Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Захист інформації в бездротових мережах»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Гонтковська Єлизавета Андріївна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Даков С.Ю.	

Нормоконтроль	Зюбіна Р.В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Гонтковській Єлизаветі Андріївні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Захист інформації в бездротових мережах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Бездротові мережі, технології захисту інформації в бездротових мережах

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно проаналізувати особливості бездротового середовища, виявити проблематику захисту інформації та вразливості бездротового середовища, дослідити існуючі методи захисту інформації при роботі в бездротовому середовищі, розробити програмне забезпечення, що дозволить робити моніторинг мережі та виявляти підозрілий трафік.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблене програмне забезпечення може бути використано як додатковий метод захисту інформації у мережі. Може бути вдосконалено для покращення роботи.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав	_____	С.Ю. Даков
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання	_____	Є.А. Гонтковська
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 28.01.2020	*виконано*
2	Аналіз літератури	29.01.2020 – 11.02.2020	*виконано*
3	Обґрунтування вибору рішення	12.02.2020 – 15.02.2020	*виконано*
4	Аналіз особливостей бездротового середовища	16.02.2020 – 04.03.2020	*виконано*
5	Виявлення проблематики захисту інформації в бездротовому середовищі, дослідження вразливостей та загроз	05.03.2020 – 22.03.2020	*виконано*
6	Дослідження існуючих методів захисту	23.03.2020 – 08.04.2020	*виконано*
7	Розробка програмного забезпечення на базі отриманої інформації	09.04.2020 – 10.05.2020	*виконано*
8	Оформлення пояснювальної записки	11.05.2020 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2021– 21.06.2021	*виконано*

Завдання видав	_____	С.Ю. Даков
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	Є.А. Гонтковська
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 60 сторінок основного тексту, 3 таблиці та 2 схеми. Список використаних джерел містить 17 найменувань і займає 2 сторінки.

Об'єктом дослідження є бездротові мережі та пристрої, що в них знаходяться.

Методами дослідження є системний підхід, методи порівняння, структурний аналіз.

Метою даної роботи є оцінка поточного стану захищеності бездротових мереж, аналіз методів захисту бездротових мереж, порівняння технологій захисту бездротових мереж та розробка програмного забезпечення, що дозволить моніторити бездротову мережу та виявляти підозрілий трафік.

У роботі проаналізована існуюча література з теорії використання і налаштування бездротових технологій, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми захисту бездротових технологій, розроблено рекомендації з вибору технологій захисту.

Розроблений лістинг програми, використовує аналіз бездротової мережі та може використовуватися користувачами для оцінки захищенності мережі та виявлення підозрілого трафіку.

Розроблені рекомендації призначені для користувачів, що хочуть забезпечити безпеку своїх даних для персонального або корпоративного використання .

Ключові слова: бездротова мережа, технологія, точка доступу, середовище передачі даних, безпека даних в бездротовому середовищі.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
AP	–	Application Programming
API	–	Application Programming Interface
(D)DOS	–	(Distributed) Denial-of-Service
DFS	–	Dynamic Frequency Selection
IEEE	–	Institute of Electrical and Electronics Engineers
IT	–	Information Technology
MAC	–	Media Access Control
MITM	–	Man In The Middle
OFDM	–	Orthogonal Frequency Division Multiplexing
SSID	–	Service Set Identifier
SSL	–	Secure Sockets Layer
TLS	–	Transport Layer Security
WEP	–	Wired Equivalent Privacy
WiMAX	–	Worldwide Interoperability for Microwave Access
WLAN	–	Wireless Local Area Network
WPA(1,2,3)	–	Wi-Fi Protected Access
VPN	–	Virtual Private Network
ІКТ	–	Інформаційно-комунікаційні технології
ЛОМ	–	Локальна обчислювальна мережа
ПЗ	–	Програмне забезпечення
3GPP	–	Консорціум розгортання специфікацій для мобільної телефонії

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається не захищенністю бездротових мереж. Враховуючи поширеність і популярність бездротових мереж як серед звичайних користувачів так і потенційних зловмисників безумовно зростають потреби у захисті бездротових технологій.

Доступність, простота розгортання, доволі легке налаштування і можливість підключити велику кількість пристроїв пояснюють популярність бездротових мереж, але не зважаючи на велику кількість переваг бездротових мереж можна стверджувати, що якщо мережа не захищена, то переваги не матимуть сенсу. Саме тому важливим є розуміння роботи мережі та розуміння необхідності захисту бездротових мереж за допомогою сучасних методів і технологій.

Не зважаючи на те що сьогодні в захисті бездротових мереж і застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних, контролю цілісності їх передачі, і досі можна сказати, що навіть не використовуючи складного обладнання і спеціальних програм можна підключитись до деяких корпоративних мереж просто знаходячись у межах дії мережі.

З вищесказаного випливає висновок про необхідність розробки нових способів захисту інформації при передачі в розподілених бездротових мережах в умовах впливу навмисних атак. У зв’язку з цим тема роботи є актуальною і практично важливою.

Аналіз останніх досліджень та літератури. Вчені та науковці, які зробили вклад у вивчення бездротових мереж і технологій їх захисту: Росс Джон, Вишневский В.М., Владимиров А.А. Гавриленко К.В., Михайловський А.А., Бирюков А.А. та інші.

Метою роботи є розробка програмного забезпечення що дозволить моніторити бездротову мережу та виявляти підозрілий трафік.

Завдання, які необхідно вирішити для досягнення поставленої мети:

- проаналізувати особливості бездротового середовища;
- виявити проблематику захисту інформації та вразливості бездротового середовища;
- дослідити існуючі методи захисту інформації при роботі в бездротовому середовищі;
- розробити програмне забезпечення, що дозволить робити моніторинг бездротової мережі та виявляти підозрілий трафік.

Об'єктом дослідження є процес захисту передачі даних в бездротових мережах

Предметом дослідження є методи захисту інформації в бездротовому середовищі

Методи дослідження дипломної роботи:

- аналіз технічної літератури;
- аналіз існуючих стандартів бездротових мереж;
- порівняння технологій захисту бездротових мереж;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1 АНАЛІЗ БЕЗДРОТОВИХ МЕРЕЖ ТА ЇХ ВРАЗЛИВОСТЕЙ

У сучасному світі великого поширення набули безпровідні мережі. Вони набули такого поширення, що охоплюють майже всю поверхню землі. Локальні мережі, персональні мережі, глобальні мережі – всі вони являються частиною нашого життя. Тому питання розуміння безпеки у бездротових мережах є дуже важливим для їх користувачів.

Для того щоб поглибитись у питання аналізу і безпеки бездротових мереж спочатку треба розуміти що собою представляє бездротова мережа і як вона працює.

Бездротову мережу можна схарактеризувати як комп'ютерну мережу, яка використовує для підключення до мережевих вузлів і передачі даних бездротове з'єднання.

Бездротові мережі бувають різними. Їх можна поділити за технологіями, за дальністю дії (рис.1.1) та за середовищами в яких вони передаються.

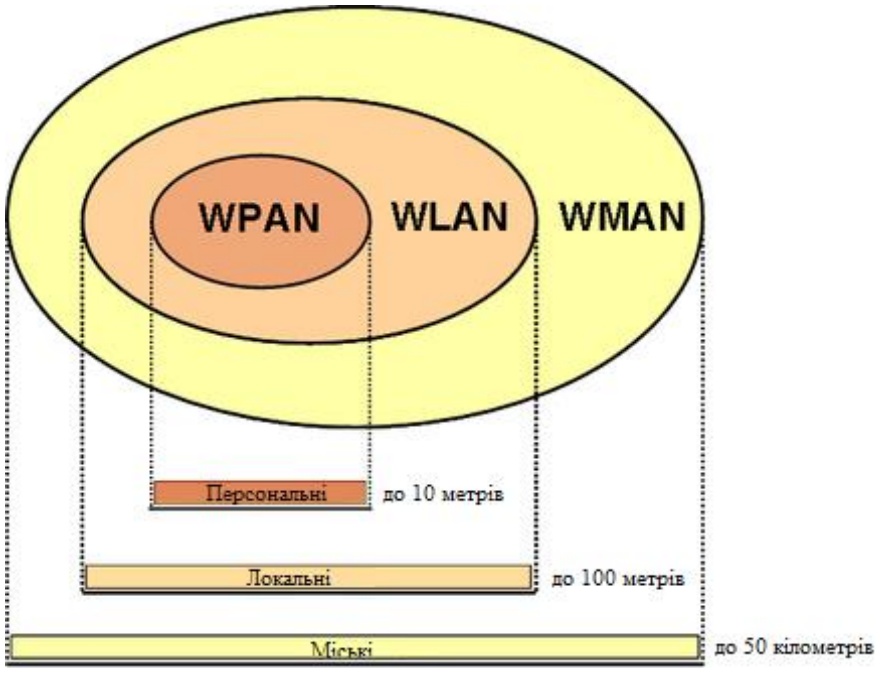

Рисунок 1.1 – Розділ безпровідних мереж за областю дії.

До передавальних середовищ та технологій бездротових мереж можна віднести: радіорелейні системи, системи лазерного зв’язку, інфрачервоні системи, системи з використанням низькоорбітальних супутників та на мережі на радіомодемах, та мережі на стільникових модемах [10].

За дальністю дії бездротові мережі можна віднести до таких категорій (Таблиця 1.2):

- Бездротові персональні мережі (WPAN — Wireless Personal Area Networks). Приклади технологій — Bluetooth.
- Бездротові локальні мережі (WLAN — Wireless Local Area Networks). Приклади технологій — Wi-Fi.
- Бездротові мережі масштабу міста (WMAN — бездротовий Metropolitan Area Networks). Приклади технологій — WiMAX.
- Бездротові глобальні мережі (WWAN — бездротова глобальна мережа). Приклади технологій — CSD, GPRS, EDGE, EV-DO, HSPA, LTE.

Залежно від використовуваної технології бездротові мережі можна розділити на три типи:

- локальні обчислювальні мережі;
- розширені локальні обчислювальні мережі;
- мобільні мережі (переносні комп’ютери).

Локальними обчислювальними мережами є системи, які можуть містити в собі інтеграцію різних комп’ютерів та пристроїв, розташованих не тільки в межах одного приміщення, а і віддалено. Вони призначені для об’єднання обчислювальної техніки в єдину мережу передачі даних. Локальні мережі можуть бути розширені за допомогою мережевих концентраторів або Ethernet-комутаторів.

Мобільною мережею можна назвати мережу стаціонарних радіостанцій, які обслуговують невелику площу і забезпечують радіозв’язок абонентом у зоні своєї дії.

Розширеними мережами можна назвати мережі в яких поєднані між собою локальні мережі або мобільні мережі з локальними.

Таблиця 1.2

Типи безпровідних мереж

Тип мережі	WLAN – Local area Network	WMAN – Metropolitan area network	WPAN – Personal area network	WWAN – Wide area network
Ціль	Забезпечує доступ до Інтернету в будівлі або на обмеженій території під відкритим небом	Надає доступ за межами офісних та домашніх мереж, як правило, регіональних	Передають сигнали між пристроями на обмежених ділянках, як правило, 100 метрів	Надає доступ за межами діапазону WLAN та WMAN
Підключення	Стільникове	IEEE 802.16 WiMax	Bluetooth, infrared	LTE

Бездротові мережі можуть бути різними, але всі мережі поєднує фізичний момент перенесення даних у вигляді сигналів від однієї точки до іншої по каналу передачі даних. Цей момент називається передачею даних або обміном даних.

В передачі даних бездротовою мережею беруть участь три основних елементи: радіосигнали, формат даних і структура мережі. З точки зору еталонної моделі OSI радіосигнали взаємодіють на фізичному рівні, а формат даних може бути розташованим на декількох верхніх рівнях моделі. У мережеву структуру входять адаптери інтерфейсів і базові станції, які передають і приймають радіосигнали [5].

У бездротовій мережі адаптери на кожному пристрої перетворюють цифрові дані в радіосигнали, які вони передають і на інші мережеві пристрої. Також перетворюють вхідні радіосигнали від зовнішніх мережевих елементів у цифрові

дані назад. IEEE розробив набір стандартів та специфікацій для бездротових мереж під назвою «IEEE 802.11», який визначає форму і зміст цих сигналів. Базовий стандарт 802.11 був прийнятий в 1997 році. Він орієнтувався на кілька бездротових середовищ: два види радіопередачі та мережі з використанням інфрачервоного випромінювання. На даний момент часу існує багато додаткових модифікацій стандарту адаптованих під сучасні швидкості і технології [2].

Що стосується формату даних, то сучасні комп'ютери можуть розпізнавати два інформаційних стани: стан сигналу присутнього на вході або відсутнього сигналу. Ці дві умови також позначаються як 1 і 0 та називаються бітами. Окремі біти не є особливо корисними, але, якщо поєднати вісім байтів у рядок, то можна отримати 256 комбінацій. Цього достатньо для присвоєння різних послідовностей всім літерам алфавіту, десяти цифр від 0 до 9, прогалин між словами та іншими символам, наприклад додавання знаків пунктуації та деяких букв, які використовуються в іноземних алфавітах. Сучасний комп'ютер розпізнає кілька 8-бітових байтів одночасно. По завершенні обробки комп'ютер використовує той же бітовий код. Результат може бути виведений на принтер, відеодисплей або канал передачі даних.

Аналогічно процесору комп'ютера канал даних може розпізнавати тільки один біт в момент часу. Або сигнал присутній в лінії, або його немає [8].

На коротких дистанціях можна відправляти дані по кабелю, який переносить вісім (або кратне восьми число) сигналів паралельно через окремі дроти. Очевидно, що паралельне підключення може бути у вісім разів швидше, ніж посилання одного біта по окремому проводу, але ці вісім проводів і за ціною виходять у вісім разів дорожче одного. Коли інформація відправляється на довгі дистанції, додаткова вартість може стати непомірно високою. А при використанні наявних ланцюгів, наприклад телефонних ліній, необхідно знайти спосіб посилання всіх восьми бітів через один і той же провід (або інший носій).

Рішенням є передача одного біта в момент часу з декількома додатковими бітами і паузами, що визначають початок кожного нового байта. Такий спосіб

називається послідовним каналом передачі даних, оскільки біти відправляються один за іншим. Не має значення, яка проміжна середа використовується для передачі бітів. Це можуть бути електричні імпульси в проводі, два різних аудіосигнали, послідовності миготливих індикаторів та інші приклади одночасної передачі бітів.

В ідеальному представленні ситуації сигнал що надходить на один кінець мережі, буде абсолютно ідентичним вихідному. Але в реальному світі практично завжди є завади і майже завжди знаходиться таких різновид шуму, який може впроваджуватися в чистий вихідний сигнал. Шум визначається як щось, що додається до вихідного сигналу; він може бути викликаний розрядом блискавки, перешкодою від іншого комунікаційного каналу або нещільного контакту десь в ланцюзі. Яким би не було джерело, шум у каналі може пошкодити потік даних. У сучасній комунікаційній системі біти протікають через ланцюг гранично швидко - мільйони за кожну секунду, тому вплив шуму навіть в частку секунди може знищити достатню кількість бітів, щоб перетворити дані в нісенітницю [2].

Це означає, що для будь-якого потоку даних необхідно включити перевірку помилок. Під час перевірки помилок в кожен байт додається такий собі різновид стандартної інформації, званої контрольної сумою. Якщо приймальний пристрій виявляє, що контрольна сума відрізняється від передбачуваної, вона запитує передавач про повторне посилання цього ж байта.

1.1 Сучасні бездротові мережі

Поняття сучасних бездротових мереж досить не чітке адже сучасний світ розвивається і технології стрімко змінюють одне одну. Тому для дослідження обрано найбільш популярні бездротові мережі у даний проміжок часу.

Випливаючи з поняття бездротових мереж можна сказати що бездротовою мережею є комп’ютерна мережа, яка використовує бездротові з’єднання даних між вузлами мережі. Бездротові мережі можуть передавати інформацію різними

швидкостями, використовувати не однакові технології передачі та мати різну територію покриття.

Є декілька поколінь бездротових мереж: 1G, 2G, 3G, 4G, 5G та інші проміжні варіанти. Певне покоління відповідає за проміжок швидкостей, якими користувач може передавати інформацію, також покоління можуть відрізнятися технологіями передачі даних, які використовуються під час передачі інформації.

До сучасних бездротових мереж, які найбільш поширені у даний проміжок часу можна віднести такі мережі: 4G, LTE та 5G.

1.1.1 4G

До четвертого покоління прийнято відносити перспективні технології, що дозволяють здійснювати передачу даних зі швидкістю, що перевищує 100 Мбіт / с.

Ще в 2008 році для 4G було встановлено такі вимоги до швидкості передачі даних:

- 100 Мбіт/с – для абонентів, які рухаються швидко (потяг чи автомобіль);
- 1 Гбіт/с – для абонентів, які пересуваються повільно (пішохід).

До технологій, які претендують на роль 4G можна віднести:

- LTE
- TD-LTE
- мобільний WiMAX
- UMB
- HSPA +

Зараз 4G складається з двох стандартів – WiMAX та LTE:

- WiMAX (англ. Worldwide Interoperability for Microwave Access) – це еволюціонуючий Wi-Fi з великою площею покриття.
- LTE (англ. Long Term Evolution) – довгостроковий розвиток або черговий виток в розвитку GSM.

Мережі четвертого покоління працюють з цифровими даними і не використовують канали для передачі голосу на відміну від 1G, 2G та 3G. Також системи зв'язку 4G засновані на пакетних протоколах передачі даних. Для пересилки даних у 4G використовується протокол IPv4.

Сьогодні 4G відомий насамперед своїми широкосмуговими можливостями та значно вищою швидкістю, ніж 3G, що забезпечує можливість швидкої передачі даних у просторі.

1.1.2 LTE

LTE (Long Term Evolution) є маркетинговою фразою, яка означає прогресивний рух технології у напрямку справжнього 4G. Тобто кожен раз, коли йдеться річ про 4G LTE – мається на увазі прогрес у розвитку від 3G до 4G.

LTE базується на стандартах, розроблених Проектом партнерства третього покоління - 3GPP, але на даний момент Міжнародний стандарт LTE є слабко визначеним і враховуючи те що він дуже часто оновлюється ускладнюється розуміння дійсного стандарту LTE.

LTE можна сформулювати як модернізований 3G трохи гірший за справжній 4G. Мережі 4G LTE надсилають дані на телефони 4G LTE зі швидкістю нижче 100 Мбіт / с із швидкістю завантаження.

Мережі LTE призначені для подолання розриву функціонального обміну даними між фіксованими бездротовими локальними мережами (LAN) та дуже високою мобільністю стільникових мереж.

Основними цілями LTE є:

- збільшена пікова швидкість передачі даних ніж у 3G по висхідній та висхідній лініях;
- масштабована пропускна здатність;
- покращена спектральна ефективність;

- стандартний інтерфейс, який може підтримувати безліч типів користувачів.

Оскільки для LTE не існує справжнього стандарту, він охоплює весь діапазон мінімальних швидкостей завантаження від 20 Мбіт / с для 3G до 100 Мбіт / с для 4G, надаючи йому величезний діапазон потенційних швидкостей.

Беручи до уваги те що досі LTE використовується дуже поширено і велика кількість операторів використовують його замість справжнього 4G. LTE досі являється лише перехідною ланкою між 3G та 4G

1.1.3 5G

5G - це відносно новий стандарт. В контексті мобільного зв'язку з 5G швидкість інтернету коливається від 10 до 25 Гбіт / с з мінімальними затримками в передачі сигналу (всього 1-2 мс). 5G, як видається, революціонізує та швидкість завантаження може повністю змінити спосіб збереження зв'язку між пристроями. Це відкриває величезне поле можливостей: нові послуги, сервіси та цілі бізнес-моделі, які були неможливі в мережах 4G. Для масового споживача вже зараз найбільш популярними технологіями, які можуть використовуввати 5G є віртуальна і доповнена реальність. Наприклад, в 2018 році під час футбольного матчу Росія - Туреччина на стадіоні було встановлено п'ять камер з охопленням 360 градусів, зображення з яких передавалося по мережі 5G в офіс «Мегафону». Трансляцію можна було дивитися в шоломі віртуальної реальності, повністю занурившись в те, що відбувалося на стадіоні.

Зараз 5G перебуває в процесі розробки, виробники телефонів випускають телефони, сумісні з 5G, але мережі операторів не наближаються до мінімальних 1 Гбіт / с із затримкою в 1 мілісекунду, необхідною для стандарту. Також оператори розраховують досягнути швидкості в 30-50 разів вищої, ніж у LTE.

Наприкінці жовтня 2015 року південнокорейська компанія SK Telecom заявила про свій намір стати першим провайдером 5G. SK Telecom вдалося передати дані із швидкістю 19,1 Гбіт/с, що в кілька разів швидше за існуючий 4G [14].

Технології для мереж 5 покоління 5G в квітні 2019 р були розгорнуті в Південній Кореї (перша країна, яка запустила комерційні послуги п’ятого покоління 5G), Швейцарії, Китаї. Основним розробником обладнання є китайська компанія Huawei. «Основним завданням для мереж п’ятого покоління стане розширення спектра використовуваних частот і збільшення ємності мереж. Очікується, що нова технологія вирішить завдання, над якою працюють всі оператори в світі, - підвищить ефективність мережевої інфраструктури », - заявили в Huawei [13].

Через обізнаність людей про 5G, компанії вже намагаються продати свої існуючі мережі вгору, при цьому AT&T називає свою мережу 4G "5Ge", незважаючи на те, що вона не наближається до стандартів 5G. T-Mobile заявляє, що пропонує найбільшу мережу 5G в Америці, а Verizon заявляє про найшвидшу швидкість 5G на всіх смугах пропускання. Усі вони не є "справжніми 5G", принаймні, як визначено MCE-R (сектором радіозв’язку Міжнародного союзу радіозв’язку). Проте вони, звичайно, швидші, ніж 4G або 4G LTE.

Також після розгортання мереж стільникового зв’язку 5 покоління 5G у вчених та інженерів посилився інтерес до розробки обладнання наступного покоління стільникового зв’язку. Фахівці сходяться на думці, що в наступному поколінні вони отримають подальший розвиток і вдосконалення недостатньо повно реалізованих підходів в попередньому поколінні. Наступні покоління скоріше всього можуть бути засновані на застосуванні штучного інтелекту, квантових комунікацій, що дозволить досягти швидкості передачі даних від сотень Гбіт / с до 1 Тбіт / с.

1.2 Необхідність захисту бездротових мереж

Бездротові мережі не являються безпечними. Більшу частину часу вони дійсно являються доволі незагрозливими для її користувачів, але вони все ж мають велику кількість вразливостей.

Беручи до уваги те, що бездротова мережа використовує радіосигнали з певним набором характеристик, і при зацікавленості третьої особи, яка може при

бажанні виділити велику кількість часу на вивчення мережі, є можливим варіант перехоплення даних у мережі. Навіть якщо конфіденційна інформація пересилається бездротовим з'єднанням, то зловмисник все одно може скопіювати її. Паролі облікових записів, персональні дані, номери кредитних карток являються частиною вразливої інформації.

Шифрування та інші методи захисту можуть трохи ускладнити процес перехвату даних, але вони все одно не в змозі забезпечити повний захист від зловмисника, який володіє досвідом роботи з бездротовими мережами і перехопленням інформації.

Ситуація стає більш небезпечною завдяки недбалому відношенню до безпеки адміністраторів і користувачів мережі, які часто залишають мережі відкритими або не використовують технологій захисту бездротових мереж або найпростішого шифрування, яке б мінімізувало вразливості мереж.

Головна відмінність між дротяними і бездротовими мережами - наявність неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє порушнику, що знаходяться в безпосередній близькості від бездротових структур, виробляти ряд нападів, які неможливі в дротовому світі.

При використанні бездротового доступу до локальної мережі загрози безпеки істотно зростають [8].

При побудові бездротових мереж також дуже явно стоїть проблема забезпечення їх безпеки.

Устаткування мереж WLAN (Wireless Local Area Network) включає точки бездротового доступу і робочі станції для кожного абонента.

Точки доступу AP (Access Point) виконують роль концентраторів, які забезпечують зв'язок між абонентами і між собою, а також функцію мостів, які здійснюють зв'язок з кабельної локальної мережею і з Інтернет. Кожна точка доступу може обслуговувати кілька абонентів. Кілька прилеглих точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, забезпечені бездротовими адаптерами, отримують доступ до мережі. Такі зони доступу

створюються в місцях масового скупчення людей: в аеропортах, студентських містечках, бібліотеках, магазинах і бізнес-центрах.

У точки доступу є ідентифікатор набору сервісів SSID (Service Set Identifier). SSID - це 32-бітний рядок, що використовується в якості імені бездротової мережі, з якої асоціюються всі вузли. Ідентифікатор SSID необхідний для підключення робочої станції до мережі. Щоб зв'язати робочу станцію з точкою доступу, обидві системи повинні мати один і той же SSID. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися з точкою доступу і з'єднатися з мережею.

Доступ до мережі і підключення також можуть бути вразливою ланкою тому треба також приділяти увагу підключеним робочим станціям до мережі.

Важливо розуміти, що є декілька основних загроз безпеці бездротової мережі. Першою з них є небезпека підключення до мережі сторонньої особи без відома або дозволу адміністратору мережі; другою є можливість перехоплення даних досвідченим спеціалістом при передачі інформації. Кожна з цих вразливостей є окремою потенційною проблемою і кожна з них потребує окремого спеціального методу профілактики і захисту. Не дивлячись на правоту ствердження про те що забезпечення повної безпеки бездротової мережі не являється можливим, проте мінімізація ризиків може значно ускладнити життя випадковим злочинцям і зменшити можливості перехоплення інформації досвідченими спеціалістами тим самим покращити життя адміністраторам і користувачам мережі.

1.3 Інформаційні загрози та атаки

Як і в домашній, так і в інших бездротових мережах завжди є ризики реалізування загроз зі сторони порушників.

Типовий діапазон трансляції в приміщенні точки доступу становить 150–300 футів. На відкритому повітрі цей діапазон може сягати до 1000 футів. Отже, якщо зона дії мережі знаходиться у тісному населеному пункті, то відсутність захисту бездротової мережі може відкрити мережеве з'єднання з Інтернетом для багатьох ненавмисних користувачів. Такі користувачі можуть мати можливість здійснювати

незаконні дії, відстежувати та фіксувати веб-трафік мережі або красти особисті файли.

Широкий діапазон бездротової точки доступу може відкрити доступ до Інтернету за межами будинку, у якому знаходиться мережа. Розумні користувачі комп'ютерів це знають, і деякі з них проїжджаючи міста і квартали за допомогою бездротового обладнаного комп'ютера - іноді з потужною антеною - у пошуку незахищених бездротових мереж. Подібна практика відома під назвою "охорона праці" [7].

Також багато громадських точок доступу не захищені, а трафік, який вони несуть, не зашифрований. Це може загрожувати конфіденційним комунікаціям або операціям користувачів. Оскільки зв'язок передається „в чистому вигляді", зловмисні актори можуть використовувати інструменти сніфингу, щоб отримати конфіденційну інформацію, таку як паролі або номери кредитних карток.

Незахищена громадська бездротова мережа в поєднанні з незахищеним спільним використанням файлів може дозволити зловмисному користувачеві отримати доступ до будь-яких каталогів та файлів, які ви ненавмисно надали для спільного використання. Тож підключаючи пристрої до загальнодоступних мереж, краще заборонятиспільний доступ до файлів та папок. Дозволяти використовувати спільний доступ доцільно лише у визнаних домашніх мережах і лише тоді, коли необхідно ділитися елементами.

У громадських місцях зловмисні користувачі можуть просто поглянути через плече людини під час друкування. Просто спостерігаючи, вони можуть викрасти конфіденційну або особисту інформацію. Захисні екрани, які заважають серфінгістам бачити екран вашого пристрою, можна придбати за невеликі гроші.

Не всі зловмисники покладаються на отримання доступу до даних за допомогою бездротового зв'язку. Викравши ваш пристрій фізично, зловмисники могли мати необмежений доступ до всіх його даних, а також до будь-яких підключених хмарних облікових записів. Вжити заходів для захисту пристроїв від втрати або крадіжки є важливим, але якщо трапиться найгірше, невелика підготовка

може захистити дані всередині. Більшість мобільних пристроїв, включаючи портативні комп'ютери, тепер мають можливість повністю зашифрувати свої збережені дані, роблячи пристрої марними для зловмисників, які не можуть надати належний пароль або персональний ідентифікаційний номер (PIN-код). На додаток до шифрування вмісту пристрою, доцільно також налаштувати програми вашого пристрою на запит інформації для входу, перш ніж дозволити доступ до будь-якої хмарної інформації. Нарешті, індивідуально зашифрованні або захищені паролем набагато складніше викрасти. Це забезпечить ще один рівень захисту у випадку, якщо зловмисник зможе отримати доступ до пристрою.

До основних вразливостей і загроз бездротових мереж можна віднести:

- сигнали радіомаяку;
- виявлення WLAN;
- підслуховування;
- помилкові точки доступу в мережу;
- відмова в обслуговуванні;
- атаки типу «людина-в-середині»;
- анонімний доступ в Інтернет.

Сигнали радіомаяку. Точка доступу включає з певною частотою широкомовний радіомаяк, щоб оповіщати навколишні бездротові вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку бездротового доступу, включаючи, як правило, SSID, і вони запрошують бездротові вузли зареєструватися в даній області. Будь-яка робоча станція, що знаходиться в режимі очікування, може отримати SSID і додати себе в відповідну мережу. Мовлення радіомаяка є «вродженою патологією» бездротових мереж. Багато моделей дозволяють відключати видимість SSID, щоб кілька утруднити бездротове підслуховування, але SSID, тим не менш, надсилається при підключенні, тому все одно існує невелике вікно уразливості [4].

Виявлення WLAN. Для виявлення бездротових мереж WLAN використовується, наприклад, утиліта NetStumber спільно з супутниковим

навігатором глобальної системи позиціонування GPS. Дана утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері уможливлює виявлення мереж WLAN під час обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером в руках.

Підслуховування. Підслуховування ведуть для збору інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Обладнання, що використовується для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі. Бездротові мережі за своєю природою дозволяють з'єднувати з фізичної мережею комп'ютери, що знаходяться на деякій відстані від неї, як якщо б ці комп'ютери знаходилися безпосередньо в мережі. Наприклад, підключитися до бездротової мережі, що розташовується в будівлі, може людина, що сидить в машині на стоянці поруч. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Помилкові точки доступу в мережу. Досвідчений атакуючий може організувати неправдиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад аутентифікаційну інформацію. Цей тип атак іноді застосовують в поєднанні з прямим «глушінням» істинної точки доступу в мережу.

Під час виконання атак зловмисник збирає інформацію про точку доступу загальнодоступної мережі, а потім налаштовує свою систему, щоб видавати себе за неї. Противник використовує широкомовний сигнал, сильніший за той, що генерується законною точкою доступу; тоді нічого не підозрюючі користувачі підключаються, використовуючи сильніший сигнал. Оскільки жертва підключається до Інтернету через систему зловмисника, зловмиснику легко використовувати спеціалізовані інструменти для зчитування будь-яких даних, які жертва надсилає

через Інтернет. Ці дані можуть включати номери кредитних карток, комбінації імені користувача та пароля та іншу особисту інформацію. Завжди підтверджуйте ім’я та пароль загальнодоступної точки доступу Wi-Fi перед використанням. Це забезпечить підключення до надійної точки доступу.

Відмова в обслуговуванні. Повну паралізації мережі може викликати атака типу DoS (Denial of Service) - відмова в обслуговуванні. Її мета полягає в створенні перешкоди при доступі користувача до мережевих ресурсів. Бездротові системи особливо сприйнятливі до таких атак. Фізичний рівень в бездротової мережі - абстрактний простір навколо точки доступу. Зловмисник може включити пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком - така задача зазвичай не викликає особливих труднощів. Сам факт проведення DoS-атаки на фізичному рівні в бездротової мережі важко довести.

Атаки типу «людина-в-середині». Атаки цього типу виконуються на бездротових мережах набагато простіше, ніж на провідних, так як в разі провідної мережі потрібно реалізувати певний вид доступу до неї. Зазвичай атаки «людина-в-середині» використовуються для руйнування конфіденційності і цілісності сеансу зв’язку. Атаки MITM складніші, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Він використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад для спуфінгу IP-адрес, зміни MAC-адрес і для імітування іншого хоста [1].

Анонімний доступ в Інтернет. Незахищені бездротові локальні обчислювальні мережі забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використовувати незахищену мережу WLAN організації для виходу через неї в Інтернет, де вони будуть здійснювати протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною локальною обчислювальною мережею формально стає джерелом атакуючого трафіку, націленого на іншу

комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяну шкоду жертві атаки хакерів.

Описані вище атаки не є єдиними атаками, використовуваними хакерами для злому бездротових мереж, але є одними з найпоширеніших атак та вразливостей бездротових мереж.

Висновок за розділом 1

Аналізуючи те, що при передачі інформації бездротовою мережею відправлення і приймання даних здійснюється радіохвилями та приймати їх може хто завгодно при наявній техніці випливає питання необхідності додаткових механізмів захисту.

В передачі даних бездротовою мережею беруть участь три основних елементи: радіосигнали, формат даних і структура мережі. З точки зору еталонної моделі OSI радіосигнали взаємодіють на фізичному рівні, а формат даних може бути розташованим на декількох верхніх рівнях моделі. У мережеву структуру входять адаптери інтерфейсів і базові станції, які передають і приймають радіосигнали.

Бездротові мережі мають безліч слабких моментів, які можуть стати дуже небезпечними через незахищеність мереж у підключенні, через великий спектр даних які може надати сама мережа для організації подібної і у наслідок її підміни і через не пильне відношення до захисту адміністраторів мережі наприклад у відсутності використання протоколів захисту або шифруванні, або використанні застарілих методів захисту. Також слабкою ланкою бездротових мереж можуть бути самі користувачі які можуть розповсюджувати паролі до мереж або відкривати інформацію про дані, що пережаються у мережі стороннім особам.

До основних вразливостей і загроз бездротових мереж можна віднести:

- сигнали радіомаяку;
- виявлення WLAN;
- підслуховування;
- помилкові точки доступу в мережу;

- відмова в обслуговуванні;
- атаки типу «людина-в-середині»;
- анонімний доступ в Інтернет.

Одними з самих неприємних по наслідкам і по можливостям роботи з мережею є атаки відмови в обслуговуванні та атаки типу людина в середині. У першому випадку створюються перешкоди при доступі користувача. До мережевих ресурсів. Зловмисник може включити пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком, який звичайно буде заважати вільно користуватися мережею.

У випадку атаки «Людина посередині» реалізація відбувається у наслідок ретельного обстеження мережі. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Він використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад для спуфінгу IP-адрес, зміни MAC-адрес і для імітування іншого хоста. Зазвичай ця атака використовується для руйнування конфіденційності і цілісності сеансу зв’язку.

Описані вище атаки не є єдиними атаками, використовуваними хакерами для злому бездротових мереж, але є одними з найпоширеніших атак та вразливостей бездротових мереж.

Отже можна зробити висновок що захист бездротових мереж є доволі недосконалим і важливим є розробка нових методик захисту та вдосконалення існуючих технологій. Також обізнане використання методів і технологій захисту може мінімізувати вплив на слабкі місця бездротових мереж.

РОЗДІЛ 2 МЕТОДИКИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ У БЕЗДРОТОВИХ МЕРЕЖАХ

На даний момент існує доволі багато методів і технологій захисту бездротових мереж, таких як обмеження доступу до мережі, фільтрація адрес або захист мережі за допомогою шифрування. Але для проведення досліджень методів захисті необхідно розуміти стандарти які описують процес передачі даних відповідними протоколами та згідно яким вдосконалюються технології захисту бездротових мереж.

Базовим стандартом, який визначає набір протоколів для передачі даних в бездротових мережах є IEEE 802.11. Цей стандарт постійно доповнюється та оновлюється, таким чином його нові версії були опубліковані в 1999, 2007, 2012 роках, а також в 2016 році [2].

2.1 Стандарти інформаційної безпеки для бездротових мереж

Бездротова мережа - це гнучка інфраструктура, що представляє собою комплекс апаратно - програмних засобів для передачі інформації. Бездротові мережі можуть і виступати як альтернатива провідним мережам, і успішно доповнювати їх, надаючи додаткові функції. Бездротові мережі підпорядк

Сучасні бездротові мережі дозволяють вирішувати безліч завдань: від організації мережі всередині приміщення до розподілених мереж масштабу міста, регіону і навіть цілої держави. Низька вартість, швидкість розгортання, широкі функціональні можливості з передачі трафіку даних, IP телефонії, мультимедійного трафіку - все це робить бездротову технологію одним з найбільш швидкозростаючих телекомунікаційних напрямків. Бездротові мережі, також як і провідні, прийнято класифікувати за територіальною ознакою. Зазвичай виділяють чотири типи: WWAN, WMAN, WLAN, і WPAN. Для різних зон охоплення створено специфічні нормативні документи, які визначають правила, настанови або характеристики

використання бездротового середовища на тих чи інших швидкостях. Такі документи називаються стандартами бездротових мереж. На рис.2.1 показана классіфікація безпровідних стандартів за територіальною ознакою.

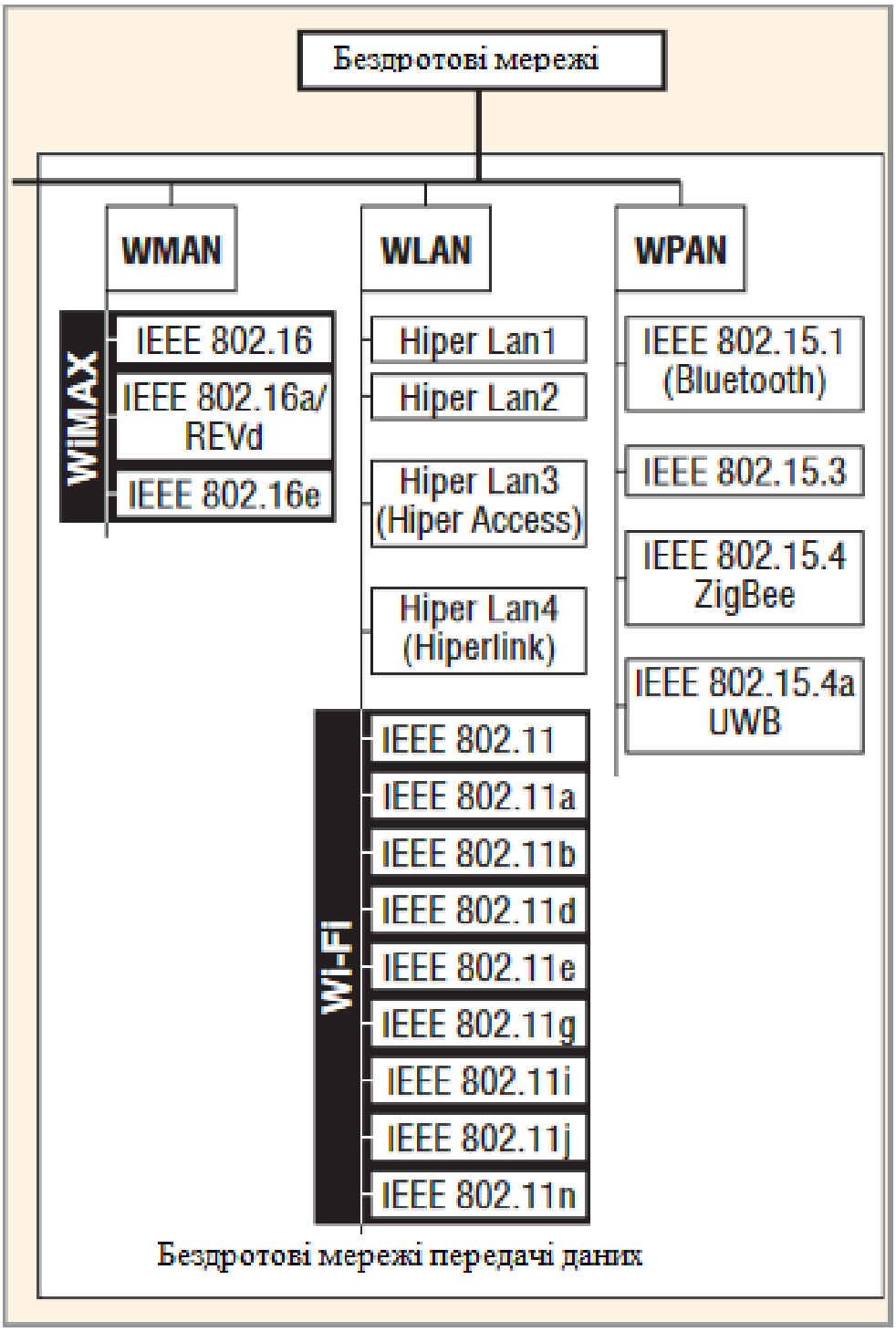

Рисунок 2.1 – Стандарти передачі даних у бездротових мережах WMAN, WLAN, WPAN.

2.1.1 Стандарти для мережі WPAN

IEEE 802.15.1 (Bluetooth)

Технологія Bluetooth була розроблена компанією Ericsson. Свою назву технологія отримала в честь датського короля Гарольда Синій Зуб, який правив Данією і Норвегією в X столітті. Згодом для просування на ринок був утворений консорціум у складі Ericsson, IBM, Intel, Nokia і Toshiba. Сьогодні до складу основних членів входять 3Com, Agere Systems, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, Toshiba. Мета творців Bluetooth - забезпечити найрізноманітнішим електронним приладам (комп'ютерів, стільникових телефонів, побутової техніки) можливість зв'язуватися один з одним без проводів на відстані до 100 м і обмінюватися даними.

Стандарт Bluetooth використовує радіочастоти 2400 - 2483,5 МГц. Цей діапазон, іменований ISM (Industrial, Scientific, Medicine - промисловий, науковий і медичний), використовується в багатьох країнах для безліцензійного доступу. У технології Bluetooth весь діапазон розбитий на 78 каналів шириною 1 МГц кожен. У верхній і нижній частинах діапазону передбачені захисні невикористовувані смуги шириною 3,5 і 2 МГц відповідно. У деяких країнах, наприклад у Франції, діапазон ISM значно вужче [16].

За вихідними потужностями всі пристрої діляться на три класи:

- перший клас - до 100 мВт,
- другий - до 2,5 мВт і
- третій - до 1 мВт.

Для передачі даних використовується гауссова частотна модуляція, яка передбачає зміну частоти несучої в часі відповідно до кривої Гаусса (рис.2.2), що дозволяє обмежити спектр випромінюваного сигналу. Обмін даними здійснюється всередині тимчасових інтервалів (слотів) довжиною 625 мкс. Після передачі кожного слота виробляється перехід на інший частотний канал. Частина слотів можна зарезервувати для синхронних каналів (передача голосу), а всього

передбачено до трьох синхронних каналів зі швидкістю 64 Кбіт / с. Паралельно з синхронними даними можуть передаватися і асинхронні.

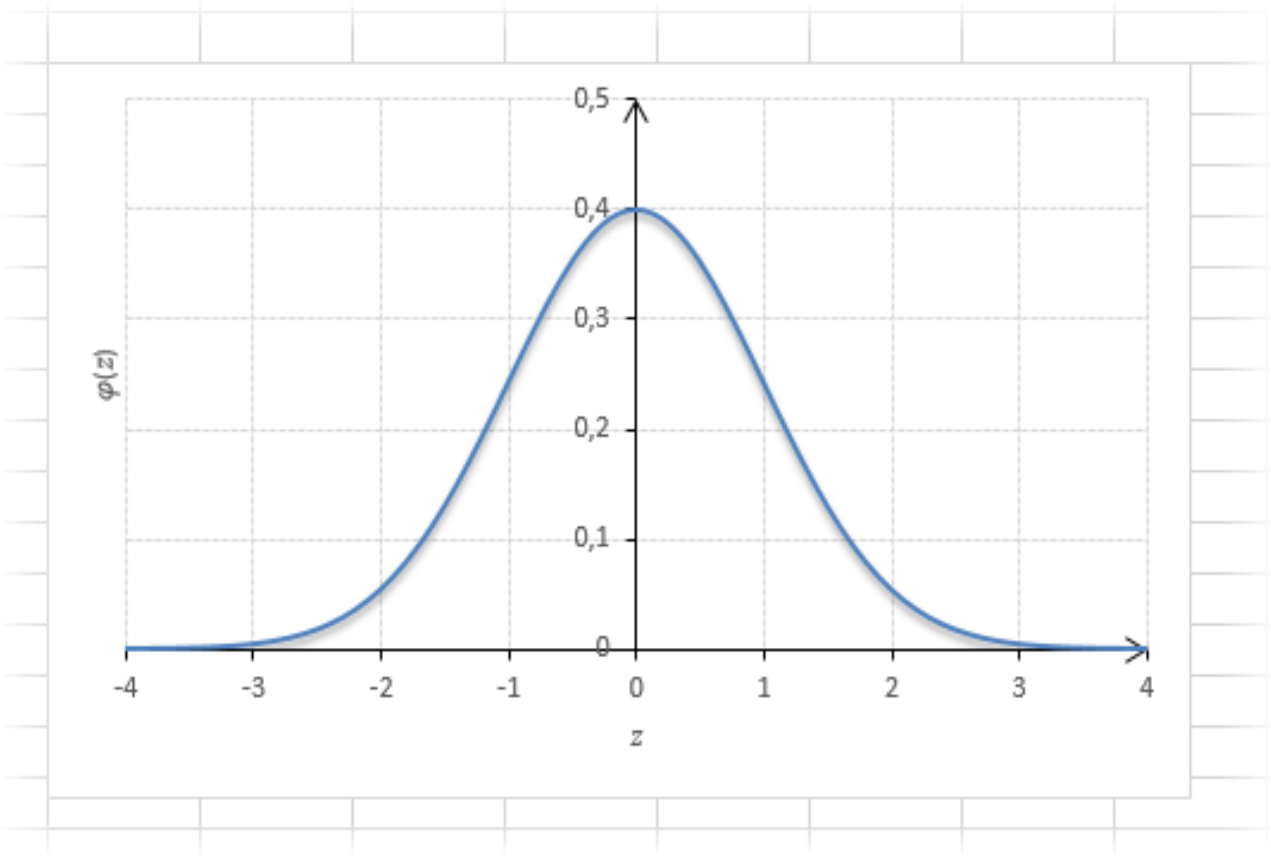

Рисунок 2.2 – Крива Гаусса

Для організації дуплексного зв'язку використовується метод тимчасового мультиплексування, тобто в одному часовому слоті передає один пристрій, а в наступному - інший. При симетричній організації обміну асинхронними даними максимальна швидкість становить 433,9 Кбіт / с в кожну сторону. Максимальна швидкість обміну досягається при асиметричному обміні і становить 723,2 Кбіт / с в одну сторону і 57,6 Кбіт / с - в іншу.

Bluetooth служить головним чином для організації каналів зв'язку типу «точка - точка», однак можлива так само і організація типу «точка - багато - точка». Організацію топологій мереж Bluetooth зображено на Рисунку 2.3.

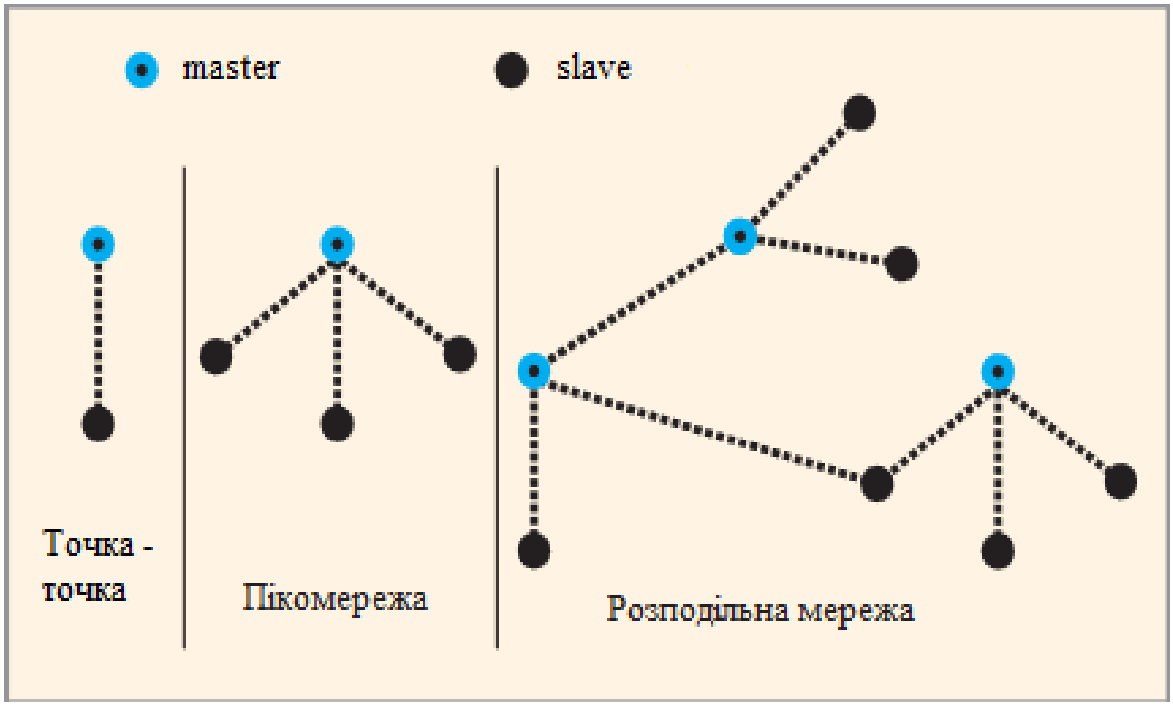

Рисунок 2.3 – Організації топології мереж Bluetooth

У будь-якому випадку один з пристроїв є провідним (master), а всі інші - відомими (slave). Утворена таким чином структура називається пікомережа (piconet). В одній такій мережі можуть брати участь один провідний пристрій і до семи відомих пристроїв. Додатково в пікомережі можуть бути присутні й інші пристрої, які називаються блокованими (parked) і не беруть участь в обміні даними, але знаходяться в синхронізації з провідним пристроєм.

IEEE 802.15.3

Стандарт IEEE 802.15.3 є прямим спадкоємцем Bluetooth.

IEEE 802.15.3 забезпечує швидкість передачі даних до 55 Мбіт / с на відстані до 100 м та дозволяє одночасно працювати в такій мережі до 245 користувачів. При виникненні перешкод з боку інших побутових пристроїв чи інших мереж, мережі на основі IEEE 802.15.3 можуть автоматично перемикати канали. Також підтримуються швидкості передачі даних - 11, 22, 33 і 44 Мбіт / с. Шифрування даних в мережах IEEE 802.15.3 може здійснюватися за стандартом AES 128.

IEEE 802.15.4 (ZigBee)

Стандарт IEEE 802.15.4 (ZigBee) орієнтований головним чином на використання в якості засобу зв’язку між автономними приладами та обладнанням. У корпоративному секторі це можуть бути, наприклад, складські системи, системи автоматизації виробництва, різні датчики, сенсори, сервоприводи, електронні мітки, а в домашніх умовах - ПК, ігрові приставки, системи безпеки, освітлення, кондиціонування, радіофіковані іграшки і навіть пульти дистанційного керування.

Стандарт IEEE 802.15.4 визначає параметри фізичного рівня (PHY) і протокол управління доступом (MAC), пропонуючи підтримку різних топологій мереж. Ключові функції PHY включають в себе контроль за енергією і якістю ланок, а також оцінку каналів для більш успішного співіснування з мережами інших бездротових операторів. MAC визначає автоматичне підтвердження отримання пакетів, забезпечує можливість передачі даних в певні часові інтервали і підтримує 128 бітні функції безпеки AES. Якщо в межах досяжності ZigBee пристроїв виявиться обладнання WiFi або Bluetooth, їх канали можуть бути використані як тунель для трафіку ZigBee.

Стандарт IEEE 802.15.4 передбачає невелику дальність дії (близько 10 метрів) і пропускну можливість каналу (до 250 Кбіт / с). Передача на цій швидкості ведеться вдіапазоні 2,4 ГГц. Невелика потужність і швидкість обумовлені малою споживаною потужністю пов’язаних пристроїв. Доступні також діапазони 858 МГц (20 Кбіт / с) і902. . .928 МГц (40 Кбіт / с) [12].

IEEE 802.15.4a (UWB)

UWB (Ultra Wideband) - технологія надширокосмугового радіозв’язку, розроблена корпорацією Intel для швидкостей передачі даних до 500 Мбіт / с на відстань кількох метрів. Для передачі даних використовуються дуже короткі радіоімпульси (менше 1 нс) в широкому діапазоні частот 3,1. . .10,6 ГГц. За допомогою UWB технології можна створювати спеціальні мережі, в яких кілька понад широкосмугових пристроїв зможуть підтримувати зв’язок між будь-якими вузлами.

Короткі сигнали UWB порівняно стійкі до багатопроменевого загасання, що виникає при відображенні хвилі від стін, стелі, будівель, транспортних засобів. Високошвидкісні UWB пристрої добре підходять для роботи з відеопотоками і додатками, що вимагають швидкого пересилання даних. Низькошвидкісне UWB обладнання може застосовуватися для відстежування місцеположення на місцевості власників бездротових пристроїв і різних об'єктів. Для мобільних пристроїв важливим є той факт, що в широкому спектрі потрібно набагато менше витрат енергії, ніж для передачі у вузькосмуговому сигналі, в силу різного рівня сигналу: в широкому спектрі можна використовувати шумоподібні сигнали з малим відношенням сигнал / шум. Тому (як очікується) чіпи UWB будуть економічніше, ніж, наприклад, чіпи Bluetooth, володіючи при цьому набагато більшою пропускною спроможністю.

2.1.2 Стандарти для мережі WLAN

Технологія Wi-Fi (Wireless Fidelity) призначена для побудови бездротових локальних мереж, організації точок публічного доступу до Інтернету (Hot-Spots). Технологія базується на стандартах IEEE 802.11. Це сімейство є базовим стандартом WLAN, що підтримує передачу даних зі швидкостями від 1 до 2 Мбіт / с і працює на фізичному і канальному рівні моделі OSI. На фізичному рівні визначені два широкосмугових радіочастотних методи передачі і один - в інфрачервоному діапазоні. Радіочастотні методи працюють в ISM діапазоні 2,4 ГГц і зазвичай використовують смугу 83 МГц в діапазоні 2,400. . .2,483 ГГц.

Стандарт 802.11 використовує технологію розширення спектру сигналу прямої послідовністю (Direct Sequence SpreadSpectrum, DSSS) і технологію розширення спектру сигналу стрибкоподібною перебудовою частоти (Frequency Hopping Spread Spectrum, FHSS). Для модуляції сигналу FHSS використовує технологію Frequency Shift Keying (FSK). Приклад технології зображено на рисунку 2.4.

При роботі на швидкості 1 Мбіт / с використовується FSK модуляція по Гауса другого рівня, а при роботі на швидкості 2 Мбіт / с - четвертого рівня. Метод DSSS використовує технологію модуляції Phase Shift Keying (PSK). При цьому на швидкості 1 Мбіт / с використовується диференціальна двоичная PSK, а на швидкості 2 Мбіт / с - диференціальна квадратична PSK модуляція. Заголовки фізичного рівня завжди передаються на швидкості 1 Мбіт / с, в той час як дані можуть передаватися зі швидкостями 1 і 2 Мбіт / с.

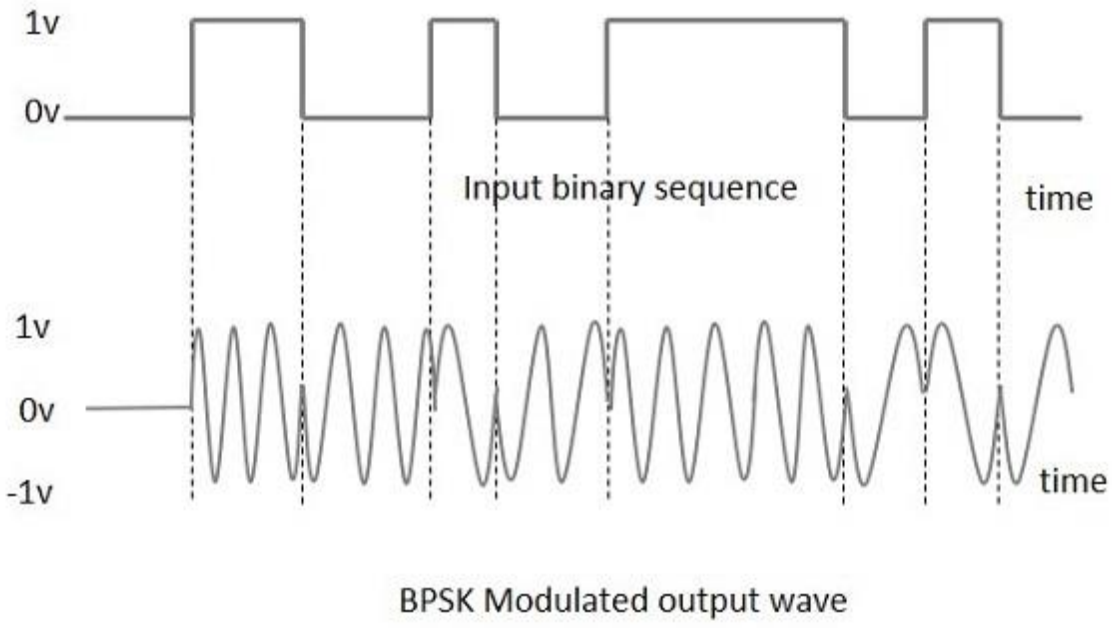

Рисунок 2.4 – Бінарна технологія модуляції PSK із по’єдням DSSS і FHSS.

Існує кілька різновидів WLAN-мереж, які розрізняються схемою організації сигналу, швидкостями передачі даних, радіусом охоплення мережі, а також характеристиками радіопередавачів і приймальних пристроїв.

Найбільш поширеними у використанні користувачами стали бездротові мережі стандарту IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac і інші.

IEEE 802.11a

Стандарт 802.11a був прийнятий в 1999 році, проте знайшов своє застосування тільки з 2001 року. Даний стандарт використовується, в основному, в США і Японії. У Росії і в Європі він не отримав широкого розповсюдження.

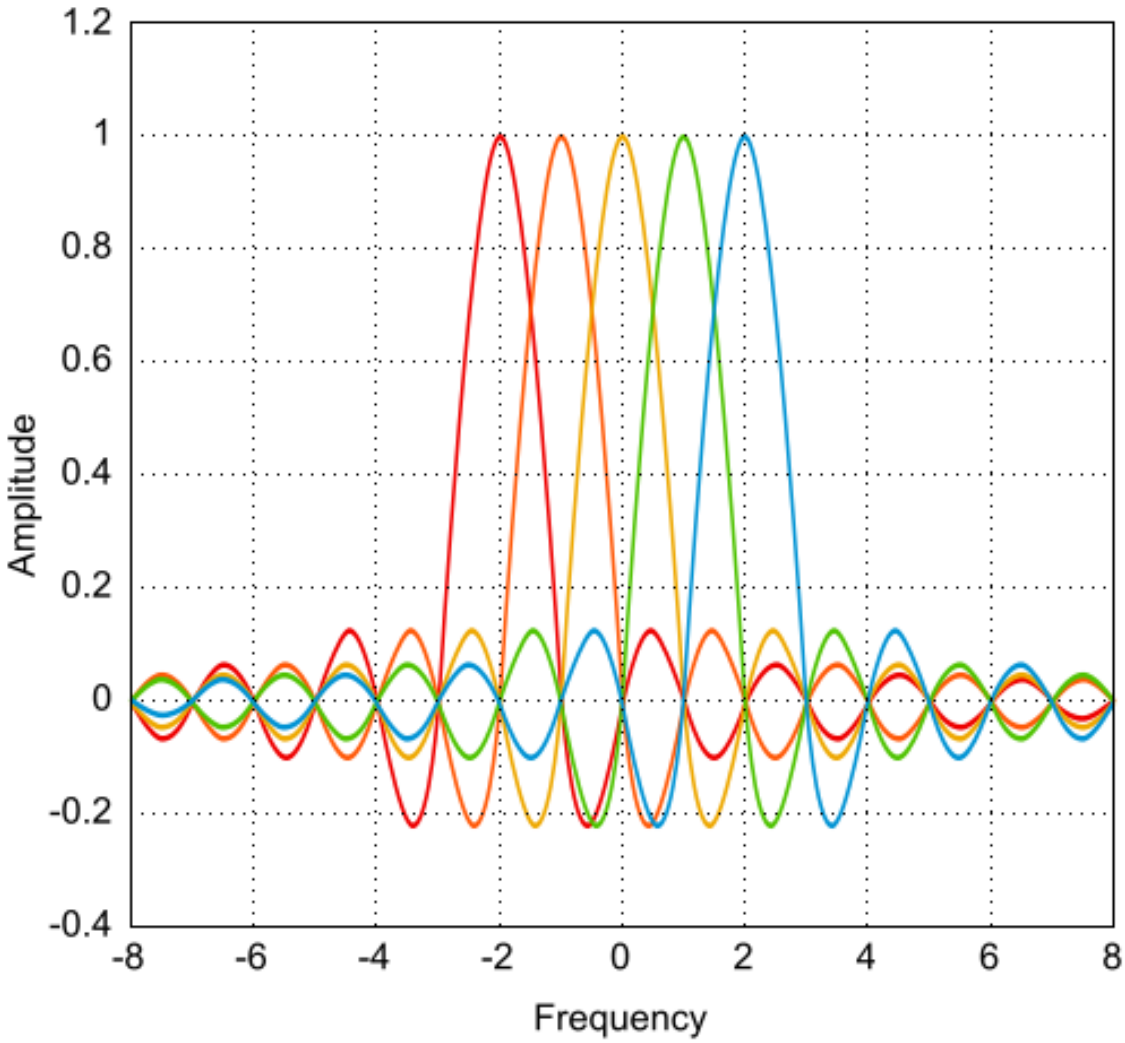

Рисунок 2.5 – Технологія мультиплексування з поділом по ортогональних частотах OFDM

Високошвидкісний стандарт WLAN для частоти 5 ГГц. Підтримує швидкість передачі даних 54 Мбіт / с. У 802.11a застосовується схема модуляції сигналу - мультиплексування з поділом по ортогональних частотах (Orthogonal Frequency Division Multiplexing, OFDM). Технологія мультиплексування з поділом по ортогональних частотах зображена на рисунку 2.5. Основний потік даних розділяється на кілька паралельних субпотоків з відносно низькою швидкістю

передачі, і потім для їх модуляції застосовується відповідне число несучих. Стандартом визначено три обов'язкові швидкості передачі даних (6, 12 і 24 Мбіт / с) і п'ять додаткових (9, 18, 24, 48 і 54 Мбіт / с). Також є можливість одночасного використання двох каналів, що підвищує швидкість передачі даних в 2 рази.

До недоліків 802.11a можна віднести високу споживану потужність радіопередавачів для частот 5 ГГц.

IEEE 802.11b

Стандарт WLAN для частоти 2,4 ГГц був прийнятий в 1999 р. Заснований на методі широкосмугової модуляції з прямим розширенням спектра. В якості базової радіотехнології у ньому використовується метод DSSS (Direct Sequence Spread Spectrum) з 8 розрядними послідовностями Уолша. Весь робочий діапазон ділиться на 14 каналів, рознесених на 25 МГц для виключення взаємних перешкод. Дані передаються по одному з цих каналів без перемикання на інші. Можливо одночасне використання всього 3 каналів.

Підтримує швидкість передачі даних 11 Мбіт /с. Оскільки обладнання, що працює на максимальній швидкості 11 Мбіт /с, має менший радіус дії, ніж на більш низьких швидкостях, то стандартом 802.11b передбачено автоматичне зниження швидкості при погіршені якості сигналу. Швидкість передачі даних може автоматично змінюватися в залежності від рівня перешкод і відстані між передавачем і приймачем [11].

IEEE 802.11ac

Стандарт 802.11ac є подальшим розвитком технологій, запроваджених в стандарт 802.11n. У специфікаціях пристрою стандарту 802.11ac віднесені до класу VHT (Very High Throughput) - з дуже високою пропускною здатністю. Мережі стандарту 802.11ac працюють виключно в діапазоні 5 ГГц. Смуга радіоканалу може становити 20, 40, 80 і 160 МГц. Можливо також об'єднання двох радіоканалів 80 + 80 МГц.

IEEE 802.11e

Дозволяє розширити функціональні можливості стандарт IEEE 802.11a, IEEE 802.11b за допомогою використання методів забезпечення якості обслуговування (QoS).

IEEE 802.11f

Описує порядок зв'язку між рівнозначними точками доступу, що необхідно для побудови розподілених бездротових мереж передачі даних.

IEEE 802.11g

Стандарт 802.11g остаточно був затверджений в червні 2003р. Він є подальшим удосконаленням специфікації IEEE 802.11b і реалізує передачу даних в тому ж частотному діапазоні. 802.11g встановлює додаткову техніку модуляції для частоти 2,4 ГГц.

Головною перевагою цього стандарту є підвищена пропускна здатність - швидкість передачі даних в радіоканалі досягає 54 Мбіт / с в порівнянні з 11 Мбіт / с у 802.11b. Як і IEEE 802.11b, нова специфікація функціонує в діапазоні 2,4 ГГц, однак для підвищення швидкості використовується та ж схема модуляції сигналу, що і в 802.11a - ортогональное частотне мультиплексування (OFDM).

Стандарт 802.11g сумісний з 802.11b. Так адаптери 802.11b можуть працювати в мережах 802.11g (але при цьому не швидше 11 Мбіт / с), а адаптери 802.11g можуть знижувати швидкість передачі даних до 11 Мбіт / с для роботи в старих мережах 802.11b.

802.11g призначений для забезпечення швидкостей передачі даних до 54 Мбіт / с.

IEEE 802.11h

В даному стандарті рівні MAC і PHY доповнюються алгоритмами оптимального вибору частот. Передбачається, що їх рішення буде базуватися на протоколах DFS (Dynamic Frequency Selection) і TCP (Transmit Power Control), створених ETSI. Процедура динамічного регулювання потужності для 802.11h передбачає її зміну в залежності від рівня перешкод з наступним переходом на

інший радіоканал в тому випадку, якщо підвищенням потужності не вдається забезпечити необхідне відношення сигнал / шум.

IEEE 802.11i

Виправляє існуючі проблеми безпеки в областях аутентифікації і протоколів шифрування.

IEEE 802.11n

Стандарт 802.11n був ратифікований 11 вересня 2009 року Він збільшує швидкість передачі даних практично в 4 рази в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт / с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Максимальна теоретична швидкість передачі даних складає 600 Мбіт / с, застосовуючи передачу даних одразу за чотирма антен. За однією антени - до 150 Мбіт / с.

Пристрої 802.11n функціонують в частотних діапазонах 2,4 - 2,5 або 5,0 ГГц.

В основі стандарту IEEE 802.11n лежить технологія OFDM-MIMO. Більшість функціоналу запозичена зі стандарту 802.11a, проте в стандарті IEEE 802.11n є можливість застосування як частотного діапазону, прийнятого для стандарту IEEE 802.11a, так і частотного діапазону, прийнятого для стандартів IEEE 802.11b / g. Таким чином, пристрої, що підтримують стандарт IEEE 802.11n, можуть функціонувати в частотному діапазоні або 5, або 2,4 ГГц, причому конкретна реалізація залежить від країни. Для Росії пристрої стандарту IEEE 802.11n будуть підтримувати частотний діапазон 2,4 ГГц.

Збільшення швидкості передачі в стандарті IEEE 802.11n досягається за рахунок: подвоєння ширини каналу з 20 до 40 МГц, а також внаслідок реалізації технології MIMO.

2.1.3 Стандарти для мережі WMAN

Розроблений Інститутом інженерів з електротехніки та електроніки (IEEE) стандарт 802.16 є стандартом розрахованим на впровадження в міських бездротових мережах технологій.

IEEE 802.16

Завданням 802.16 є забезпечення мережевого рівня між локальними мережами (IEEE 802.11) і регіональними мережами (WAN).

Короткі характеристики стандарту 802.16:

- Пропускна здатність до 135 Мбіт / с при смузі несучої 28 МГц. Модуляція OFDM - 64-QAM.
- Доступ до середовища адаптивний, динамічний.
- Управління мережею централізоване.
- Стандарт 802.16e призначений для мобільних систем. Безпека в мережі забезпечується на рівні протоколу 3-DES.

IEEE 802.16a

Технічні характеристики стандарту 802.16a, передбачають роботу устаткування в діапазоні від 2 до 11 ГГц, є розширеним варіантом технічних характеристик стандарту IEEE 802.16, затверджених в грудні 2001 р Широкий діапазон частот, що передбачається стандартом 802.16, дозволяє розгортати канали передачі даних з високою пропускною здатністю з використанням передавачів, що встановлюються на щоглах мереж стільникового зв'язку та висотних будівлях. Приймає і передає обладнання, що працює за цим стандартом, може перебувати тільки в зоні прямої видимості.

Стандарт 802.16 надає широкі можливості для масштабування, необхідного для забезпечення підтримки сотень тисяч користувачів силами однієї базової станції. Основні характеристики стандартів 802.16 описано у таблиці 2.1 Також відзначаючи сумісність устаткування, здатного працювати в цьому стандарті можна сказати, що він дозволяє операторам скоротити витрати на кінцеве клієнтське

обладнання та одночасно використовувати обладнання різних виробників. Обслуговування клієнтів і управління цим обслуговуванням можна здійснювати віддалено, що дозволяє скоротити поточні витрати.

Таблиця 2.1

Характеристики стандартів 802.16, 802.16a та 802.16e

Назва стандарту	802.16	802.16a	802.16e
Рік впровадження	2001	2003	2004
Швидкодія	10-66 ГГц	2-11 ГГц	2-6 ГГц
Модуляція	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
Ширина каналу	20, 25 та 28 МГц	1,5 – 20 МГц (Можна регулювати)	1,5 – 20 МГц (Можна регулювати)
Радіус дії	2-5 км	7-10 км	2-5 км
Умови для роботи	Пряма видимість	Робота на відображеннях	Робота на відображеннях

Серед інших переваг стандарту можна відзначити широку зону покриття та високу швидкість передачі даних.

2.2 Методи захисту інформації

Для розглядання методів захисту інформації обрано мережі стандарту 802.11, як найбільш поширені і вразливі до атак. У стандарті 802.11 середовище передачі інформації у мережі бездротове і має межі, у яких клієнтське обладнання може їх сприймати. Спираючись на цю інформацію можна сказати, що зловмисник має змогу проникнути до мережі коли він знаходиться у радіусі поширення сигналу цієї

мережі. Оцінюючи можливості проникнення до мережі можна виділити декілька способів, якими можна обмежити поширення радіосигналу. Можна у радіусі поширення сигналу використати охорону або огородження, яке може зменшити ризики проникнення в мережу. Цей спосіб може допомогти зловмиснику не помітити мережу, але якщо на неї йдеться цілеспрямована атака то метод зони під охороною не зможе захистити мережу. Також є можливим захист будівлі за допомогою екранування стін металевою сіткою, яка може дуже сильно послабити рівень сигналу [1]. Користувачі мережі яка використовує екранування стін можуть зі впевненістю користуватися ресурсами мережі в межах будівлі і не відчувати незручностей у роботі.

Також, як один із способів захисту мережі можна виділити приховування імені точки доступу, хоча одним із головних недоліків цього методу захисту є той факт, що мережу приховати можна а її користувачів ні. Тож під час сканування сучасним програмним забезпеченням таку мережу можна буде досить просто ідентифікувати.

Одним із самих вдалих методів захисту мережі є фільтрація по MAC ідентифікаторам. Беручи до уваги те, що кожний бездротовий адаптер має свій унікальний ідентифікатор, то при підключенні до точки доступу адміністратор мережі має додати MAC адресу або унікальний ідентифікатор у спеціальний список MAC адрес точки доступу. Цей сформований список зберігається на точці доступу і змінюється при необхідності адміністратором мережі. При підключенні до мережі будь-якого клієнту точка доступу перевіряє унікальний фізичний ідентифікатор пристрою, що підключається, і якщо данні з таблицею MAC адрес співпадають, то пристрій має змогу підключитися до мережі. Якщо збігів з жодною адресою у таблиці не знайдено то пристрій ігнорується. Недоліком цього способу є можливість зміни MAC адрес на сучасних адаптерах. Також за допомогою спеціального програмного забезпечення можна прослуховувати ефір та ідентифікувати окремих користувачів.

Вказані методи не можуть забезпечити конфіденційність даних що передаються у мережі, вони лише обмежують доступ до мережі. Для більш вдалого

захисту використовують налаштовані складні паролі та додаткові технології захисту.

Одним із найважливіших моментів захисту бездротової мережі також являється пильне відношення адміністраторів мережі до методів і технологій захисту мережі, до паролів які встановлюються для підключення користувачів.

2.3 Технології захисту даних

Серед основних технологій захисту бездротових мереж можна виділити шифрування даних. Існує декілька технологій, які використовують алгоритми шифрування для захисту бездротових мереж - WEP, WPA, WPA2, VPN [3]. Опис технологій можна побачити у таблиці 2.2

Технологія WEP. (Wired Equivalent Privacy) – технологія яка використовує алгоритм RC4 на статичному ключі з динамічним вектором ініціалізації. В процесі роботи мережі ключ який має динамічну частину змінюється в процесі роботи мережі. Недоліком WEP є те, що вектор ініціалізації повторюється через деякі проміжки часу і за допомогою оцінювання проміжків часу цих повторів можна отримати іншу частину ключа.

Технологія WPA (Wi-Fi Protected Access) використовує алгоритм RC4, але на відміну від технології WEP ключі змінюються динамічно. Беручи до уваги те, що вектор ініціалізації довший, ніж у попередньої технології та є можливість використання криптографічної контрольної суми для підтвердження цілісності пакетів, то можна сказати, що WPA є більш надійною ніж WEP. Також є можливість вибору шифрування TKIP/AES.

У WPA є два основних режими роботи WPA-PSK та WPA-Enterprice. Перший режим є корисним для персонального використання. Під час роботи режиму WPA-PSK на точці доступу прописується ключ доступу, ввівши який користувач може користуватися ресурсами мережі. Але для адміністрування мережі з великою кількістю клієнтів доречніше буде використовувати WPA-Enterprice, в якому для

аутентифікації користувачів використовується зовнішній відносно точки доступу сервер. У такому разі при підключенні у мережу користувачі матимуть вводити власну унікальну пару логіну та паролю.

Технологія WPA2. Протокол, який входить до стандарту безпеки бездротових мереж 802.11i. Так як і WPA, WPA2 працює в двох режимах аутентифікації: персональному (Personal) та корпоративному (Enterprise). У персональному режимі з введеної парольної фрази формується 256-розрядний ключ (PreSharedKey).Ідентифікатор ключа (Service Set Identifier) та сам ключ використовуються для генерації тимчасових сеансових ключів (Pairwise Transient Key) для підключення до мережі і взаємодії бездротових пристроїв. Недоліком технології є необхідність розподілу та підтримки ключів на бездротових пристроях підключених до мережі. Для корпоративних мереж оптимальним варіантом використання є WPA2-Enterprice який діє за аналогією до попередньої технології за допомогою підключення до віддаленого серверу автентифікацією користувачів мережі.

Технологія WPA3. 27 червня 2018 року Wi-Fi Alliance оголосив про закінчення розробки нового стандарту безпеки -WPA3. Одним великим нововведенням WPA3 є підтримка PMF (Protected Management Frames) для контролю цілісності трафіку. Але в майбутньому підтримка PMF стане обов'язковою і для WPA2. WPA3 включає програми Wi-Fi Easy Connect і Wi-Fi Enhanced Open. Wi-Fi Easy Connect дозволяє реалізувати спрощену настройку пристроїв без екрану. Для цього можна використовувати інший пристрій вже підключений до бездротової мережі.

Ще одна особливість Wi-Fi Easy Connect -можливість заміни точки доступу без необхідності перенастроювати всі пристрої. Wi-Fi Enhanced Open –шифрування всіх потоків даних між клієнтом і точкою доступу. Ця технологія дозволить захистити приватність користувача в публічних мережах, де не потрібна аутентифікація. Для генерації ключів в таких мережах буде застосовуватися процес

узгодження з'єднання, що реалізовується розширенням Opportunistic Wireless Encryption(OWE).

Так само як і WPA2, третя версія технології захищеного доступу має два режими роботи –Personal та Enterprise. WPA3-Personal відрізняється простішим вибором пароля, щоб користувачі могли легко запам'ятати його. Він також володіє більш високим рівнем безпеки, при якому збережені дані і трафік даних в мережі не будуть скомпрометовані, навіть якщо пароль зламаний і дані вже були передані. WPA3-Enterprise передбачає шифрування на основі як мінімум 192-розрядних ключів, які відповідають вимогам CNSA.

Таблиця 2.2

Технології захисту даних в бездротових мережах

Технології захисту даних	Шифрування	Ключі
WEP	RC4	Статичний ключ з динамічним вектором ініціалізації
WPA	RC4	Ключі, що динамічно змінюються
WPA2	AES	Ключі, що динамічно змінюються
WPA3	WPA3-PSK -128 бітне шифрування і Suite B – 192 бітне OWE	Ключі, що динамічно змінюються
VPN	DES, Triple DES, AES, MD5.	Ключі, що динамічно змінюються

Технологія VPN (Virtual Private Network) може бути прекрасною додатковою технологією захисту бездротової мережі. Вона дозволяє створювати віртуальну персональну мережу у межах будь-якої мережі або декількох мереж. VPN надає великі можливості щодо забезпечення конфіденційності клієнтів за допомогою шифрування та маскування IP адреси. Також деякі служби мають власну систему

доменних імен, що дозволяє замість довгих IP адрес вводити назви сайтів, на які клієнт бажає потрапити. Сукупність захисних можливостей VPN може надати гарний додатковий захист мережі.

Принципом дії VPN є створення безпечного «тунелю» між користувачем і сервером. Для шифрування трафіку VPN може використовувати такі протоколи: IPSec, PPTP та L2TP. У поєднанні з цим найчастіше використовуються такі алгоритми шифрування: DES, Triple DES, AES, MD5.

Технологія VPN найчастіше використовується у великих корпоративних мережах, але вона може бути корисною і для домашнього використання. Висока надійність та сумісність з великою кількістю платформ таких як Windows, Linux та Mac OS надає змогу використовувати технологію як додатковий засіб захисту у будь-якій мережі із можливістю поєднання з будь-якою технологією захисту бездротових мереж.

Також для того щоб мінімізувати ризики втручання або злому для бездротової мережі у якості захисту можна використовувати:

Зміну паролів за замовчуванням. Для спрощення налаштування більшості мережевих пристроїв, включаючи бездротові точки доступу, попередньо адміністратори мережі налаштовують паролі за замовчуванням. Ці паролі легко доступні для отримання в Інтернеті, тому забезпечують лише граничний захист. Зміна паролів за замовчуванням ускладнює доступ зловмисників до пристрою. Використання складних паролів та періодична їх зміна - це перша захисна лінія захисту пристрою.

Обмеження доступу. Дозвіл доступу до мережі лише авторизованим користувачам є гарною ланкою захисту. Кожна апаратна частина, підключена до мережі, має адресу контролю доступу до медіа (MAC). Можна обмежити доступ до мережі, відфільтрувавши MAC-адреси. Також для надання доступу користувачам у мережі можна використовувати обліковими записами "гість", які широко використовується у багатьох бездротових маршрутизаторах. Ця функція дозволяє

надати гостям бездротовий доступ на окремому бездротовому каналі з окремим паролем, зберігаючи конфіденційність основних даних.

Шифрування даних у мережі. Шифрування бездротових даних перешкоджає перегляду інформації всіма, хто може отримати доступ до мережі. Для забезпечення цього захисту доступно кілька протоколів шифрування. Захищений доступ до Wi-Fi наприклад шифрується за допомогою розглянутих технологій захисту: (WPA), WPA2 та WPA3. На даний момент WPA3 є найсильнішим шифруванням. WPA та WPA2 все ще доступні; однак бажано використовувати обладнання, яке спеціально підтримує WPA3 або WPA2 у поєднанні наприклад з фаєрволом, оскільки використання інших протоколів може залишити вашу мережу відкритою для експлуатації.

Захист ідентифікатору набору послуг (SSID). Щоб сторонні особи не могли легко отримати доступ до мережі, необхідно уникати оприлюднення SSID. Усі маршрутизатори Wi-Fi дозволяють користувачам захищати SSID свого пристрою, що ускладнює пошук зловмисників мережі. Принаймні, можлива заміна SSID на щось унікальне. Залишення за замовчуванням виробника може дозволити потенційному зловмисникові визначити тип маршрутизатора та, можливо, використати будь-які відомі вразливості.

Встановлення брандмауеру. Можливість встановлення брандмауера безпосередньо на бездротових пристроях (брандмауер на основі хоста), а також у домашній мережі (брандмауер на основі маршрутизатора або модему) також є гарним методом захисту бездротової мережі. Зловмисники, які можуть безпосередньо підключитися до мережі, можуть обійти мережевий брандмауер - брандмауер на основі хоста додасть рівень захисту даних на пристрої безпосередньо.

Підтримка антивірусного програмного забезпечення. Встановлення антивірусного програмне забезпечення та постійно оновлення не тільки допоможе у визначення вірусів, а й у аналізі підозрілих отриманих пакетів по трафіку мережі. Також деякі антивіруси мають функцію попередження про небезпечні веб ресурси,

що також корисно. Багато антивірусних програм також мають додаткові функції, які виявляють або захищають від шпигунське та рекламного ПЗ.

Використовування обміну файлами з обережністю. Спільний доступ до файлів між пристроями слід вимкнути, коли це не потрібно. Доступ до файлів завжди має бути дозволеним лише лише в домашніх або робочих мережах, ніколи в загальнодоступних мережах. Можливим є створення спеціального каталогу для обміну файлами та обмеження доступ до всіх інших каталогів. Крім того треба захищати паролем все що можливо.

Слідкування за оновленням програмного забезпечення точки доступу. Виробник бездротової точки доступу періодично видає оновлення та виправлення програмного забезпечення та мікропрограми пристрою. Обов'язковим є перевірка веб-сайту виробника на наявність оновлень або виправлень для мережевого ристрою.

Перевірка варіантів бездротової безпеки провайдера або виробника маршрутизатора. Постачальники послуг Інтернету та виробник маршрутизаторів можуть надати інформацію або ресурси, які допоможуть захистити бездротову мережу. Отже також можна перевірити область підтримки клієнтів на веб-сайтах, щоб отримати конкретні пропозиції чи інструкції.

Використання віртуальної приватної мережі (VPN). Багато компаній та організацій мають VPN. VPN дозволяють працівникам безпечно підключатися до своєї мережі, коли вони не в офісі. VPN шифрують з'єднання на кінцях надсилання та отримання та утримують трафік, який не зашифрований належним чином. Він може бути використаний як додатковий спосіб захисту мережі.

Висновок за розділом 2

Оцінюючи можливості проникнення до мережі можна виділити декілька способів, якими можна обмежити поширення радіосигналу і захистити мережу – це обмеження території у межах якої діє мережа та екранування стін будівель. Разом із

обмеженням поширення радіосигналу є доцільним використання фільтрації по MAC ідентифікаторам.

Вказані методи не можуть забезпечити конфіденційність даних що передаються у мережі, вони лише обмежують доступ до мережі. Для більш вдалого захисту використовують налаштовані складні паролі та додаткові технології захисту.

Серед технологій захисту безпровідних мереж за допомогою алгоритмів шифрування розглянуто декілька технологій захисту для бездротових мереж - WEP, WPA, WPA2, VPN.

Під час ознайомлення з технологіями захисту бездротових мереж найбільш стійкою виявилася WPA2, адже WPA та WEP не можуть дати надійний захист бездротової мережі. Використання протоколу WPA2 у поєднанні з технологією Virtual Private Network може бути оптимальним захистом для користувачів будь-якої мережі. Також важливо не забувати, що безпека мережі залежить від її адміністрування, наприклад стійкості і надійності паролів та зміна їх та від користувачів, які також не повинні нехтувати безпекою мережі.

Оцінюючи принципи роботи бездротових мереж, аналізуючи їх вразливості та можливості проведення атак на них можна зробити висновок що захист бездротових мереж є доволі недосконалим і важливим є розробка нових методик захисту та вдосконалення існуючих технологій. Також обізнане використання існуючих методів і технологій захисту може мінімізувати вплив на слабкі місця бездротових мереж.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ ПРОГРАМНИХ ЗАСТОСУНКІВ ЗАХИСТУ ІНФОРМАЦІЇ ЩО ПЕРЕДАЄТЬСЯ

3.1 Опис ключових характеристик програмного забезпечення

Базуючись на попередніх аналізах вразливостей бездротових середовищ і недосконалості існуючих методів захисту можна стверджувати що бездротові мережі потребують у додаткових механізмах захисту. У наслідок проведеного аналізу було розроблено програмне забезпечення на базі антисніферу для моніторингу стану мережі і пошуку підозрілого трафіку. У процесі розробки програмного забезпечення було використано програмну мову C# та графічну підсистему для створення користувацького інтерфейсу WPF (Windows Presentation Foundation).

Програмне забезпечення зібрало в собі декілька функцій для захисту інформації в бездротових мережах, а саме:

- Збирання інформації про всі доступні точки доступу
- Збирання інформації про підключену точку доступу
- Аналіз трафіку та додавання його до бази програмного забезпечення
- Оповіщення користувача про підозрілий трафік

Ціль програмного забезпечення в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

Програмне забезпечення працює майже як і більшість аналізаторів мереж Wi-Fi, у ньому як і у звичайних аналізаторах мереж обирається бездротовий спектр для дослідження, наприклад 2,4 ГГц або 5 ГГц і потім досліджується цей спектр, щоб переглянути мережі, їх канали та потужність сигналу.

Простіше кажучи, аналізатор Wi-Fi збирає інформацію про точки доступу та канали у вашій мережі та відображає її легко зрозумілим, візуально доступним способом. У розробленій програмі реалізований зручний користувацький інтерфейс який спрощує процес аналізу мережі (рис.3.1).

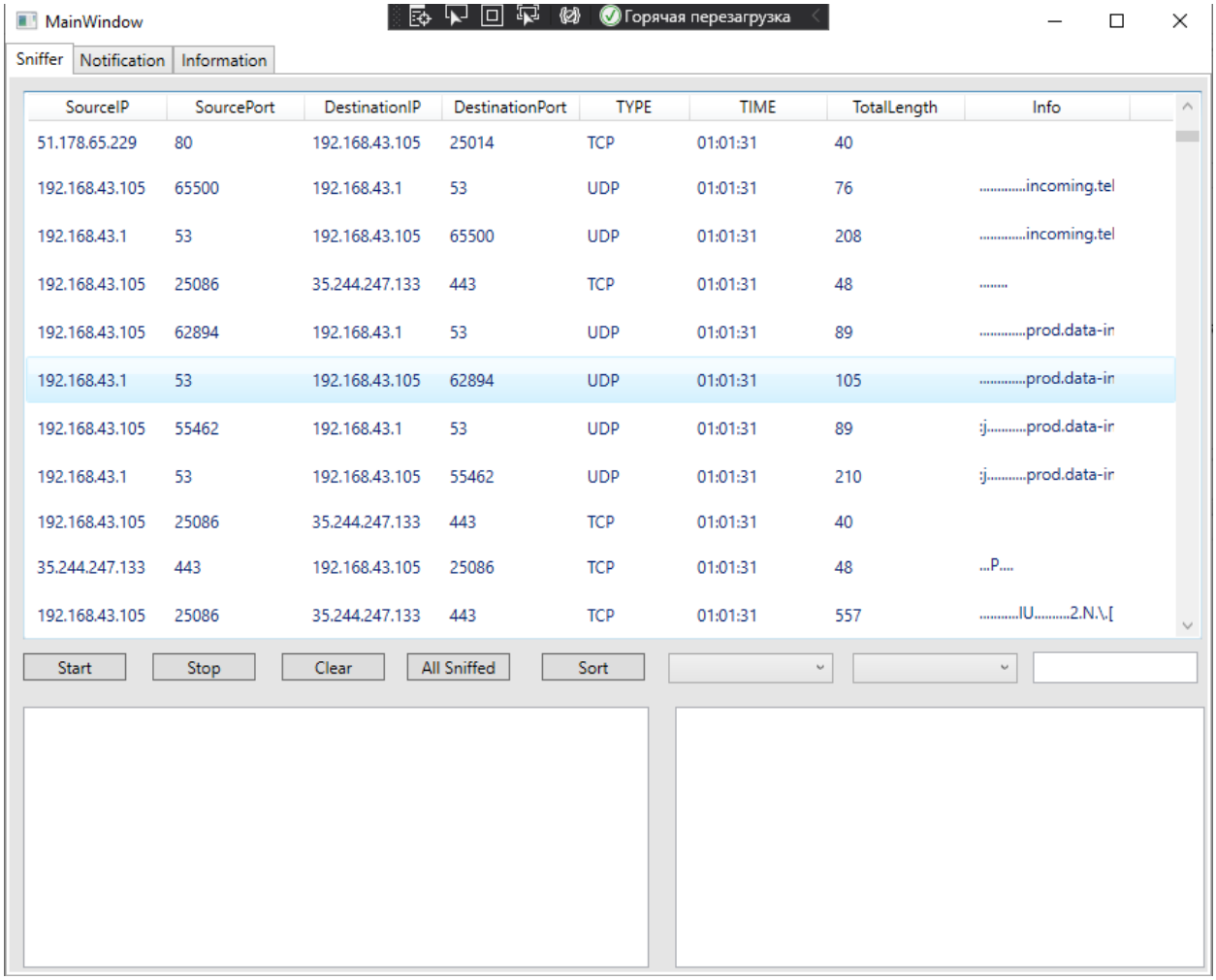

Рисунок 3.1 – Інтерфейс програмного забезпечення

Разом із функціями аналізатору мережі програмне забезпечення підтримує можливість аналізу трафіку, який передається у мережі. За допомогою подібного трафіку можна виділити дані IP адрес, пакети що передаються та порти, якими передано ту чи іншу інформацію.

Аналізатор бездротової мережі може допомогти підтримувати якість з’єднання, що може бути важливим моментом для підняття показників продуктивності у мережі. Сигнали Wi-Fi постійно змінюються, і незначні зміни в мережі можуть мати значний вплив на загальну тривалість роботи з’єднання.

Використання мережевого аналізатора Wi-Fi допомагає збирати дані та виявляти проблеми або вказувати на потенційні рішення, такі як перехід на інший канал для зменшення перевантажень.

3.2 Головні функції програмного забезпечення

Аналіз трафіку, який проходить через програмне забезпечення, дозволяє:

- Виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку;
- У перспективі виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші.
- Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.
- Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами).

Дослідження стану мережі у програмному забезпеченні було розроблено на базі алгоритмів сніферів. До нього входить збір даних про інформацію яка передається у мережі, вивід інформації про всі доступні точки доступу у мережі, вибір протоколу передачі, яким інформація передається та вивід інформації щодо портів і пакетів даних які були відправлені або отримані. Схема роботи програмного забезпечення зображена на Рисунку 3.2.

У програмному забезпеченні реалізовано такі функції:

- вивід кількості отриманих пакетів;
- вивід інформації в середині пакетів;
- можливість сортування пакетів за протоколом, IP адресою та портом;
- можливість отримання інформації всередині переданих пакетів даних;
- вивід інформацію про кількість пакетів надісланих з певної адреси за короткий проміжок часу;
- вивід отриманої інформації щодо реєстрованих даних о власниках мережі за допомогою команди WHOIS;
- вивід інформації про мережі навколо;
- вивід поширеної інформації про мережу, до якої підключено пристрій;

- інформування користувача мережі про не звичний для неї трафік.

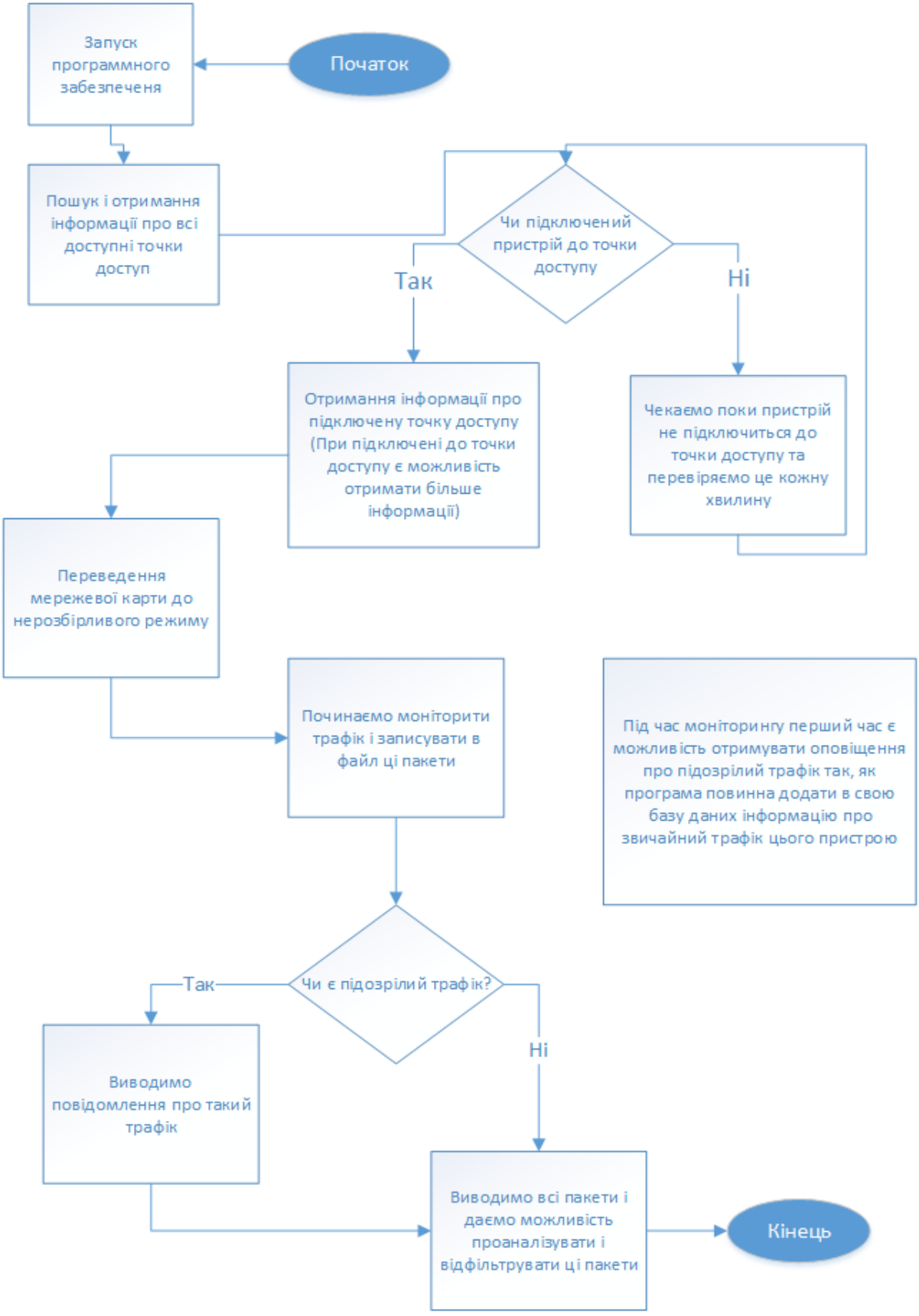

Рисунок 3.2 – Схема роботи програмного забезпечення

Вивід кількості просканованих пакетів вспливає спеціальним повідомленням після закінчення сканування (рис.3.3). Закінчити або тимчасово зупинити роботу сканування можна за допомогою кнопки «Stop», а розпочати або продовжити роботу програми можна відповідно за допомогою кнопки «Start». Якщо є необхідність очистити список просканованої мережі у програмному забезпеченні то зробити це можна за допомогою кнопки «Clear».

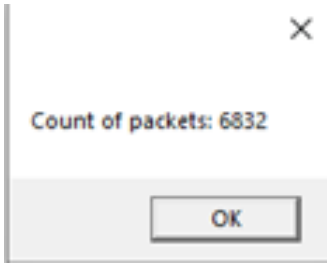

Рисунок 3.3 – Повідомлення про кількість отриманих пакетів за певний проміжок часу

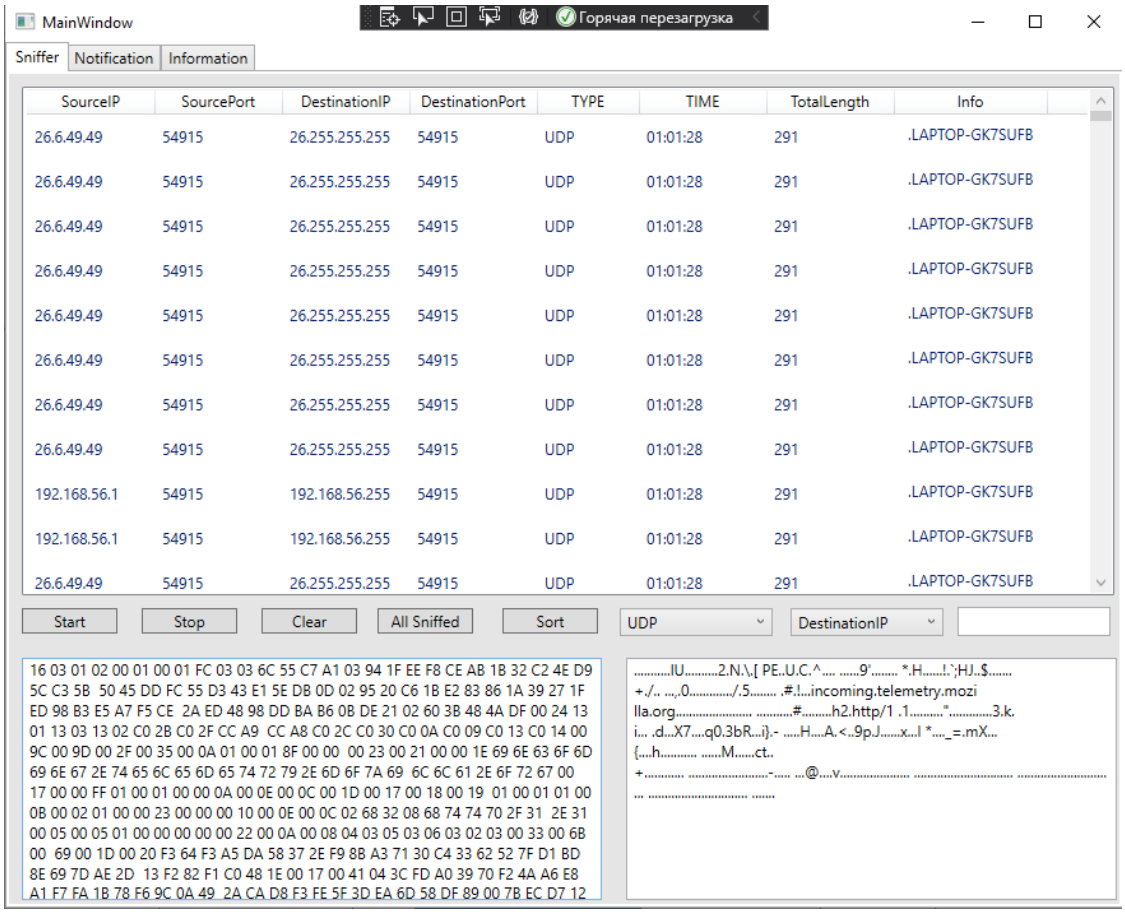

Рисунок 3.4 – Сортування отриманих пакетів за протоколом UDP

Також у програмному забезпеченні реалізована можливість сортування пакетів за протоколами передачі. На рисунку 3.4 зображено відсортировані пакети, які передавались за допомогою UDP.

Програмне забезпечення реалізує механізм сортування за такими протоколами: TCP, UDP, GGP, ICMP, IDP, IGMP, IP, ND, PUP, OTHERS. Механізм сортування зображено на рисунку 3.5.

Також являється можливим сортування за IP адресою та портом. Механізм сортування відбувається при виборі з випливаючого вікна протоколів потрібного для сортування і натисканні кнопки «Sort» або при вводі IP адреси у стрічку вводу, якщо потребується сортування за певною адресою.

Кнопка «All sniffed» повертає назад проаналізований початковий трафік, тож при необхідності можна повернутися до повного списку захопленого програмним забезпеченням трафіку.

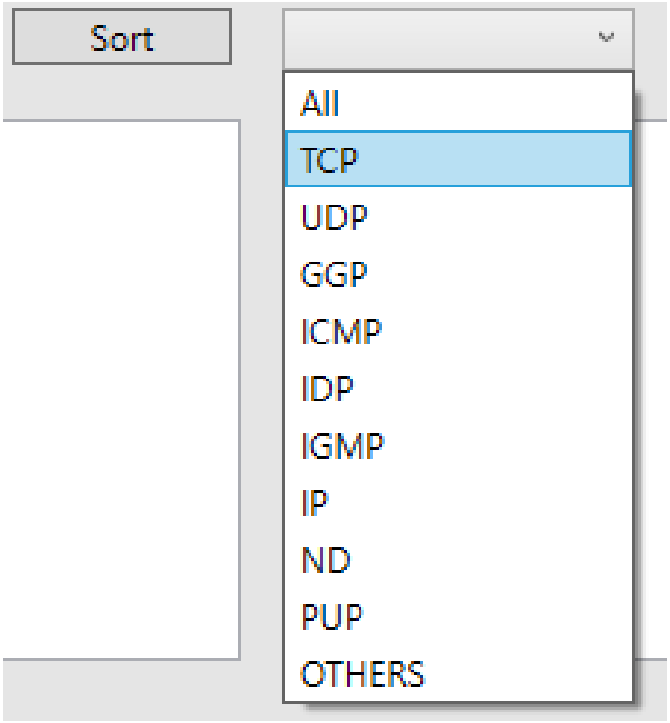

Рисунок 3.5 – Сортування трафіку за протоколами

Програма підтримує функцію отримання інформації щодо реєстрованих даних про власників мережі за допомогою команди WHOIS і реалізується при виборі певної IP адреси і натисканні кнопки «WHOIS» відповідно (рис.3.6.). Дана функція

може бути використана для запитів баз даних для визначення доменної зони, IP адреси або автономного системного номеру у глобальній мережі Інтернет.

У програмному забезпеченні також є функція вираховування кількості пакетів, що були відправлені з певної адреси. Вона допомогає оцінитити небезпечний трафік, який як раз може бути спрямований на перенасичення мережі великою кількістю пакетів у малий проміжок часу. Подібний небезпечний трафік може не тільки сповільнити роботу мережі, а і спровокувати відмову роботи мережі. Отже аналіз кількості отриманих пакетів може попередити адміністратора мережі про можливу загрозу або атаку яка реалізується.

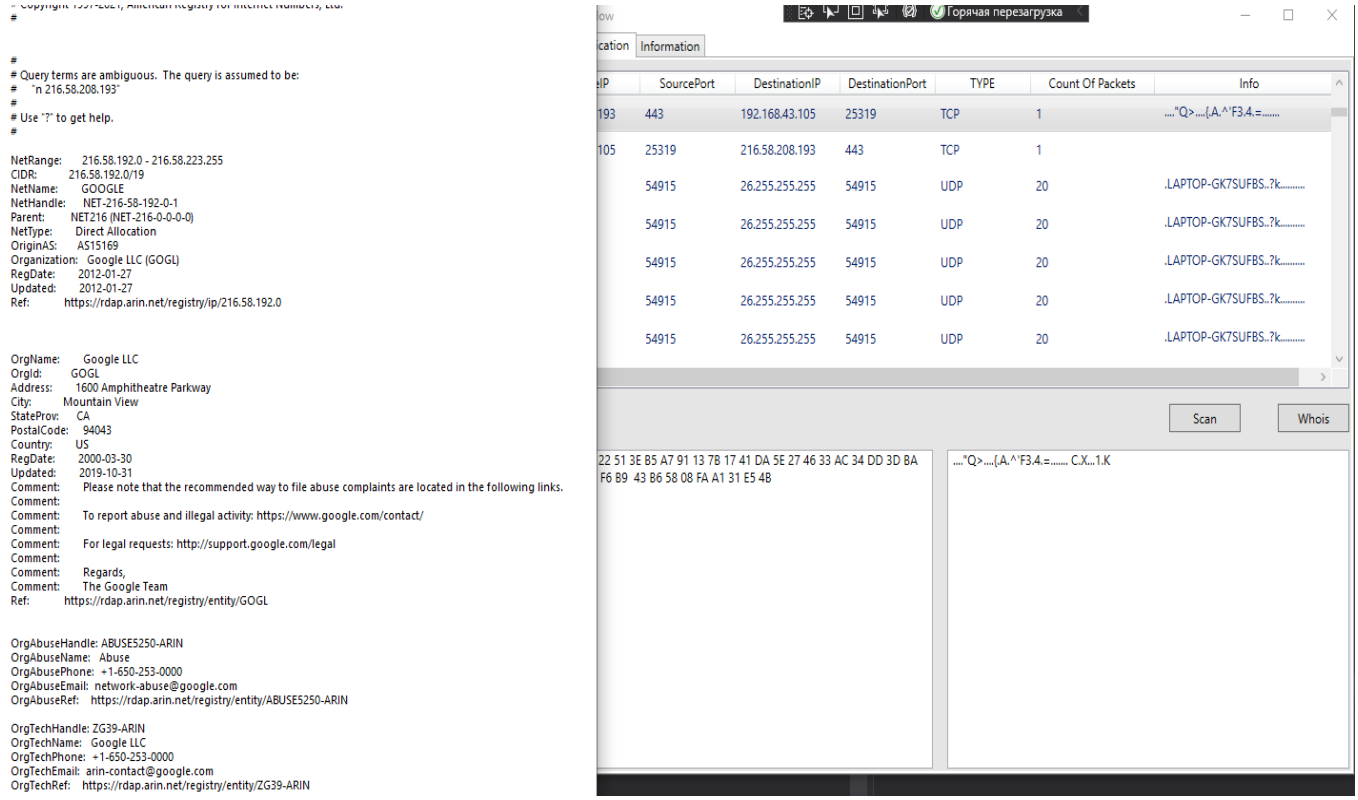

Рисунок 3.6 – Отримання інформації щодо реєстрованих даних про власників мережі за допомогою команди WHOIS

Важливою частиною розробки програмного забезпечення також була можливість аналізу інформації про найближчі точки доступу та про підключену точку доступу. Мережа, яку було просканована мала назву «Weirana». Результат отриманий під час сканування можна побачити на рисунку 3.7.

Сканування мережі дало змогу дізнатися такі характеристики мережі:

- Аутентифікація: RSNA_PSK;
- Шифрування: CCMP;
- Тип мережі: Infrastructure;
- BSSID 1: A:C5:E1:D7:F2:CE;
- Сигнал: 100;
- Частота: 2,462 GHz;
- Тип функції: Wireless80211;
- Канал: 11;
- Базова частота (MBit/s): 11;
- Інші частоти (MBit/s): 1 2 5,5 11 18 24 36 54 6 9 12 48.

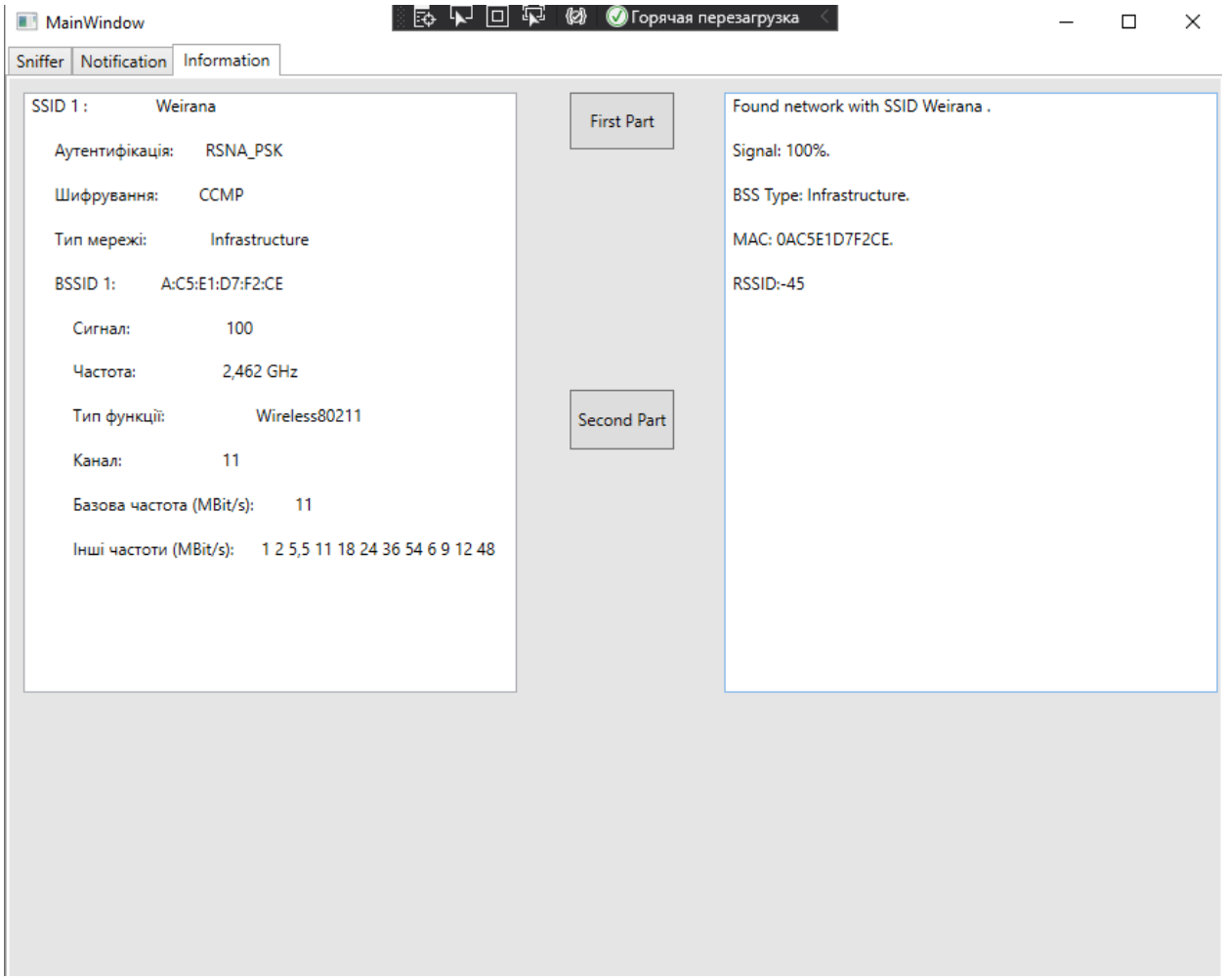

Рисунок 3.7 – Отримання інформації про власну і оточуючі мережі.

Повідомлення про підозрілий трафік у мережі також є невід'ємною частиною програмного забезпечення. При визначенні подібного програмне забезпечення відкриває вікно, щоб повідомити користувача мережі для того щоб він міг приділити увагу до ситуації (рис.3.8).

Підозрілим трафіком програмне забезпечення вважає нові IP адреси і трафік, який з ними пов'язаний. Попередньо програма шукає інформацію у базі даних щодо IP і надісланих з неї пакетів інформації.

На початку старту роботи програми буде дуже багато не звичного трафіку, але з поширенням бази даних програма зможе чіткіше формулювати список підозрілого трафіку. Цю функцію можна вдосконалювати у майбутньому наприклад додавши нейронну мережу, яка буде навчатись розпізнавати такий трафік, порівнювати його з локальною базою даних та відслідковувати загрози мережевого середовища звіряючи отримані данні з мережі з глобальними базами загроз і шкідливого програмного забезпечення.

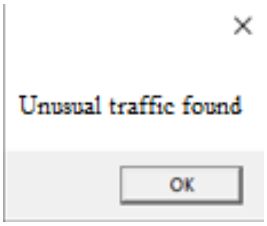

Рисунок 3.8 – Повідомлення про незвичний трафік

Також не звичним трафіком програмне забезпечення вважає велику кількість трафіку що може надсилатися з певних адрес. Тобто якщо програма аналізує те, що більша частина трафіку тобто більше половини трафіку за деякий невеликий проміжок часу була надіслана з одної адреси, то ця адреса потрапить у список підозрілого трафіку. Це може попередити адміністратора мережі про можливість атаки відмови в обслуговуванні. У наслідок адміністратор мережі може не тільки просканувати власну мережу, але й відслідкувати не звичний для цієї мережі трафік і при пильному користуванні програмним забезпеченням у наслідок мінімізувати ризики втручання у мережу при необхідності.

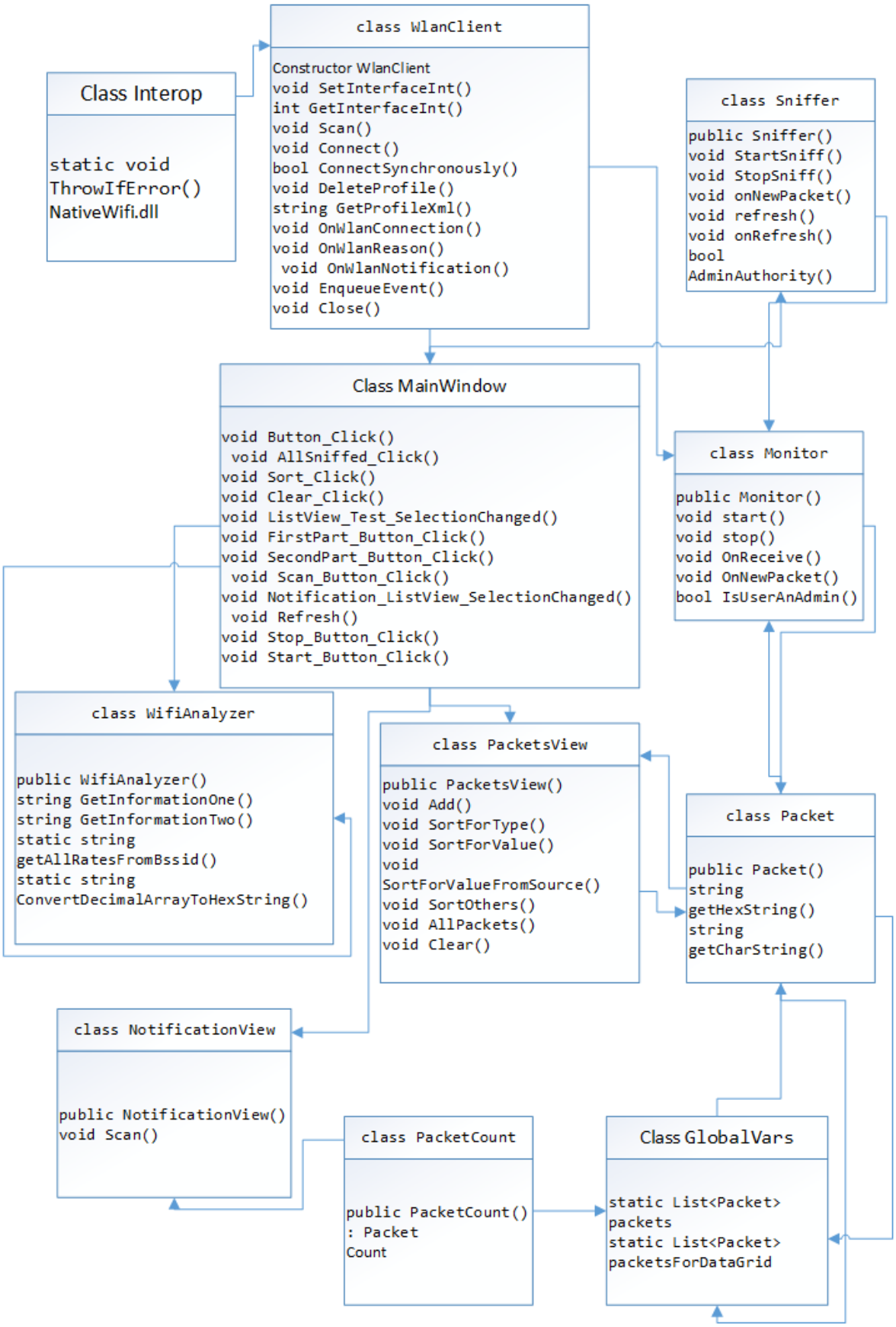

Рисунок 3.9 – Схема класів програмного забезпечення

Програма має 11 основних класів для виконання: Main window, Sniffer, Monitor, Wifi analyzer, Packets View, Packet Count and Global vars (рис.3.9). Функції сканування мережі, аналіз пакетів і трафіку використовуються завдяки класам Sniffer, Monitor, Packets View, Packet Count аналіз мережі, до якої підключено пристрій реалізовано у класі Wifi analyzer. Інші класи являють собою по більшій частині допоміжну функцію для правильної роботи програми.

Програмне забезпечення на базі антисніферу є корисним застосунком для досвідчених користувачів мережі, які бажають підкращити можливості власної мережі за допомогою аналізатору мереж. Також програмне забезпечення може бути використано в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

Можливості програмного забезпечення можуть бути використані для наукових цілей. Також можливим є варіант вдосконалення програми у подальшому.

Оцінивши існуючі програми захисту бездротових мереж під час створення програмного забезпечення можна сказати що у програми є майбутне в плані розвитку роботи з нейромережами і машинним навчанням. Ця функція може значно покращити функції аналізатору трафіку за допомогою глобальних баз даних загроз, які можуть використовуватись для пошуку пакетів із зловмисним трафіком і безперечно такий аналіз покращить захищеність бездротових мереж.

Висновок за розділом 3

У результаті аналізу роботи бездротових мереж, їх вразливостей і дослідження методів і технологій захисту бездротових мереж було розроблено програмне забезпечення яке виконує функції моніторингу з аналізом трафіку бездротової мережі, протоколів передачі у мережі. Також програмним забезпеченням виконується аналіз підозрілого трафіку у мережі.

У процесі розробки програмного забезпечення було використано програмну мову C# та графічну підсистему для створення користувацького інтерфейсу WPF (Windows Presentation Foundation).

Розроблене програмне забезпечення зібрало в собі такі функції для захисту інформації в бездротових мережах, а саме

- Збирання інформації про всі доступні точки доступу
- Збирання інформації про підключену точку доступу
- Аналіз трафіку та додавання його до бази програмного забезпечення
- Оповіщення користувача про підозрілий трафік

Програмне забезпечення на базі антисніферу може стати застосунком для досвідчених користувачів мережі, які бажають підкращити можливості власної мережі за допомогою аналізатору мереж. Також програмне забезпечення може бути використано в покращенні зручності адміністрування мережі за допомогою можливості сканування мережі і дослідження підозрілого або не звичного трафіку у мережі.

ВИСНОВКИ

В дипломній роботі було проведено дослідження щодо захищеності бездротових мереж і проведено оцінку їх вразливостей. Було проаналізовано можливі атаки на бездротове середовище та виділено слабкі місця бездротових мереж. Також були досліджені сучасні методи і технології захисту бездротових мереж і у наслідок написано програмне забезпечення, яке дозволить моніторити стан мережі і виявляти підозрілий трафік.

Під час аналізу особливостей роботи бездротового середовища, передачі даних та під час оцінки поширеності бездротових мереж у сучасному світі було розглянуто існуючі мережі і виділено декілька основних типів бездротових мереж за територіальною ознакою: WLAN, WMAN, WPAN. Також було виявлено проблематику захисту інформації в бездротовому середовищі і зроблено висновок щодо важливості їх захисту.

Не зважаючи на те що сьогодні в захисті бездротових мереж і застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних, контролю цілісності їх передачі, і досі можна сказати, що бездротові мережі являються дуже вразливими.

Результатом дослідження захищеності мережі було отримання даних про те що бездротові мережі вразливі до зламу паролів, перехоплення трафіку, підміни мережі, та затримки роботи мережі або атаки відмови в обслуговуванні. Кожна з цих атак може внести значний вплив на роботу мережі або може відобразитися на користувачах і їх даних, які потрапили у мережу і могли бути скомпроментовані зловмисником. Отже після дослідження захищеності мережі можна сказати, що бездротові мережі потребують у додаткових методах захисту. Також є доцільним використання спеціальних механізмів і технологій захисту.

Аналізуючи методи і технології захисту було описано сучасні технології захисту даних у мережі, які використовують шифрування інформації для безпечної передачі даних. Шифрування та інші методи захисту ускладнюють процес перехвату

даних, що у комплексі з іншими методами захисту і пильним адмініструванням мережі створюють гарну систему захисту бездротової мережі. Також було проаналізовано технологію роботи стандарту Wi-Fi і суміжних протоколів та алгоритмів, що розроблялися для підвищення захищеності мереж.

На основі отриманих даних було розроблено програмне забезпечення яке виконує функції моніторингу з аналізом трафіку бездротової мережі, протоколів передачі у мережі. Також програмним забезпеченням виконується аналіз підозрілого трафіку у мережі.

Виходячи з вищесказаного можна з певністю сказати що була виконана основна мета роботи по розробці аналазатору трафіку на базі отриманих у процесі дослідження даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Информационная безопасность: защита и нападение. А. А. Бирюков

2 Росс Джон. Wi-Fi. Беспроводная сеть

3 Вишневский В.М. Широкополосные беспроводные сети передачи информации (2005). - 592 с.

4 Максим М. Безопасность беспроводных сетей / М. Максим, Д. Поллино — М.: ДМК-Пресс, 2004. - 288с.

5 Барнс К. Защита от хакеров беспроводных сетей / К. Барнс, Т. Боутс, Д. Лойд М.: ДМК-Пресс, 2005. - 480с.

6 ISO 15408 Общие критерии оценки безопасности информационныхтехнологий

7 Ященко В.В. Введение в криптографию. / В.В. Ященко. М: МЦНМО, 1998.- 272 с.

8. Хансен Д. Атаки на беспроводные сети Електроний ресурс. / Д. Хансен. - Режим доступу: http://www.securitylab.ru/analytics/216360.php

9. Фридланд А. Я. Информатика и компьютерные технологии: Основные термины: Толков, слов.: Более 1000 базовых понятий и терминов. — 3-е изд., испр. и доп. / А. Я. Фридланд, Л .С. Ханамирова, И. А. Фридланд. — М.: ООО «Издательство Астрель»: ООО «Издательство АСТ», 2003

10. Общее понимание связи пятого поколения. Електроний ресурс. Режим доступу:

https://trends.rbc.ru/trends/industry/cmrm/5daed56a9a7947b119ba88dd

11. Барнс К. Защита от хакеров беспроводных сетей / К. Барнс, Т. Боутс, Д. Лойд М.: ДМК-Пресс, 2005. - 480с.

12. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. М.: Горячая линия - Телеком, 2000. - 452 с.

13. Ben Salem N. Securing Wireless Mesh Networks / N. Ben Salem, J.-P. Hubaux // IEEE Wireless Communications. 2006. - №13/2.

14. Dorges T. A Network of IDS Sensors for Attack Statistics / T. Dorges, O. Gellert, K. Kossakowski // Praxis der Informationsverarbeitung und Kommunikation. — 2004. №27. - P. 202-208.

15. Феллер В. Введение в теорию вероятностей и ее приложения / В. Феллер —1. М.: Мир, 1964-752 с.

16. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко СПб.: БХВ-Петербург, 2009. - 576 с.

17. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. / М.А. Иванов. — М.: КУДИЦ-ОБРАЗ, 2001.-368 с.

ДОДАТОК А

Sniffer.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Net;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
namespace ProjectOne
{
    class Sniffer
    {
        #region Vars
        List<Monitor> monitorList = new List<Monitor>();
        TimeSpan amountOfLifeTime;
        bool started = false;
        #endregion
        #region Accesses
        public List<Monitor> MonitorList
        {
            get { return monitorList; }
        }
        public TimeSpan AmountOfLifeTime
        {
            get { return amountOfLifeTime; }
            set { amountOfLifeTime = value; }
        }
        #endregion
        #region Constructors
        public Sniffer()
        {
        }
        public Sniffer(TimeSpan amountOfLifeTime)
        {
            this.amountOfLifeTime = amountOfLifeTime;
        }
        #endregion
        #region Methods
        public void StartSniff()
        {
            if(AdminAuthority())
            {
                IPAddress[] hosts = Dns.GetHostEntry(Dns.GetHostName()).AddressList;
                if (hosts == null || hosts.Length == 0)
                {
                    MessageBox.Show("No hosts detected, please check your network!");
                }
                for (int i = 0; i < hosts.Length; i++)
                {
                    Monitor monitor = new Monitor(hosts[i]);
                    monitorList.Add(monitor);
                }
                foreach (Monitor monitor in monitorList)
                {
                    monitor.start();
                }
                started = true;
```

```
            }
        }
        public void StopSniff()
        {
            if(started)
            {
                foreach (Monitor monitor in monitorList)
                {
                    monitor.stop();
                }
            }
        }
        private void onNewPacket(Monitor monitor, Packet p)
        {
        }
        delegate void refresh(Packet p);
        private void onRefresh(Packet p)
        {
        }
        /// <summary>
        /// </summary>
        /// <returns></returns>
        bool AdminAuthority()
        {
            bool result = false;
            System.Security.Principal.WindowsIdentity identity =
System.Security.Principal.WindowsIdentity.GetCurrent();
            System.Security.Principal.WindowsPrincipal principal = new
System.Security.Principal.WindowsPrincipal(identity);
            //whether the current operation is executed by administrators or not;
            if (principal.IsInRole(System.Security.Principal.WindowsBuiltInRole.Administrator))
            {
                //MessageBox.Show("You are admin!");
                result = true;
            }
            else
            {
                //MessageBox.Show("You are user!");
            }
            return result;
        }
        #endregion
    }
}
```

WifiAnalyzer.cs

```
using System;
using NativeWifi;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using static NativeWifi.Wlan;
using System.Windows;

namespace ProjectOne
{
    class WifiAnalyzer
    {
        WlanClient client = new WlanClient();
        Dictionary<int, int> GHz24 = new Dictionary<int, int>();
        int[] GHz24Channel = { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 };
        int[] GHz24Frequency = { 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457,
2462, 2467, 2472, 2477, 2482 };
```

```
        int i = 0;
        public WifiAnalyzer()
        {
            GHz24Channel.ToList().ForEach(delegate (int channel)
            {
                GHz24.Add(GHz24Frequency[i], channel);
                i++;
            });
        }
        public string GetInformationOne()
        {
            string result = "";
            foreach (WlanClient.WlanInterface wlanIface in client.Interfaces)
            {
                Wlan.WlanAvailableNetwork[] networks = wlanIface.GetAvailableNetworkList(0);
                Wlan.WlanBssEntry[] bssidds = wlanIface.GetNetworkBssList();
                i = 1;
                foreach (WlanAvailableNetwork network in networks)
                {
                    int x = 1;
                    if (!network.profileName.Equals(""))
                    {
                        string tempString = "SSID " + i + " :                " +
network.profileName +"\n" + "     Аутентифікація:       " + network.dot11DefaultAuthAlgorithm +
"\n"
                            + "     Шифрування:         " + network.dot11DefaultCipherAlgorithm +
"\n" + "     Тип мережі:               " + network.dot11BssType + "\n";

                        result += tempString;
                    }
                    foreach (Wlan.WlanBssEntry bssidd in bssidds)
                    {
                        if (bssidd.dot11Ssid.SSID.SequenceEqual(network.dot11Ssid.SSID) &&
!network.profileName.Equals(""))
                        {
                            string tempStringTwo = "     BSSID " + x + ":          " +
ConvertDecimalArrayToHexString(bssidd.dot11Bssid) + "\n" + "         Сигнал:
"
                                + bssidd.linkQuality + "\n" + "         Частота:
" + bssidd.chCenterFrequency / 1000000.0 + " GHz" + "\n" + "         Тип функції:
"
                                + wlanIface.NetworkInterface.NetworkInterfaceType + "\n" + "
Канал:                      " + wlanIface.Channel + "\n"
                                + "         Базова частота (MBit/s):         " +
GHz24[(int)bssidd.chCenterFrequency / 1000] + "\n" + "         Інші частоти (MBit/s):      " +
getAllRatesFromBssid(bssidd.wlanRateSet) + "\n";
                            x++;
                            result += tempStringTwo;
                        }
                    }
                    i++;
                }
            }
            return result;
        }
        public string GetInformationTwo()
        {
            string result = "";
            try
            {
                foreach (WlanClient.WlanInterface wlanIface in client.Interfaces)
                {
                    Wlan.WlanBssEntry[] wlanBssEntries = wlanIface.GetNetworkBssList();
                    foreach (Wlan.WlanBssEntry network1 in wlanBssEntries)
```

```
                    {
                        int rss = network1.rssi;
                        //     MessageBox.Show(rss.ToString());
                        byte[] macAddr = network1.dot11Bssid;
                        string tMac = "";
                        for (int i = 0; i < macAddr.Length; i++)
                        {
                            tMac += macAddr[i].ToString("x2").PadLeft(2, '0').ToUpper();
                        }
                        string tempString = "Found network with SSID " +
System.Text.ASCIIEncoding.ASCII.GetString(network1.dot11Ssid.SSID).ToString() + " .\n"
                            + "Signal: " + network1.linkQuality + "%.\n" + "BSS Type: " +
network1.dot11BssType + ".\n" + "MAC: " + tMac + ".\n" + "RSSID:" + rss.ToString() + "\n\n";
                        result += tempString;
                    }
                }
            }
            catch (Exception ex)
            {
                MessageBox.Show(ex.Message);
            }
            return result;
        }
        private static string getAllRatesFromBssid(WlanRateSet wlanRateSet)
        {
            string ret = "";
            for (int x = 0; x < 100; x++)
            {
                if (wlanRateSet.GetRateInMbps(x) != 0)
                {
                    ret += wlanRateSet.GetRateInMbps(x) + " ";
                }
            }
            return ret.Remove(ret.Length - 1);
        }
        private static string ConvertDecimalArrayToHexString(byte[] ar)
        {
            String ret = "";
            foreach (byte b in ar)
            {
                ret += b.ToString("X");
                ret += ":";
            }
            return ret.Remove(ret.Length - 1);
        }
    }
}
```

Monitor.cs

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Runtime.InteropServices;
using System.Security.Principal;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
namespace ProjectOne
{
    class Monitor
    {
        private DateTime startDateTime;
```

```
        TimeSpan time;
        bool checkTime = false;
        public event Test newTest;
        public delegate void Test();
        private const int SECURITY_BUILTIN_DOMAIN_RID = 0x20;
        private const int DOMAIN_ALIAS_RID_ADMINS = 0x220;
        private const int IOC_VENDOR = 0x18000000;
        private const int IOC_IN = -2147483648;
        private const int SIO_RCVALL = IOC_IN | IOC_VENDOR | 1;
        private const int BUF_SIZE = 1024 * 1024;
        private Socket monitor_Socket;
        private IPAddress ipAddress;
        private byte[] buffer;
        public Monitor(IPAddress ip)
        {
            this.ipAddress = ip;
            this.buffer = new byte[BUF_SIZE];
        }
        ~Monitor()
        {
            stop();
        }
        public void start()
        {
            start(TimeSpan.Zero);
        }
        public void start(TimeSpan time)
        {
            if (monitor_Socket == null)
            {
                try
                {
                    if (ipAddress.AddressFamily == AddressFamily.InterNetwork)
                    {
                        monitor_Socket = new Socket(AddressFamily.InterNetwork, SocketType.Raw,
System.Net.Sockets.ProtocolType.IP);
                    }
                    else
                    {
                        monitor_Socket = new Socket(AddressFamily.InterNetworkV6, SocketType.Raw,
System.Net.Sockets.ProtocolType.IP);
                    }
                    monitor_Socket.Bind(new IPEndPoint(ipAddress, 0));
                    monitor_Socket.IOControl(SIO_RCVALL, BitConverter.GetBytes((int)1), null);
                    monitor_Socket.BeginReceive(buffer, 0, buffer.Length, SocketFlags.None, new
AsyncCallback(this.OnReceive), null);
                }
                catch (Exception e)
                {
                    MessageBox.Show("Close2");
                    monitor_Socket.Close();
                    monitor_Socket = null;
                    MessageBox.Show(e.ToString());
                }
            }
        }
        public void stop()
        {
            if (monitor_Socket != null)
            {
                monitor_Socket.Close();
                monitor_Socket = null;
            }
        }
```

```
        private void OnReceive(IAsyncResult ar)
        {
            if(newTest != null)
            {
                newTest.Invoke();
            }
            if(true)
            {
                try
                {
                    int len = 0;
                    if (monitor_Socket != null)
                    {
                        len = monitor_Socket.EndReceive(ar);
                        byte[] receivedBuffer = new byte[len];
                        Array.Copy(buffer, 0, receivedBuffer, 0, len);
                        try
                        {
                            Packet packet = new Packet(receivedBuffer);
                            GlobalVars.packets.Add(packet);
                        }
                        catch (ArgumentNullException ane)
                        {
                            MessageBox.Show(ane.ToString());
                        }
                        catch (ArgumentException ae)
                        {
                            MessageBox.Show(ae.ToString());
                        }
                        monitor_Socket.BeginReceive(buffer, 0, buffer.Length, SocketFlags.None,
new AsyncCallback(this.OnReceive), null);
                    }
                }
                catch (Exception e)
                {
                    stop();
                }
            }
            else
            {
                string result = "";
                foreach(Packet p in GlobalVars.packets)
                {
                    result = result + "SRC IP: " + p.Src_IP.ToString() + "\nDES IP: " +
p.Src_PORT.ToString() + "\nProtocol Type: " + p.Type.ToString();
                }
                MessageBox.Show(result);
            }
        }
        protected void OnNewPacket(Packet p)
        {
            if (newPacketEventHandler != null)
            {
                newPacketEventHandler(this, p);
            }
        }
        public event NewPacketEventHandler newPacketEventHandler;
        public delegate void NewPacketEventHandler(Monitor monitor, Packet p);
        /// <summary>
        /// </summary>
        /// <returns></returns>
        private bool IsUserAnAdmin()
        {
            WindowsIdentity identity = WindowsIdentity.GetCurrent();
```

```
            WindowsPrincipal principal = new WindowsPrincipal(identity);
            return principal.IsInRole(WindowsBuiltInRole.Administrator);
        }
        [DllImport("advapi32.dll")]
        private extern static int AllocateAndInitializeSid(byte[] pIdentifierAuthority, byte
nSubAuthorityCount, int dwSubAuthority0, int dwSubAuthority1, int dwSubAuthority2, int
dwSubAuthority3, int dwSubAuthority4, int dwSubAuthority5, int dwSubAuthority6, int
dwSubAuthority7, out IntPtr pSid);
        [DllImport("advapi32.dll")]
        private extern static int CheckTokenMembership(IntPtr TokenHandle, IntPtr SidToCheck, ref
int IsMember);
        [DllImport("advapi32.dll")]
        private extern static IntPtr FreeSid(IntPtr pSid);
    }
}
```