проаналізовано спроби атак на мережу, яка функціонує згідно цього протоколу. Виявлено, що слабким місце у протоколі є момент ініціалізації мережі, так як протягом нього поширюється спільний ключ, і саме в цей момент зловмисники можуть реалізувати атаки прослуховування та підміни вузла. Окрім того, зловмисники можуть ініціювати повторну ініціалізацію мережі та провести атаку.

У роботі обгрунтовано використання методу адаптивного підбору вільних каналів передачі даних в безпровідних сеснорних мережах, що дозволить отримувати оперативну інформацію про стан ефіру, у режимі реального часу виявляти можливі завади і несанкціонований вплив, а також підвищити стійкість та інформаційну безпеку сенсорних мереж.

Було розглянуто метод так званої модифікованої прямокутної квадратурної амплітудної модуляції, використовуючи можна зменшити взаємний вплив мереж та підвищити максимальну просторову розв’язку сусідніх сузір’їв.

Для підвищення функціональної безпеки безпровідних сенсорних мереж пропонується застосовувати прискорюючі лінзи, їх конструкція адаптується до багатопроменевих систем. Їх поляризаційні властивості чинять вплив на цілісність інформації, що дає змогу узгодити за поляризацією антенні системи пере-

давача і приймача, а також сприйяють зростанню потужності електромагнітної хвилі у точці прийому та збільшенню пропускної здатності.

Для розв'язанння задачі ідентифікації пристрою сенсорної запропоновано застосовувати інтелектуальні технології, а саме – штучну нейронну мережу. У розглянутій системі ідентифікації вхідний пароль згідно алгоритму перетворюється у навчальною вибірку нейроннної мережі.

В економічній частині роботи були розрахована вартість розробки, виробнича собівартість, ціна реалізації та термін окупності нового пристрою.

В розділі "Безпека життєдіяльності" проаналізовані умови праці в лабораторії для досліджень, виконано організаційно-технічні, санітарно-гігієнічні заходи та протипожежні заходи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, T. Radivilova and D. Ageyev, "Secure Based Traffic Engineering Model in Softwarized Networks," 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 143-147, doi: 10.1109/ATIT50783.2020.9349301.
2. T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh, V. Bulakh and P. Zinchenko, "Intrusion Detection Based on Machine Learning Using Fractal Properties of Traffic Realizations," 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 218-221, doi: 10.1109/ATIT49449.2019.9030452.
3. D. Ageyev, O. Bondarenko, W. Alfroukh and T. Radivilova, "Provision security in SDN/NFV," 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2018, pp. 506-509, doi: 10.1109/TCSET.2018.8336252.
4. Борисенко А.С., Галкин П.В. Адекватность моделей беспроводных сенсорных сетей в сре-дах имитационного моделирования // Восточно-Европейский журнал передовых техноло-гий. – 2013. – № 4/ 9 (64). – С. 52–55.
5. Алгулиев Р. .М. Сенсор.ные сети: состояние, решение и перспективы / Р.М. Алгули.ев, Т.Х. Фаталиев, Б.С. Агаев, Т.С. Алиев // ISSN 1684-2588 Телекоммун.икации. Ежемесячный научно-технический информацио.нно-аналитический и учебно-методический журнал. — 2013. — № 4.. — С. 27—32.
6. Горяєва С.М.. Застосування сенсорних мереж зв’язку для дистанційного контролю психічного стану рятувальника / С.М. Горяєва, Г.В. Щербак // Проблеми екс.тремальної та кризової психології. Збірник наукових праць. Вип. 3.Ч..1. — Х.: УЦЗУ, — 2012. — С. 122—126.

7. Тимченко О.В., Зеляновський М.Ю. Методи і протоколи обміну даними сенсорних мереж // Зб. наук. пр. ІПМЕ НАН України. – Вип.46. – К.: 2008. – С. 176–183.
8. Побудова та моделювання сенсорних мереж на сучасних інформаційних технологіях та забезпечення їх інформаційної безпеки / С. В. Толюпа, Л. Т. Пархуць, О. М. Власов // Наукові записки Українського науково-дослідного інституту зв'язку . – 2011. – № 4. – С. 9–14.
9. Зеляновський М.Ю., Тимченко О.В. Інтелектуальна система для бездротових спеціалізованих сенсорних та мереж персонального радіусу дії: програмно-апаратна платформа вузла бездротової мережі // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.49. – К.: 2008. – С. 185–193.
10. Габарчук В. Кибернетический подход к проектированию систем защиты информации / В. Габарчук, З. Зинович, А. Свиц – К.: Киев-Луцк-Любляны, 2003. – 653 с.
11. Щербаков В. Б Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.
12. Замула О. А. Застосування теорії нечітких множин та лінгвістичної невизначеності при оцінюванні ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш, О. І. Аніщенко // Системи обробки інформації. - 2011. - Вип. 5. - С. 152-155.
13. Москаленко А. О. Дослідження механізмів забезпечення інформаційної безпеки в існуючих та перспективних системах рухомого зв’язку А. О. Москаленко, О. В. Федін // Наука і техніка Повітряних Сил Збройних Сил України. - 2013. - № 1. - С. 99-103.
14. Корсунский А. С. Способ аутентификации вызовов корреспондентов в сетях подвижной радиосвязи с кодовым разделением каналов / А. С. Корсунский // Труды 63-й конференции, посвященной дню радио.– СПб. : СПбГЭТУ ЛЭТИ, 2008. –458 с.

15.Особенности декодера турбокода в программируемых радиостанциях при воздействии помех / С.П. Ливенцев, С.В. Зайцев, С.В. Кныр [и др.] // Зв'язок. – 2007. – № 2. – С. 31 – 35.

16. Зайцев С.В. Анализ пропускной способности дискретно-непрерывного канала связи для программируемых радиостанций с цифровыми методами модуляции сигнала при воздействии организованных помех / С.В. Зайцев // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2006. – № 2 (13). – С. 27 – 32.

17.Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков. – М.: Изд-во НИЯУ МИФИ, 2012. – 400 с.

18. Костів Ю.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / Ю.М. Костів, В.М. Максимович, М.М. Мандрона, О.І. Гарасимчук // Комп'ютерні технології друкарства. – Львів : Вид-во Української академії друкарства. – 2013. – Вип. 29. – С. 167-174.

19.Одарченко Р.С Гнатюк В.А. Концептуальні засади підвищення рівня кібербезпеки сучасних стільникових мереж // Безпека інформації. - 2016. - Т. 22, № 2. - С. 143-149.

20.Одарченко Р.С. Обгрунтування основних вимог до систем безпеки стільніковіх мереж 5-го поколения. - Безпека информации. Віп №3 (Том 21) - 2015., С. 229-235

21.Богдан В. П. Блокування засобів стільникового зв'язку і бездротового доступу / В. П. Богдан // Сучасна спеціальна техніка. - 2013. - № 1. - С. 100-107

22. Бех С. В. Використання принципів квантової теорії вимірювальних перетворень для побудови оригінальних засобів радіоелектронної боротьби з радіоканалами безпілотних розвідувальних систем / С. В. Бех, І. В. Троцишин, Н. І Троцишина. // Вимірювальна та обчислювальна техніка в технологічних процесах. –2015. -№ 3. – С. 217 - 224.

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

24. Наказ від 08.04.2014 № 248 Про затвердження Державних санітарних норм та правил Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/topiccatalogua/labor-protection/14._nakazy_ta_rozpor_183575/248+58074-detail.html

25. ГОСТ 12.0.003-74 ССБТ. Опасные и вредные производственные факторы. Классификация. - [Електронний ресурс] - Режим доступу: http://www.znaytovar.ru/gost/2/GOST_12000374_SSBT_Opasnye_i_v.html

26. ГОСТ 12.2.032-78 Система стандартов безопасности труда. рабочее место при выполнении работ сидя. общие эргономические требования - [Електронний ресурс] - Режим доступу: http://www.yondi.ru/inner_c_article_id_1140.phtm

27. ДБН В.2.5-28-2006 Природне і штучне освітлення - [Електронний ресурс] - Режим доступу: http://document.ua/prirodne-i-shtuchne-osvitlennja-nor8425.html

28. ДНАОП 0.00-1.21-98 Правила безпечної експлуатації електроустановок споживачів - [Електронний ресурс] - Режим доступу: http://dnop.com.ua/dnaop/act3167.htm

29. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. - [Електронний ресурс] - Режим доступу: http://sop.zp.ua/norm_npaop_0_00-7_15-18_01_ua.php

30. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972

31. Про охорону праці Закон України від 14.10.1992 № 2694-XII - [Електронний ресурс] - Режим доступу: http://zakon2.rada.gov.ua/laws/show/2694-12

ДОДАТКИ

Додаток А

(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ

д.т.н., професор

В.М.Кичак

“__” _____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

СЕНСОРНИХ МЕРЕЖ

08-34.МКР.004.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Семенова О.О.

Виконавець: ст. гр. ТКС-20м

Замрій О. В.

Вінниця-2021

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “24” 09 2021 року № 277 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 01.09.2021 р.

Дата закінчення: 20.12.2021 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є дослідження механізмів забезпечення безпеки інформації у сенсорних мережах.

Об’єкт дослідження – сенсорні мережі безпровідного зв’язку.

Предмет дослідження – інформаційна безпека в сенсорних мережах безпровідного зв’язку.

Основними завданнями роботи є:

- аналіз принципів забезпечення інформаційної безпеки у сенсорних мережах;
- аналіз проблемних місць у механізмах безпеки та способи їх подолання;
- синтез методів підвищення інформаційної безпеки у сенсорних мережах.

Отримані у ході виконання роботи дані пропонується застосовувати у сенсорних мережах для підвищення ефективності їх функціонування.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Список використаних джерел розробки:

3.1 O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, T. Radivilova and D. Ageyev, "Secure Based Traffic Engineering Model in Softwarized Networks," 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 143-147, doi: 10.1109/ATIT50783.2020.9349301.

3.2 T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh, V. Bulakh and P. Zinchenko, "Intrusion Detection Based on Machine Learning Using Fractal Properties

of Traffic Realizations," 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2019, pp. 218-221, doi: 10.1109/ATIT49449.2019.9030452.

3.3 D. Ageyev, O. Bondarenko, W. Alfroukh and T. Radivilova, "Provision security in SDN/NFV," 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2018, pp. 506-509, doi: 10.1109/TCSET.2018.8336252.

3.4 Борисенко А.С., Галкин П.В. Адекватность моделей беспроводных сенсорных сетей в сре-дах имитационного моделирования // Восточно-Европейский журнал передовых техноло-гий. – 2013. – № 4/ 9 (64). – С. 52–55.

3.5 Алгулиев Р. .М. Сенсор.ные сети: состояние, решение и перспективы / Р.М. Алгули.ев, Т.Х. Фаталиев, Б.С. Агаев, Т.С. Алиев // ISSN 1684-2588 Телекоммун.икации. Ежемесячный научно-технический информацио.нно-аналитический и учебно-методический журнал. — 2013. — № 4.. — С. 27—32.

3.6 Горяєва С.М.. Застосування сенсорних мереж зв’язку для дистанційного контролю психічного стану рятувальника / С.М. Горяєва, Г.В. Щербак // Проблеми екс.тремальної та кризової психології. Збірник наукових праць. Вип. 3.Ч..1. — Х.: УЦЗУ, — 2012. — С. 122—126.

3.7 Тимченко О.В., Зеляновський М.Ю. Методи і протоколи обміну даними сенсорних мереж // Зб. наук. пр. ІПМЕ НАН України. – Вип.46. – К.: 2008. – С. 176–183.

3.8 Побудова та моделювання сенсорних мереж на сучасних інформаційних технологіях та забезпечення їх інформаційної безпеки / С. В. Толюпа, Л. Т. Пархуць, О. М. Власов // Наукові записки Українського науково-дослідного інституту зв'язку . – 2011. – № 4. – С. 9–14.

3.9 Зеляновський М.Ю., Тимченко О.В. Інтелектуальна система для бездротових спеціалізованих сенсорних та мереж персонального радіусу дії: програмно-апаратна платформа вузла бездротової мережі // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.49. – К.: 2008. – С. 185–193.

3.10 Габарчук В. Кибернетический подход к проектированию систем защиты информации / В. Габарчук, З. Зинович, А. Свиц – К.: Киев-Луцк-Любляны, 2003. – 653 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТКС-20м Замрій Олег Володимирович.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати обґрунтування методів підвищення інформаційної безпеки сенсорних мереж.

Технічні вимоги, яким повинна відповідати розробка, наступні:

частота 2,4 ГГц

кількість вузлів – 9

потужність передачі від 0 … –5 дБм

чутливістю приймання – 95 дБм

швидкість передавання – 250 кбіт/с

енергоспоживання вузла – не вище 60 мВт.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документа-ція
		початок	закінчення		
1	2	3	4	5	6
1.	Розробка технічного завдання (ТЗ)	01.09.2021р.	10.09.2021р.	Розроблене ТЗ	Додаток А
2.	Техніко-економічне обґрунтування тематики (ТЕО)	11.09.2021р.	17.09.2021р.	Розроблене ТЕО	Вступ.
3.	Огляд особливостей захисту інформації	18.09.2021р.	01.10.2021р.	Результати досліджень	Розділ 1

1	2	3	4	5	6
4.	Дослідження роботи мережі	02.10.2021р	29.10.2021р.	Схема структурна	Розділ 2
5.	Розроблення методів захисту мережі	30.10.2021р.	19.11.2021р.	Результати досліджень	Розділ 3
6.	Аналіз економічної ефективності розробки	20.11.2021р.	30.11.2021р.	Економічна частина	Розділ 4
7.	Аналіз безпеки життєдіяльності (БЖД), цивільний захист (ЦЗ)	01.12.2021р.	06.12.2021р.	Частина БЖД, ЦЗ	Розділ 4
8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	07.12.2021р.	13.12.2021р.	Оформлена документа-ція	ПЗ та графічна частина
9.	Попередній захист та рецензування МКР	4.12. 2021р.	17.12.2021р.	Позитивні відзиви	Відзив. Рецензія
10.	Захист МКР ДЕК		20.12.2021р.	Позитивний захист	Протокол ДЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- функціональна схема вузда;
- структурна схема нейронної мережі;
- економічна частина МКР;
- розділ безпеки життєдіяльності і ЦЗ.

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій шляхом впровадження нових технологій.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується підвищення попиту на інфокомунікаційні послуги і, відповідно, підвищення їх якості.

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:

- функціональну схему вузла;
- структурну схему нейронної мережі;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання отриманих результатів.

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.

Додаток Б

(обов’язковий)

Класифікація сенсорних мереж

Плакат

Додаток В

(обов’язковий)

Методи виявлення атак

Плакат

Додаток Д

(обов’язковий)

Механізм виявлення вторгнень

Плакат

Додаток Е

(обов’язковий)

Класифікація протоколів управління ключами

Плакат

Додаток Ж

(обов’язковий)

Захищена передача пакетів ZigBee

Плакат

Додаток И

(обов’язковий)

Вузол сенсорної мережі

Плакат

Додаток К

(обов’язковий)

Функціональна схема вузла сенсорної мережі

Плакат

Додаток Л

(обов’язковий)

Залежність потужності сигналу від подоланої відстані

Плакат

Додаток М

(обов’язковий)

Залежність якості зв'язку від розмірів охопленої території

Плакат

Додаток Н

(обов’язковий)

Використання прискорюючої лінзи

Плакат

Додаток П

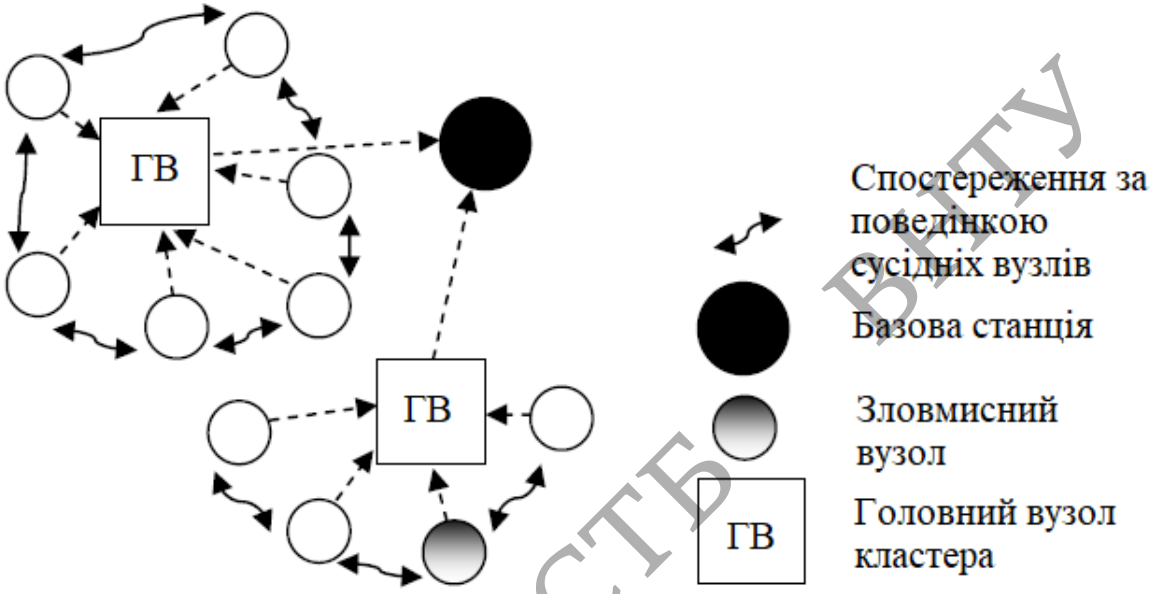
(обов’язковий)

Нейронна мережа

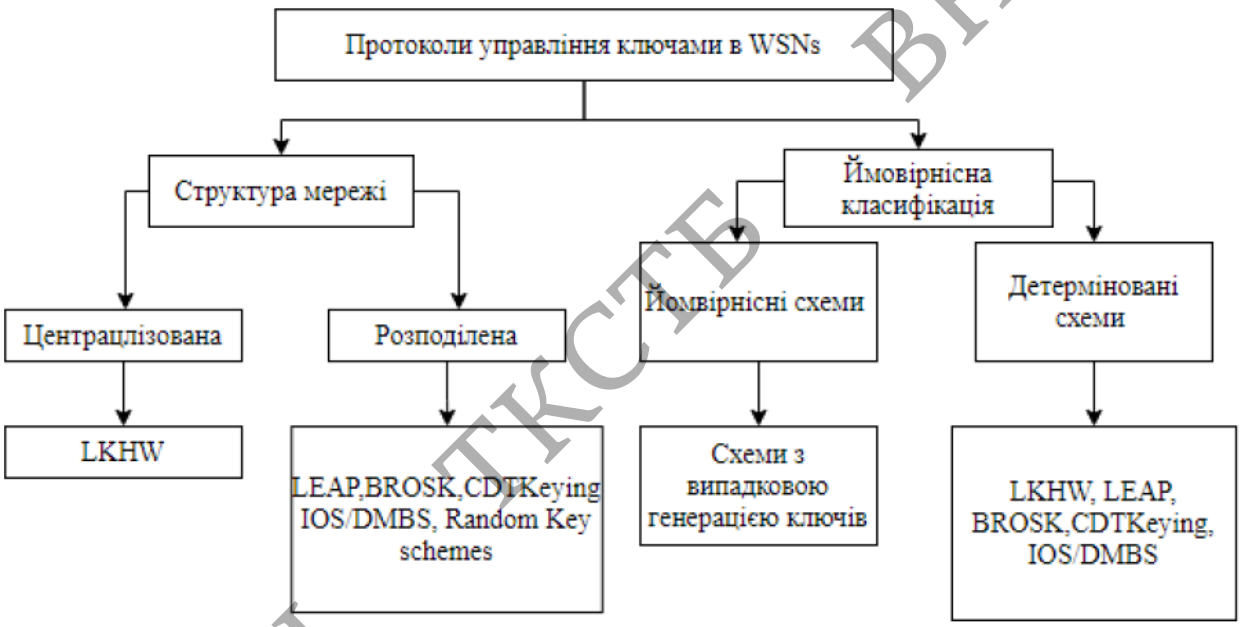
Плакат

					08-34.МКР.004.00.001 Е8		
Змн.	Лист	№ докум.	Підпис	Дата	Класифікація сенсорних мереж Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						

					08-34.МКР.004.00.002 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Методи виявлення атак Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						



					08-34.МКР.004.00.003 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Механізм виявлення вторгнень Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						



					08-34.МКР.004.00.004 Е8			
Змн.	Лист.	№ докум.	Підпис	Дата	Класифікація протоколів управління ключами Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
						ВНТУ, ТКС-20м		
Н.Контр.		Семенова О.О.						
Затверд.		Кичак В.М.						

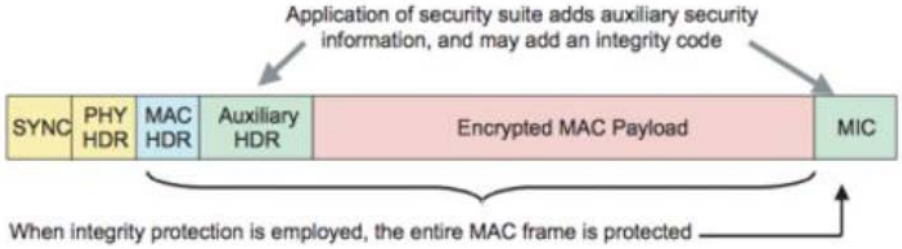


Рисунок 1 – Пакет ZigBee з захистом на MAC-рівні

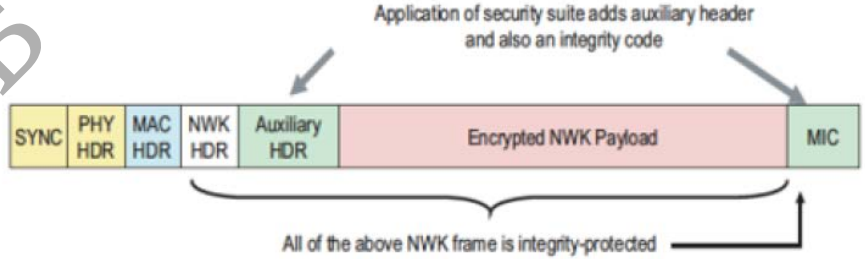


Рисунок 2 – Пакет ZigBee з захистом на рівні NWK

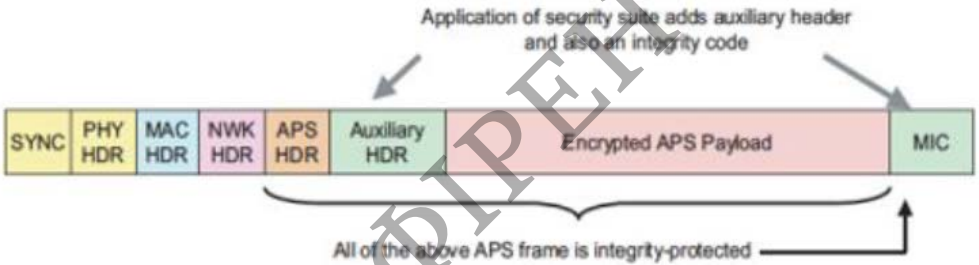
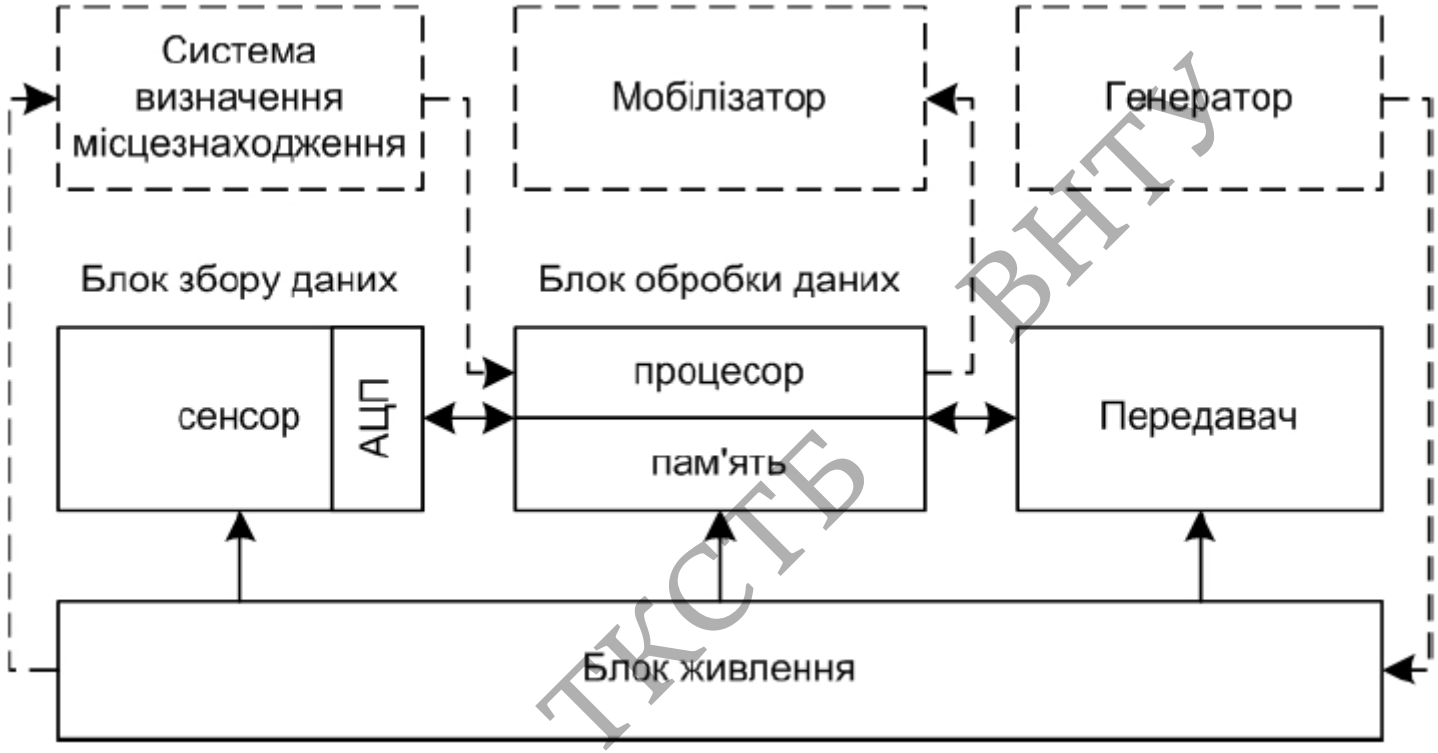
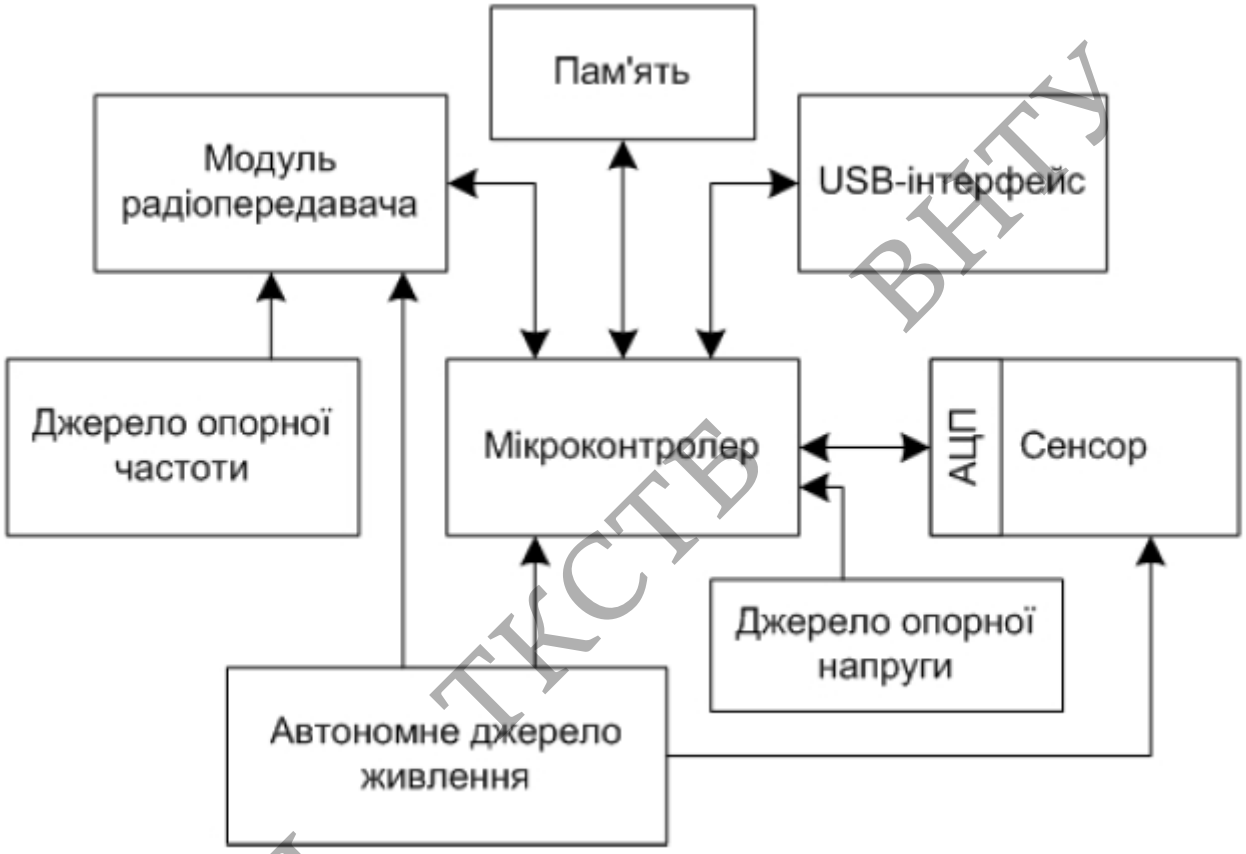


Рисунок 3 – Пакет ZigBee із захистом на рівні APL

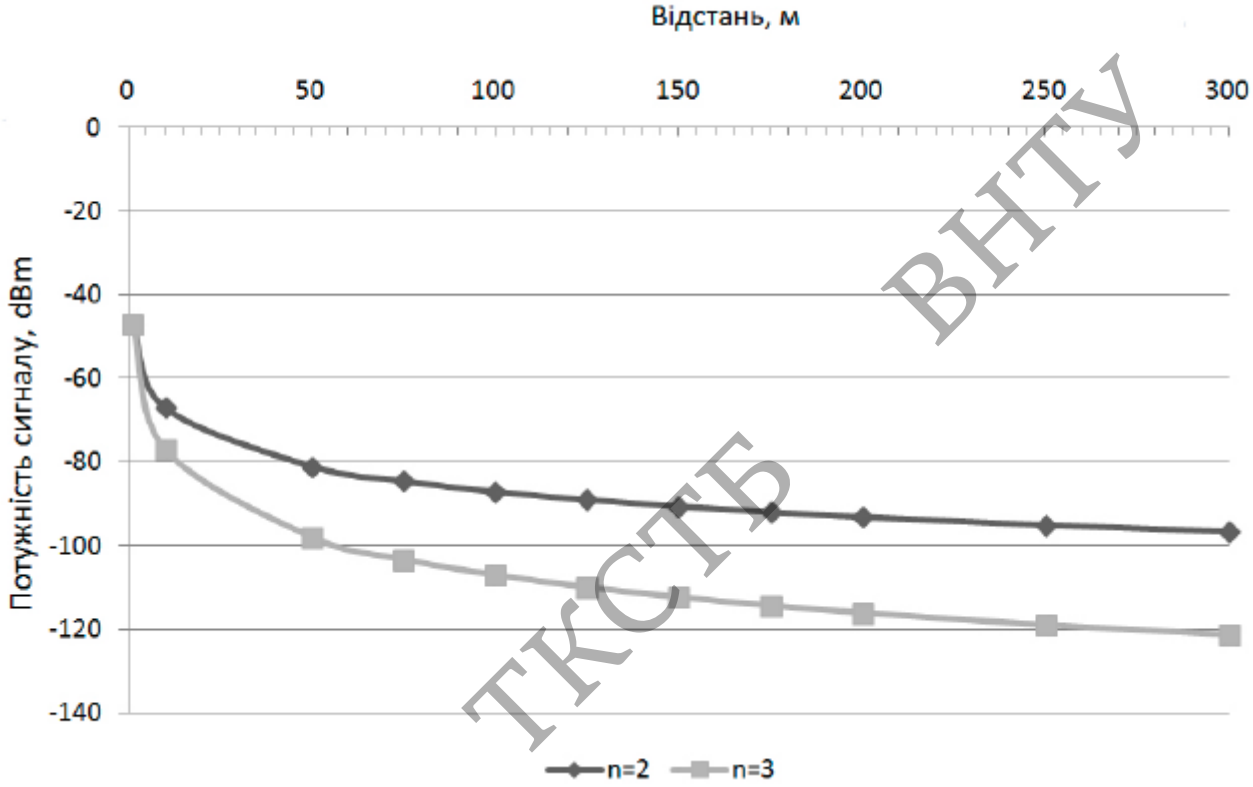
					08-34.МКР.004.00.005 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Захищена передача пакетів ZigBee Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук В.С.				ВНТУ, ТКС-20м		
Н.Контр.		Семенова О.О.						
Затверд.		Кичак В.М.						



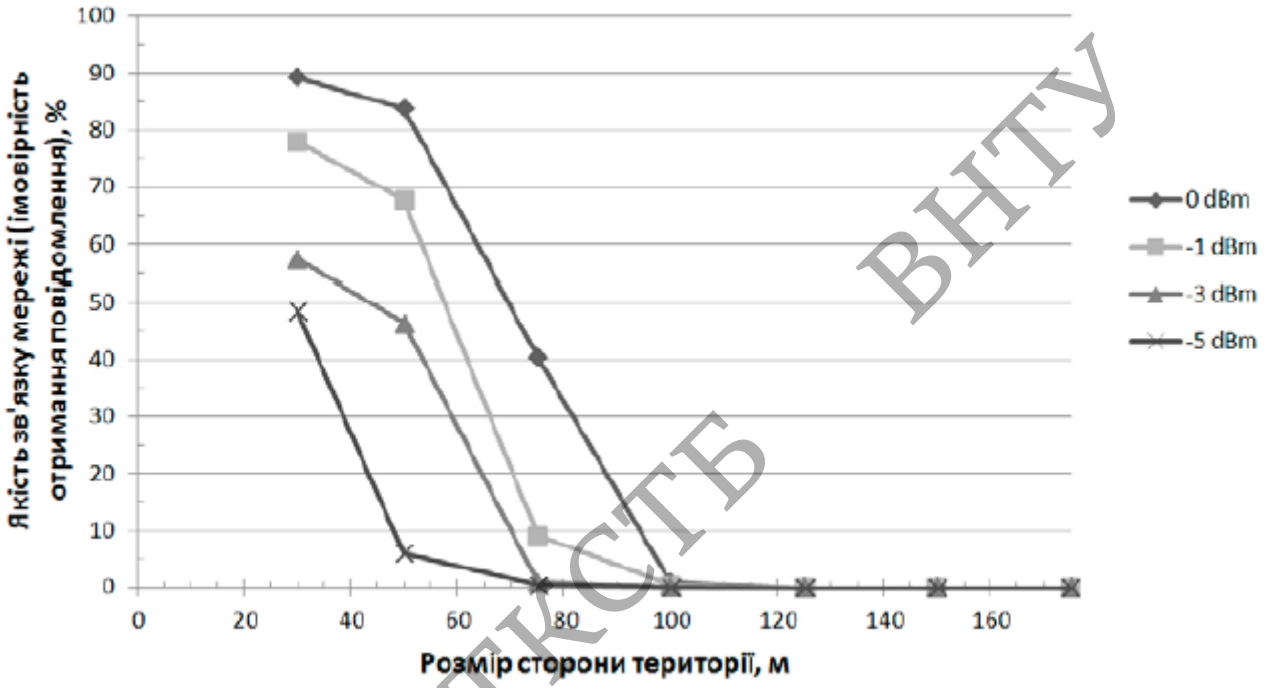
					08-34.МКР.004.00.006 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Вузол сенсорної мережі Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						



					08-34.МКР.004.00.007 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Функціональна схема вузла сенсорної мережі Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук В.С.				ВНТУ, ТКС-20м		
Н.Контр.		Семенова О.О.						
Затверд.		Кичак В.М.						



					08-34.МКР.004.00.008 Е8			
Змн.	Лист	№ докум.	Підпис	Дата	Залежність потужності сигналу від подоланої відстані Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						



					08-34.МКР.004.00.009 Е8			
Змн.	Лист.	№ докум.	Підпис	Дата	Залежність якості зв'язку від розмірів охопленої території Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук О.В.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						

Рисунок 1 – Розташування антени і прискорюючої лінзи

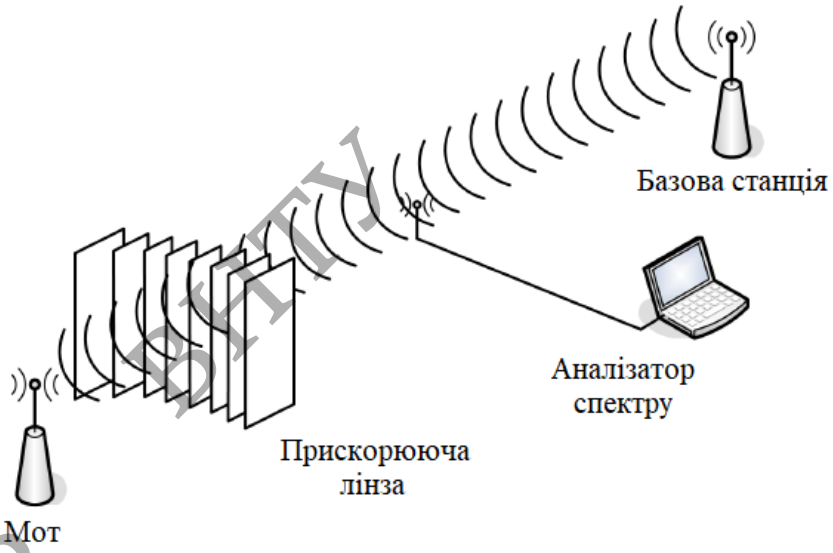


Рисунок 2 – Дослідження прискорюючої лінзи

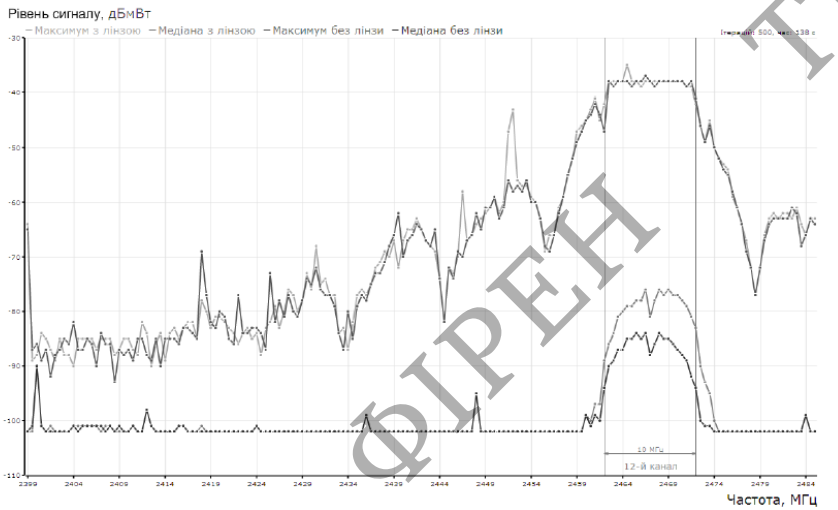


Рисунок 3 – Спектр сигналів з прискорюючою лінзою та без прискорюючої лінзи

					08-34.МКР.004.00.010 Е8		
Змн.	Лист.	№ докум.	Підпис	Дата	Використання прискорюючої лінзи Плакат	Літ.	Маса	Масштаб
Розроб.		Замрій О.В.						
Перевір.		Семенова О.О.				Арк. 1	Аркушів 1	
Т.Контр.								
Реценз.		Осадчук В.С.						
Н.Контр.		Семенова О.О.				ВНТУ, ТКС-20м		
Затверд.		Кичак В.М.						