МІНІСТЕРСТВО ОСВІТИ І НАУКИ СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфкаційної роботи бакалавра

«ЗАХИСТ МЕРЕЖ БЕЗДРОТОВОГО ДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ WI-FI З ПРОТОКОЛОМ WPA2-ENTERPRISE»

Завідуючий кафедрою
Електроніки та комп’ютерної техніки А.С Опанасюк
Керівник роботи Т.О Протасова
Студент групи ТК-81 Б.О Пустовіт

СУМИ
2022

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет _____ЕлІТ _____ Кафедра електроніки та комп′ютерної техніки
Спеціальність Телекомунікації та радіотехніка

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ

Пустовіт Богдан Олегович

1 Тема роботи Захист мереж бездротового доступу на базі технології WI-FI з протоколом WPA2-Enterprise затверджено наказом ЗВО від « 12 » квітня 2022 р. № 0241-VI

2 Термін подання студентом закінченої роботи 10.06.2022

3 Вихідні дані проекту: Мережа безпровідної передачі інформації Wi-Fi, технології IEEE 802.11, протоколи мережі WEP,WPA,WPA2,WPA2-Enterprise, WPA3, технології Wi-Fi, атаки типу: підроблена точка доступу, несанкціоновані точки доступу, атака KRACK.

4 Зміст розрахунково-пояснювальної записки: 1)Проаналізувати стандарти мереж бездротового доступу Wi-Fi. Розглянути принципи роботи Wi-Fi мережі. 2) Проаналізувати можливі типи загроз і протоколи інформаційної безпеки, що борються з ними в мережах Wi-Fi. 3)Провести аналіз на вразливість протоколу інформаційної безпеки WPA2- Enterprise та надання рекомендацій з питання розвитку рівня безпеки Wi-Fi.

5 Перелік графічного матеріалу: мережа wi-fi та її режими роботи; стандарти сімейства ieee 802.11; режими доступу до мережі; основні протоколи безпеки wi-fi; протокол безпеки wep; протокол безпеки wpa; протокол безпеки wpa2; захист корпоративних мереж з протоколом wpa2-enterprise;

Керівник Протасова Т.О.

(підпис) (прізвище, ім’я, по бітькові)

Завдання прийняв до виконання Пустовіт Б.О

Календарний план

№ п/пс	Найменування етапів дипломного проекту(роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Отримання індивідуального завдання. Збір інформації, що відповідає отриманому завданню.	31.01.2022	
2	Вивчення принципів роботи безпровідних мереж передачі інформації. Розгляд безпровідної локальної мережі.	15.02.2022	
3	Вивчення стандартів безпровідної мережі Wi-Fi. Розгляд режимів доступу до мережі	20.03.2022	
4	Розгляд вразливостей мереж безпровідного доступу. Детальний аналіз протоколів безпеки.	01.04.2022	
5	Аналіз вразливостей та методу забезпечення безпеки в корпоративних мережах.	15.05.2022	
6	Надання рекомендацій для подальшого підвищення рівня безпеки корпоративних мереж	05.06.2022	

Студент _____

(підпис)

Керівник_____

(підпис)

“_____”_____2022__ р

РЕФЕРАТ

Дипломна робота містить: 57 сторінки, 15 рисунків, 5 таблиць та 18 джерел.

Мета роботи - підвищення захищеності та надійності мереж безпровідного доступу.

В даній роботі розглянуто основні безпровідні мережі передачі інформації. Детальніше розглянуто безпровідні локальні мережі та принципи її роботи. Було проаналізовано типи атак на ці мережі, та розглянуто методи боротьби з ними. Був розглянутий варіант атак на корпоративні мережі та було запропоновано деякі рекомендації для уникнення атак і забезпечення цілісності персональних даних в майбутньому.

Ключові слова: Wi-Fi, WPA2 Enterprise, безпровідні локальні мережі, автентифікація, захист, протокол, стандарт, WEP,WPA,WPA2,

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

Wi-Fi – Wireless Fidelity DCF (Discounted cash flow) – Розподілений режим доступу

PCF (Point coordination function) – централізований метод доступу

DSSS (Direct Sequence Spread Spectrum) – широкополосна модуляція з прямим розширенням спектра

FHSS (Frequency Hopping Spread Spectrum) – Псевдовипадкова перестройка робочої частоти

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – Багатостанційний доступ з контролем несучої і запобіганням конфліктів

P2P - мережа Peer-to-Peer MAC (Medium Access Control) – Управління доступом до середи

MIMO – Multiple Input Multiple Output WLAN (Wireless Local Area Network) – бездротова локальна мережа

SSID (Service Set Identifier) – ідентифікатор бездротової мережі

WEP – Wired Equivalent Privacy WPA (WiFi Protected Access)

WPA2 (WiFi Protected Access 2) WPA3 (WiFi Protected Access 3)

IEEE - Institute of Electrical and Electronics Engineers

TKIP – Temporal Key Integrity Protocol

AES - Advanced Encryption Standard

SAE - Simultaneous Authentication of Equals

KRACK - Key Reinstallation Attack БМПІ – безпровідні мережі передачі інформації

ТД – точка доступу

ВСТУП

Злагоджена робота всіх пристроїв забезпечується за допомогою безпровідних мереж на базі стандарту IEEE 802.11, або як вони називаються в народі – Wi-Fi. Вона використовується для розгортання мереж як і в публічних місцях, так і для організації безпровідних локальних комп'ютерних мереж. Обмін, передача, скачування важливих для нас елементів проходить саме завдяки цим мережам, тому питання їх захищеності повинно бути на першому місці.

Метою даної роботи є підвищення захищеності та надійності мереж безпровідного доступу за рахунок аналізу методів забезпечення безпеки, а також аналізу вразливостей і їх вирішення.

Об'єктом дослідження є безпровідні локальні мережі, а предметом дослідження – методи забезпечення безпеки в мережах безпровідного доступу.

ПРИНЦИПИ ФУНКЦІОНУВАННЯ МЕРЕЖ БЕЗПРОВІДНОГО ДОСТУПУ СТАНДАРТІВ IEEE 802.11

За останні декілька років прогрес поширення безпровідних мереж Wi-Fi набирає великих обсягів, тому в розробників виникає думка про винайдення, виготовлення і впровадження нових стандартів зв’язку, які на відміну від своїх попередників будуть більш продуктивнішими, ефективнішими і захищеними. На початку свого існування безпровідні пристрої могли підтримувати швидкість передач даних понад 1-2 Мбіт/с, яка у порівнянні з теперішньою швидкістю являється мізерною. В сучасному світі швидкість передачі інформації у безпровідних мережах може досягати до 1Гбіт/с, що не може не створювати конкуренцію для кабельних мереж. Є дуже багато видів безпровідних мереж, кожна з яких відрізняється від своїх попередників різними параметрами – швидкістю передачі, радіусом дії і типом кодування інформації.

1.1 Класифікація безпровіднихмереж передачі інформації

В телекомунікації стрімкого розвитку набирають безпровідні мережі передачі інформації (БМПІ). Ринок має великий асортимент обладнання безпровідного доступу, а саме обладнання для побудови безпровідних мереж WiFi, GSM, WiMAX і глобальних мереж. Відомо три основні види використання таких мереж:

- Робота в замкнутому просторі (офіс, концертні зали і т. д.);
- З'єднання віддалених локальних мереж;
- Побудова територіально розподілених безпровідних мереж;

Для з'єднання мереж на великих відстанях, або великих самих по собі мереж можуть бути використанні обладнання з спрямованими антенами або підсилювачі і розміщення антен на великій висоті.

Якщо більш детальніше розглядати безпровідні мережі передачі інформації, то можна явно виділити чотири типи:

1. Безпровідні персональні мережі (WPAN - wireless personal area network) – мережа, радіус дії якої може сягати від декількох сантиметрів і до 10-15 м. Призначені для з’єднання обладнання в межах робочого місця, наприклад, зв'язку стільникового телефону і ноутбука або комп'ютера і принтера. Найбільш поширена технологія з цієї категорії - Bluetooth.

2. Безпровідні локальні мережі (WLAN - wireless local area network) – радіус дії до 100 метрів, але при розгортанні підсилювачів і напрямлених антен дальність дії зростає до понад декількох сотень метрів. Їх також називають WiFi мережами. Основне призначення таких систем - розгортання безпровідних мереж усередині приміщень, хоча є випадки їх використання на відкритих майданчиках. Базова послуга - доступ в Internet або корпоративну мережу.

3. Безпровідні міські мережі (WMAN - Wireless Metropolitan Area Network) - радіус дії базової станції - до 10 км. За допомогою обладнання, що належить до класу фіксованого широкосмугового безпровідного доступу (Fixed Broadband 13 Wireless Access, FBWA) виконується побудова розподілених безпровідних операторських мереж масштабу міста або великих корпоративних мереж.

4. Безпровідні глобальні мережі WWAN. Глобальні бездротові мережі передачі інформації представлені в основному супутниковими системами зв'язку. Щоб краще розгледіти потенціал і функціональну спроможність вище згаданих видів безпровідних мереж передачі інформації наведено таблицю, в якій описуються основні характеристики такі як, швидкість передачі даних в кожній технології і дальність зв'язку (Таблиця 1.1.).

Таблиця 1.1. Характеристики технологій БМПІ.

WPAN		
IEEE 802.15.1 (Bluetooth),	64 Кб/с-1 Мб/с	10-100 м
Home RF	1(2) Мб/с – 10(20) Мб/с	До 50 м
IEEE 802.15.3	11, 22, 33, 44, 55 Мб/с	До 10 м
IEEE 802.15.4 (ZigBee),	20, 40, 250 Кб/с	До 10 м
IEEE 802.15.3a (UWB)	100 Мб/с – 1,3 Гб/с	5-10 м
WLAN		
IEEE 802.11	1-2 Мб/с	300 м
IEEE 802.11a	6, 12, 24 (9, 18, 36, 48, 54) Мб/с	100 м
IEEE 802.11b	2, 5 – 11 Мб/с (до 33 Мб/с)	100 м
IEEE 802.11g	11 – 54 Мб/с	100 м
IEEE 802.11n	Понад 160 Мб/с	100 м
IEEE 802.11ac	Понад 1 Гбіт/с	100 м

DECT	70 Кб/с	30-70 м (в приміщені), 100- 400 м (ззовні)
WMAN		
IEEE 802.11.16 2004 (WiMAX)	30-40 Мб/с (до 70Мб/с)	2,5-5 км (рухомі абоненти (до 15км/ч)) 40-50 км (Стаціонарні абоненти)
IEEE 802.11.16e (WiMAX)	До 15 Мб/с	2-7 км
IEEE802.11.16f(h) (WiMAX)– перспективні	До 10 Тб/с	Підтримка мобілності (до 300 км/ч)
WWAN		
IEEE 802.20 (WiMAX)	Понад 1 Мб/с	Підтримка мобільності і мобільної структури
GSM	9,6 Кб/с	Сота до 35 км
CDMA	14,4 Кб/с	Сота до 20 км
IMT-2000	2 Мб/с (для малорухомих абонентів) 384 Кб/с (для рухомих абонентів)	Сота 20-40 км

Хоч всі мережі безпровідного доступу мають широке застосування в теперішньому світі, найбільшого поширення має технологія Wi-Fi. Її функціоналом користуються як і проводові мережі, так і безпровідні. В основному забезпечується покриття території і заохочення нових користувачів в свою мережу.

1.2 Wi-Fi - безпровідна локальна мережа

Безпровідні локальні мережі, більш відомі під іменем Wireless Fidelity (WiFi), створенні на основі сімейства стандартів IEEE 802.11. На перших етапах свого існування термін «Wi-Fi» застосовували тільки щоб позначати технології, які забезпечують зв’язок в діапазоні частот понад 2.4ГГц, але в теперішньому часі його використовують для безпровідних мереж і інших технологій. Мережа Wi-Fi застосовується для зв’язку і обміну даними між вузлами, однак це гнучка система обміну інформацією, що працює подібно до альтернативної провідної мережі, яка знаходиться в приміщенні чи на певній відкритій території. Також ця

мережа використовується для організації публічних точок доступу , таких як аеропорти, площі та інші багатолюдні місця і організація тимчасових безпровідних мереж на період проведення фестивалів, футбольних матчів чи виставок в музеях.

1.2.1. Формування сімейства безпровідних мереж

В 1990 році IEEE 802 створив групу для роботи по стандартам для безпровідних мереж Wi-Fi. Основним їх завданням було створення загального стандарту для мереж, які працюють в частотному діапазоні 2.4 ГГц з швидкістю з'єднання 1-2 Мбіт/с. В 1997 році розробка стандарту була завершеною і була ратифікована перша специфікація 802.11.

Цей стандарт вважався першим для пристроїв WLAN. Однак тоді початкова швидкість передачі інформації не відповідала бажанням користувачів. Саме тому, для того щоб задовільнити всіх користувачів і зробити цю технологію популярною, розробники створили новий стандарт. І вже осінню 1999 року було схвалено удосконалення вже існуючого стандарту. Новий стандарт називався 802.11 High rate або скорочено IEEE 802.11b. За допомогою цього стандарту пристрої безпровідних мереж могли передавати і отримувати дані на швидкості понад 11 Мбіт/с. Ця швидкість дозволила використовувати пристрої в великих корпоративних організаціях.

1.2.2 Режими роботи стандарту IEEE 802.11 є популярним і використовується в різних галузях, тому для більшої ефективності мережі використовуються певні мережеві топології, які в тій чи іншій ситуації будуть найбільш підходящими. Стандарт IEEE 802.11 має декілька мережевих топологій:

- Режим інфраструктури;
- Режим Ad Hoc;
- Топологія бездротової сітки;

- Режим інфраструктури

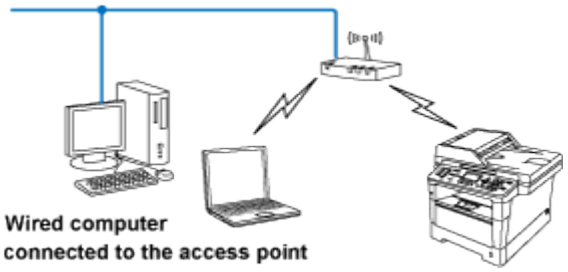

Рисунок 1.1 - Режим інфраструктури

Область, яка позначена пунктирним лінією замкнуту в коло , називається базовим набором послуг (BSS). Всі станції, що підключені до точки доступу, утворюють базовий сервісний набір. Також існує ще базова зона обслуговування (BSA). Основна зона обслуговування - це зона, яка охоплена точкою доступу. Сигнал точки доступуможе виходити замежі діапазону підключених до нього пристроїв. Ця зона покриття – являється BSA.

Режим Ad Hoc являється самодостатньою мережею Peer-to-Peer. Тобто, це мережа без точки доступу, в якій пристрої не тільки являються кінцевими точками, а й маршрутизаторами. Це показано нижче:

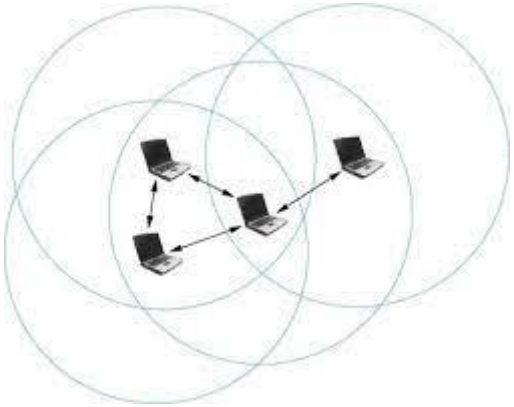

Рисунок 1.2 - Режим Ad Hoc.

- Топологія безпровідної сітки

Мережа Wireless Mesh - це взаємозв'язок підключених вузлів, які утворюють самостійну мережу. Якщо один вузолмережі «падає», то формується новий

шлях для створення мережі, що працює. Сітчасті вузли використовують стандарти 802.11, щоб спілкуватись один з одним. Резервний сітчастий вузол також може бути налаштований для підключення до загальнодоступного шлюзу, якщо первинний сітчастий вузол опуститься.До будь-якого мережевого вузла можуть бути підключені користувачі. Навантаження на мережевий трафік потрібно збалансувати між різними вузлами та створити ефективні механізми маршрутизації, щоб забезпечити найшвидший шлях до загальнодоступної мережі.

1.3 Огляд вже існуючих стандартів сімейства IEEE 802.11

І сьогодні існує велика кількість стандартів групи IEEE 802.11. Розглянемо найбільш розповсюдженні і найбільш вживані:

1. базовий 802.11;
2. 802.11a; 20
3. 802.11b;
4. 802.11g;
5. 802.11n.
6. 802.11p;
7. Mesh-мережі 802.11s;

Всі стандарти IEEE 802.11 працюють на нижніх двох рівнях моделі ISO / OSI, фізично і канальному, тому будь-який мережевий додаток, мережева операційна система, або протокол (наприклад, TCP / IP), будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet .

1.3.1. Базовий стандарт IEEE 802.11 В середині літа 1997 року був оприлюднений стандарт IEEE 802.11 який мав назву «Специфікація фізичного рівня і рівня контролю доступу до каналу передачі бездротових локальних мереж». Цей протокол ідентифікував архітектуру мережі, формати пакетів, способи захисту даних та автентифікацію, а також різні принципи доступу пристроїв до каналів зв’язку.

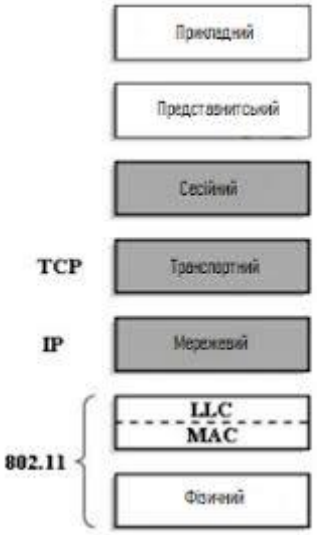

Рисунок 1.3 - Рівні моделі ISO / OSI і їх відповідність стандарту 802.11

В початковому етапі свого існування стандарт 802.11 працював з обладнанням на частоті 2.4ГГц і максимальною швидкістю до 2 Мбіт/сек. Базовий протокол 802.11 на своєму фізичному рівні реалізує 2 методи передачі даних:

- Метод частотних стрибків FHSS (Frequency Hopping Spread Spectrum);
- Метод прямої послідовності DSSS (Direct Sequence Spread Spectrum);

FHSS – Це технологія передачі в якій сигнал даних модулюється за допомогою вузькосмугового сигналу-носія, що «перескакує» у випадковій, але передбачуваній послідовності від частоти до частоти. Сигнал поширюється у часовій області. Ця технологія забезпечує менший рівень перешкод, адже сигнал з вузькосмугової системи буде мати вплив на сигнал розповсюдженого спектру лише в тому випадку, коли обидва сигнали мають однакову частоту. Енергія сигналу поширюється у часовій області, а не подрібнюючи кожен біт невеликими шматочками в частотній області. Ця методика зменшує перешкоди, оскільки сигнал із вузькосмугової системи впливатиме на сигнал розповсюдженого спектру лише тоді, коли обидва передають однакову частоту. При правильній синхронізації підтримується єдиний логічний канал. Частоти на яких буде відбуватись передача обирається кодом, що розповсюджується чи «стрибає». Саме на цей код має бути налаштований приймач і повинен слухати вхідний сигнал у потрібний час та правильну частоту, щоб правильно приймати сигнал. (DSSS) - це техніка поширення спектру, за допомогою якої вихідний сигнал даних множиться на псевдо-випадковий код розповсюдження шуму. Цей розповсюджую-

чий код має більш високу швидкість чіпа (це бітрейт коду). DSSS значно покращує захист від непотрібних (або 22 заклинюючих) сигналів, особливо вузькосмугових і робить сигнал менш помітним .

FHSS схожий до методу перескоку частоти, але в мережах GSM і EDGE. Пристрої цього методу працюють в частотному діапазоні від 2.402 до 2.480 ГГц і ділять його на 79 рівних неперервних каналів, шириною 1МГц. DSSS в багатьох аспектах нагадує метод в системі кодового розділення CDMA. Ці дві технології забезпечують в мережі максимально можливу для них, але мізерну по теперішнім міркам, швидкість понад 2Мбіт/с.

1.3.2 Стандарт 802.11a був впроваджений в 1999 році. Основним завданням цього протоколу є робота в частотному діапазоні понад 5ГГц з максимальною швидкістю передачі 54Мбіт/с. Стандарт має технологію побудови радіоканалу на основі мультиплексування з ортогональним поділом частот (OFDM). Тобто, передача даних виконується за допомогою ряду незалежних радіосигналів. Такий метод призводить до зниження швидкості передачі на кожній «несучій», що безпосередньо забезпечує захист від завад зв'язку при досягненні високої пропускної здатності. Несучі модулюють за допомогою BPSK, QPSK, 16- і 64- 23 позиційної квадратурної амплітудної модуляції (QAM). Стандарт має 8 швидкостей передачі, 3 з яких є обов'язковими, а інші додатковими. В таблиці 2 наведено всі види швидкостей:

Таблиця 1.2 - Швидкість передачі для різних видів модуляції стандарту 802.11a

Модуляція	Швидкість кодування	Швидкість передачі Мбіт/с
BPSK(Обов'язкова)	1/2	6
BPSK(Додаткова)	3/4	9
QPSK(Обов'язкова)	1/2	12
QPSK(Додаткова)	3/4	18
QAM-16(Обов'язкова)	1/2	24
QAM-16(Додаткова)	3/4	36
QAM-64(Додаткова)	2/3	48
QAM-64(Додаткова)	3/4	54

Стандарт 802.11a розбитий на 3 піддіапазони, які відрізняються між собою обмеженнями по максимальній потужності випромінювання:

- Нижній діапазон (5170 – 5330МГц) – потужність передачі до 100мВт;
- Середній діапазон (5470–5730МГц)– потужність передачі до 250мВт;
- Верхній діапазон (5715 – 5835МГц) – потужність передачі до 1Вт; Недоліками цього стандарту є висока споживча потужність і менший радіус дії обладнання. Порівняно з обладнанням, які працюють на частоті 2.4ГГц, радіус дії менший приблизно в три рази.

1.3.3 Стандарт 802.11b був представлений в після вдосконалення раніше прийнятого стандарту IEEE 802.11. Цей стандарт має максимальну швидкість передачі інформації понад 11Мбіт/с, однак за рахунок втрат протоколу CSMA / CA в дійсності швидкість передачі через TCP – 5.9Мбіт/с, а через UDP – 7.1Мбіт/с. Стандарт IEEE 802.11b працює в частотному діапазоні 2.4ГГц з широкосмуговим каналом 83.5МГц. Діапазон розбитий на 14 каналів, з інтервалом в 5МГц, окрім останнього в якого 10МГц.

Однак одного каналу шириною в 5 МГц виявляється недостатньо, тому для передачі інформації використовується смуга частот шириною в 22МГц. Тобто об'єднуються декілька сусідніх каналів, щоб забезпечити безперешкодну передачу даних. За допомогою стандарту IEEE 802.11b на певній території можуть одночасно працювати декілька незалежних різних безпроводнихмереж, через визначену комітетом спектральну маску. Вона ідентифікує спектр потужності передавача, який працює в одному з каналів.

1.3.4 Стандарт 802.11g є удосконаленням стандарту IEEE 802.11b. Завдяки застосування ефективніших технологій модуляції сигналу було підвищено швидкість передачі інформації до 54Мбіт/с. У таблиці 3 наведено швидкості передачі даних з різними модуляціями для стандарту IEEE 802.11g.

Табл.1.3 Швидкість передачі даних в стандарті IEEE 802.11g.

Стандарт передачі	Швидкість передачі	Вид модуляції
IEEE 802.11g (обов'язковий)	5,5/11 Мбіт/с	CCK
IEEE 802.11g (обов'язковий)	до 54 Мбіт/с	OFDM

IEEE 802.11g (опціональний)	до 33 Мбіт/с	PBCC
IEEE 802.11g (опціональний)	до 54 Мбіт/с	CCK-OFDM

Провівши аналіз чутливості системи стандарту 802.11g можна дійти до висновку, що системи стандарту IEEE 802.11g масштабуються вниз до відповідної межі, тому в перехідному діапазоні швидкість передачі змінюється плавно. (Рисунок 1.4)

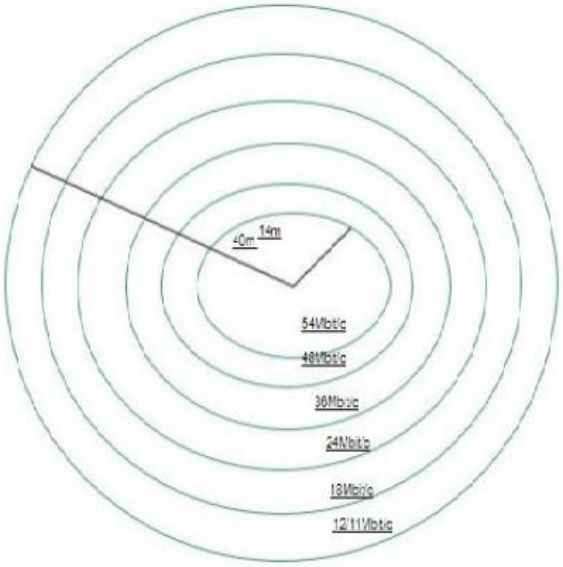

Рисунок 1.4 Радіус дії в частотному діапазоні 2,4 ГГц (802.11g) при модуляції OFDM

На рисунку 1.10 цей перехід представлений схематично. Швидкість передачі в 54 Мбіт/с досягається у відкритій офісному середовищі лише на відстані до 14 м. При наявності будь-якої завади, яка має бути подоланою, швидкість передачі зменшується.

1.3.5 802.11n включає в себе безліч удосконалень у порівнянні з пристроями стандарту 802.11g. Удосконалення дозволяє працювати на одному із діапазонів 2.4ГГц або 5ГГц. Була додана можливість одночасної передачі сигналу за допомогою чотирьох передаючих пристроїв, удосконалено модуляцію і обробку сигналу на фізичному рівні(PHY).І канальний рівень не залишився в стороні, в ньому було реалізовано більш ефективне застосування допустимої

пропускної здатності. В сукупності ці удосконалення могли забезпечувати максимальну швидкість передачі даних приблизно в 10 разів більшу ніж в своїх попередників, приблизно до 600Мбіт/с. Основними покращеннями були:

1. Створення багатоканального входу/виходу(MIMO);
2. Збільшення ширини смуги пропускання від 20МГц до 40МГц;

-Багатоканальний вхід / вихід (MIMO)

Стандарт 802.11n запровадив в мережу MIMO. Розшифровується воно як Multi-Input і Multiple-output. У 80-х та на початку 90-х років було проведено значні дослідження у галузі багатоканальної техніки передачі з метою використання багатоканального розповсюдження для передачі декількох потоків інформації через декілька антен одночасно. (Рисунок 1.4)

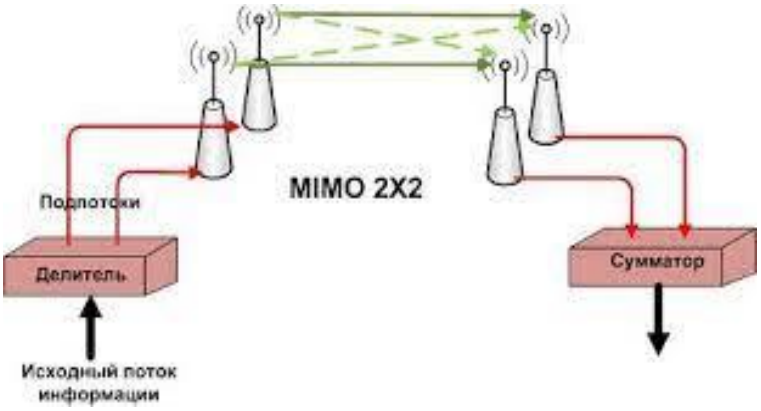

Рисунок 1.5 - Найпростіша система MIMO 2x2

В її основі лежала концепція багато шляхового поширення. Тобто кожен сигнал, який передається від антени, стикається і відскакує від непрозорих твердих предметів на шляху до приймача. Отриманий сигнал буде сумішшю переданого сигналу, що надходить на різні проміжки часу, а також під різними кутами прибуття. Теорія полягала в тому, що якщо кілька потоків були налаштовані таким чином, що передані ними сигнали були достатньо відокремленими, так що кожен з прийнятих сигналів може бути незалежно декодований на приймачі - це призвело б до збільшення пропускної здатності системи.

Кількість антен під час одночасної роботи прямо пропорційно відноситься величині максимальної швидкості передачі даних. Чим більше антен – тим

більша швидкість передачі. Але нарахування тільки великої кількості антен не збільшує максимальну швидкість передачі і розширення діапазону, це буде працювати тільки з пристроями які підтримують стандарт IEEE 802.11n. Саме в цих пристроях застосовується метод обробки сигналу, який визначає алгоритм роботи MIMO – пристроїв при застосуванні певної кількості антен.

- Ширина смуги пропускання каналу 40 МГц

Другим удосконаленням стандарту являється збільшення ширини каналу з 20МГц до 40МГц. В таблиці 4 наведено швидкості передачі і швидкості кодування видів модуляції для каналів зі смугами в 20МГц і 40МГц. Таблиця 1.4

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	65.00	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	14.40	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
...	...	...	...	...	...	...	...
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Пристрої стандарту 802.11n можуть використовувати будь-яку ширину каналу 20 або 40 МГц в будь-якому частотному діапазоні (2.4 або 5 ГГц). При використанні 29 ширини каналу 40 МГц відбувається подвоєння пропускної здатності в порівнянні з шириною каналу 20 МГц.

1.3.6. Mesh-мережі 802.11s

Стандарт IEEE 802.11s являється стандартом безпровідної мережі, який був створений для організації комірчастих мереж, або ж відомих під іншою

назвою мереж - mesh-мереж WMN (Wireless mesh network). Вони характеризуються надійністю і масштабованістю, а також мають властивості само конфігурування, відновлення і організації побудови мережі(Рисунок 1.12.).

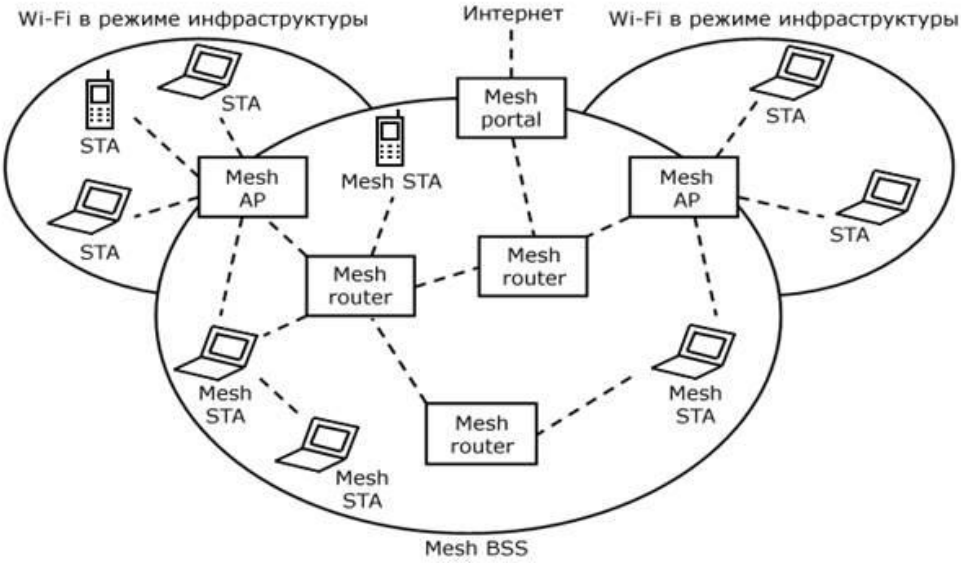

Рисунок 1.6 - Архітектура mesh-мережі 802.11s

WMN гарантує працездатність мережі при виходу з ладу певних елементів, розширення покриття мережі, рухому маршрутизацію трафіку, а також ретрансляцію кадрів між пристроями без прямої видимості. Всі нововведення введені тільки на MAC-рівні. Мережа стандарту визначена для невеликих розмірів з максимальною кількістю вузлів до 64.

1.4 Механізм доступу до середовища

Щоб створити всі умови для спільної роботи в мережі з великою кількістю пристроїв користувача без взаємних перешкод, було вирішено змінити стандартом спеціальний механізм їх переходу на режим передачі з попереднім повідомленням про передачу даних – множинний доступ з контролем несучої і 32 запобіганням колізій(Carrier Sense Multiple Access with Collision Avoidance, CSMA / CA). CSMA розшифровується як множинний доступ з контролем несучої. Усі пристрої безпровідноїмережі розпізнають, чи знаходиться мережа в режимі очікування. Тільки якщо середовище сприймається як недіюче, пристрій станції 802.11 може передавати кадр. CA в CSMA / CA означає запобігання зіткнення.

Пристрій WLAN не може одночасно передавати та приймати. Якщо середовище розпізнається як зайняте, то пристрій WLAN буде відключатись протягом деякого проміжку часу. Був розроблений алгоритм спеціального відключення, який визначає цей проміжок часу. Також до часу відключення, всі станції 802.11 ще використовують інший віртуальний механізм відключення, який називають векторним розподілом мережі (NAV). NAV – це тривалість часу. Ця тривалість отримується станцією 802.11 в останньому пакеті, який був виявлено станцією в ефірі. Тільки якщо тривалість NAV та таймер відключення відлічуються до нуля, а середовище можна вважати незайманим і може відбутись передача пакету в ефірі.

1.4.1 Фізичний рівень (Physical layer) стандарту IEEE 802.11 використовує пакетні передачі чи пакети. Кожен з цих пакетів складається з парамбули, заголовку і даними корисного навантаження.

Парамбула дозволяє приймачу отримати синхронізації часу і частоти і оцінити характеристики каналу для вирівнювання. Заголовок надає інформацію про конфігурацію пакета, таку як формат, швидкість передачі даних і т. д. На фізичному рівні стандарт 802.11 охоплює дві альтернативи DSSS і FHSS. Обидва різновиди передачі по радіо з використанням розширення спектра методом прямої послідовності (DS) і методом частотних стрибків (FH) використовують частотний діапазон 2,400 -2,4835 ГГц . Смуга пропускання 2,4 ГГц була обрана тому, що в усьому світі цей діапазон виділений для неліцензованого використання, а також в даному діапазоні можливе створення і виробництво приймально-передавального радіообладнання, що володіє низькою вартістю, невеликим випромінюванням потужності і праці на швидкостях, близьких до швидкостей в звичайних дротових Ethernet мережах.

1.4.2. MAC-рівень стандарту IEEE 802.11 відповідає за розподіл каналу, тобто обирає станцію яка буде передавати інформацію наступною. На MAC рівні обрано принцип, що визначає як пристрій буде ділити загальний канал, механізм шифрування і автентифікації даних. Оскільки стандарт 802.11 розроблявся як «бездротовий Ethernet», він передбачає пакетну передачу з 48-бітовими адресами пакетів, як і будь-яка мережа Ethernet. Рівень MAC отримує блок даних від рівня LLC і відповідає за виконання функцій, пов'язаних з доступом до середовища, і

за передачу даних. Стандарт IEEE 802.11 передбачає два режими управління мережею:

- PCF;
- DCF(розділяється ще на два підтипи);

Висновок до першого розділу:

В першому розділі була розглянута класифікація технологій безпровідних мереж передачі інформації (БМПІ). Було виявлено, що найпопулярнішою є безпровідних локальні мережах (WLAN - wireless local area network), тобто з Wi-Fi мережі, тому було розглянуто основні параметри та принципи роботи мережі, що в свою чергу привело до висновку:

Основне призначення таких систем - розгортання безпровідних мереж усередині приміщень, хоча є випадки їх використання на відкритих майданчиках. Базова послуга - доступ в Internet або корпоративну мережу.

Ще було розглянуто чотири топології мереж безпровідного доступу WiFi. А також було ознайомлено з стандартами безпровідних локальних мереж Wi-Fi, та був проведений аналіз деяких з них. Після чого виявилось, що:

Стандарт IEEE 802.11n є найбільш вживаним і найпопулярнішим. Він має безліч переваг над своїми попередниками, і саме тому застосовується для організації доступу до мережі в жилих домах та на відкритій території. Було розглянуто основний механізм та рівні доступу до мережі та класи на цих рівнях. Вивчена інформація допоможе зрозуміти основні принципи роботи цих мереж і визначити правильний підхід до подальшого розкриття теми.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ WI-FI

2.1 ВразливістіWi-Fi мереж

З кожною новою введеною технологією з’являються користувачі які бажають використовувати потенціал технології по призначенню, а ще бувають користувачі які намагаються наражати на небезпеку дані інших користувачів. Іншими словами в мережах бувають мирні користувачі і зловмисники, проти яких і застосовуються методи забезпечення безпеки. Методи забезпечення безпеки використовуються для захисту від загроз порушення інформаційної безпеки, ці загрози умовно можна розділити на два класи:

1.Прямі - загрози інформаційної безпеки, які виникають при інформаційному обміні через безпроводову мережу Wi-Fi;

2.Непрямі - загрози, пов'язані з великою кількістю точок доступу Wi-FI;

2.1.1Прямі загрози – або способи злому.

Радіоканал в межах доступності Wi-FI роутера, схильний до легкого втручання з метою отримання несанкціонованого доступу до ресурсів та інформації. У стандартах IEEE 802.11, що регламентують роботу Wi-Fi, передбачені, як автентифікація, так і шифрування, але дані елементи захисту мають свої вади і слабкі місця. На даний час відомі такі прямі атаки:

- Чужинці – це периферійні пристрої і комп'ютери, що надають можливість несанкціонованого доступу до корпоративної мережі, зазвичай в обхід захисних механізмів, визначених політикою безпеки. У ролі пристрою чужака може виступати все що завгодно, у чого є дротової і бездротової інтерфейси: роутери (включаючи програмні), проектори, сканери, ноутбуки з обома включеними інтерфейсами.

- Нефіксована природа зв'язку – безпровідні Wi-Fi пристрої можуть легко змінювати точки підключення до мережі прямо в процесі роботи і навіть непомітно для користувача. Зловмисник може перемикати на свою підставну точку доступу користувача для подальшого сканування вразливостей, фішингу або атак KRACK. А якщо для користувача пристрій при цьому підключено і до дротової локальної мережі, то він стає точкою входу, так званим чужаком.

- Уразливості мереж і пристроїв - некоректно налаштовані мережеві пристрої, пристрої зі слабкими і недостатньо довгими ключами шифрування, які використовують скомпрометовані методи автентифікації - саме ці пристрої піддаються атакам в першу чергу.

- Некоректно сконфігуровані точки доступу - варто підключити некоректно сконфігуровані точку доступу до мережі для злому останньої. Заводські настройки, так звані «за замовчуванням», зазвичай не включають шифрування і автентифікацію, або використовують ключі, прописані в інструкціях користувача, і тому вони є всім відомими навіть на офіційних форумах виробника.

- Некоректно сконфігуровані бездротові клієнти - загроза куди небезпечніше, ніж некоректне налаштування точки доступу. Це клієнтські пристрої, і вони зазвичай не конфігуруються спеціально для безпеки внутрішньої мережі підприємства. До того ж зазвичай вони знаходяться за межами периметра контрольованої зони або всередині периметра, що може дозволити зловмиснику проводити всілякі атаки, наприклад, поширювати вірусне програмне забезпечення або просто забезпечити легкодоступну і зручну точку входу.

- Імперсонації і Крадіжка особистих даних - Імперсонації (видача себе за іншу людину) авторизованого користувача - серйозна загроза для будь-якої комп'ютерної мережі, це стосується не тільки бездротової.

- Відмови в обслуговуванні - DoS атаки спрямовані на порушення якості функціонування сервісу бездротової мережі або на абсолютне припинення 41 доступу користувачів і відмова обладнання до перезавантаження. У разі Wi-Fi мережі відстежити джерело, котрий завалює мережу, специфічним для цього типу атаки, «сміттєвими» пакетами, дуже складно - його місце розташування обмежується тільки зоною покриття. До того ж є апаратний варіант цієї атаки - установка досить сильного джерела перешкод в частотному діапазоні працює точки доступу, так звані "глушилки". Очевидно, що ці загрози не були виявлені одразу після введення нового протоколу захисту. Їх наявність ставала явною тільки після деякого часу, протягом якого система працювала. На теперішній час, можна з впевненістю стверджувати, що на кожну з цих загроз є захист, але на момент впровадження нових протоколів було зовсім навпаки. Це була нова технологія, і ніхто не міг подумати, що вона може бути вразливою до якихось «Атак». Однак з часом люди зрозуміли, що захист безпровідних мереж потрібно розвивати теж, адже за цим майбутнє.

2.2 Протоколи захисту безпровіднихмереж

Існує безліч технологій безпеки, і всі вони пропонують рішення для найважливіших компонентів політики в області захисту даних: автентифікації, підтримки цілісності даних і активної перевірки. Ми визначаємо автентифікацію як автентифікацію користувача або кінцевого пристрою і його місця розташування з подальшою авторизацією користувачів і кінцевих пристроїв. Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпеку периметра і конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в області безпеки витримується на практиці, і відстежити всі аномальні випадки і спроби несанкціонованого доступу.

2.2.1 Протокол безпеки WEP

В той самий час, коли було представлено базовий стандарт IEEE 802.11, в IEEE також був затверджений механізм захисту Wired Equivalent Privacy (WEP). WEP (Wired Equivalent Privacy) – технологія стандарту 802.11, яка забезпечувала безпеку передачі інформації. Шифрування даних здійснювалося з використанням

алгоритму RC4 на ключі зі статичною складовою від 40 до 104 біт і з додатковим вектором ініціювання розміром 24 біт. Тобто в сумі шифрування даних проводилося на ключі розміром від 64 до 128 біт. У WEP не було мети повністю захистити інформацію від зловмисників, а просто зробити її недоступною для читання. Основним завданням цієї технології було шифрування потоку даних, що передавались в межах безпровідної мережі.

Для посилення захисту застосовується так званий вектор ініціалізації Initialization Vector (IV), який призначений для рандомізації додаткової частини ключа, що забезпечує різні варіації шифру для різних пакетів даних. Даний вектор є 24-бітовим. Таким чином, в результаті ми отримуємо загальне шифрування з розрядністю від 64 (40 + 24) до 128 (104 + 24) біт. Зламати подібний захист можна за допомогою утиліти (наприклад, AirSnort, WEP crack). Основне її слабке місце - це як раз-таки вектор ініціалізації. Оскільки ми говоримо про 24 біти, це має на увазі близько 16 мільйонів комбінацій (2 в 24 ступені) - після використання цієї кількості ключ починає повторюватися. Хакеру необхідно знайти ці

повтори (від 15 хвилин до години для ключа 40 біт) і за секунди зламати решту ключа. Після цього він може входити в мережу як звичайний зареєстрований ко

ристувач. Процес шифрування WEP виконується в два етапи:

1. Спочатку підраховується контрольна сума (Integrity Checksum Value - ICV) із застосуванням алгоритму Cyclic Redundancy Check (CRC-32), що 43 додається в кінець незашифрованого повідомлення і служить для перевірки його цілісності прийнятої стороною;

2. На другому етапі здійснюється безпосередньо шифрування;

Ключ для WEP-шифрування - загальний секретний ключ, який повинні знати пристрої на обох сторонах бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом з випадковим 24-бітовим IV є вхідний послідовністю для генератора псевдовипадкових чисел, що базується на шифрі Вернама для генерації рядка випадкових символів, званої ключовим потоком (key stream). Дана операція виконується з метою уникнення методів злому, заснованих на статистичних властивостях відкритого тексту. IV використовується, щоб забезпечити для кожного повідомлення свій унікальний ключовий потік.

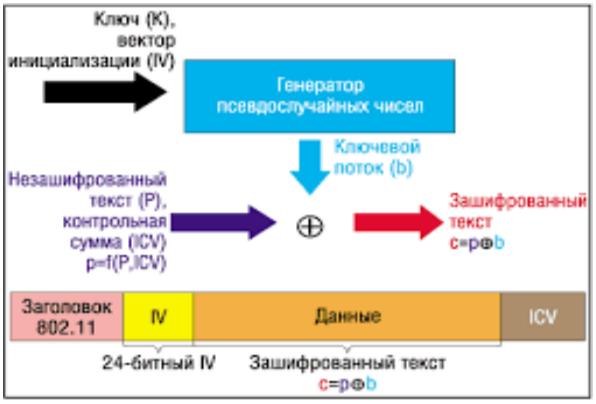

Рисунок 2.1 - Схема роботи шифрування по протоколу WEP

Зашифроване повідомлення (Рисунок 2.1.) утворюється в результаті виконання

операції XOR над незашифрованим повідомленням з ICV і ключовим потоком. Коли інформація приймається на іншій стороні, проводиться зворотний процес (p = c + b). Значення b одержувач обчислює, застосувавши код Вернама до вхідної послідовності, що складається з ключа K (який він знає заздалегідь) і

IV, який прийшов цим же повідомленням у відкритому вигляді. Для кожного чергового пакета процес повторюється з новим обраним значенням IV. До числа відомих властивостей алгоритму RC4 відноситься те, що при використанні одного і того ж значення ключа і вектори ініціалізації ми завжди будемо отримувати однакове значення b, отже, застосування операції XOR до двох текстів, зашифрованим RC4 за допомогою того ж значення b, являє собою не що інше, як операцію XOR до двох початковим текстам.

$$c1 = p1 + b \qquad c2 = p2 + b \qquad (2.1)$$

$$c1 + c2 = (p1 + b) + (p2 + b) = p1 + p2$$

Таким чином, ми можемо отримати незашифрований текст, який є результатом операції XOR між двома іншими оригінальними текстами. Процедура їх вилучення не складає великих труднощів. Наявність оригінального тексту і IV дозволяє обчислити ключ, що в подальшому дасть можливість читати всі повідомлення даної бездротової мережі. Після нескладного аналізу можна легко розрахувати, коли повториться b. Так як ключ K постійний, а кількість варіантів IV складає 224 = 16 777 216, то при достатній завантаженні точки доступу, середній розмір пакета в бездротової мережі, що дорівнює 1500 байт (12 000 біт), і середньої швидкості передачі даних, наприклад 5 Mbps (при максимальній 11 Mbps), ми отримаємо, що точкою доступу буде передаватися 416 повідомлень в секунду, або ж саме 1 497 600 повідомлень на годину, тобто повторення відбудеться через 11 год 12 хв (224/1 497 600 = 11,2 ч). Дана проблема носить назву "колізія векторів". Існує велика кількість способів, що дозволяють прискорити цей процес. Крім того, можуть застосовуватися атаки "з відомим простим текстом", коли одному з користувачів мережі надсилається повідомлення із заздалегідь відомим змістом і прослуховується зашифрований 45 трафік. В цьому випадку, маючи три складові з чотирьох (незашифрований текст, вектор ініціалізації і зашифрований текст), можна обчислити ключ.

З ICV, використовуваним в WEP-алгоритмі, справи йдуть аналогічно. Значення CRC-32 підраховується на основі поля даних повідомлення. Це хороший метод для визначення помилок, що виникають при передачі інформації, але він не забезпечує цілісність даних, т. Е. Не гарантує, що вони не були підмінені в процесі передачі. Контрольна сума CRC-32 має лінійне властивість: CRC (A XOR B) = CRC (A) XOR CRC (B), що надає зловмиснику можливість легко модифікувати зашифрований пакет без знання WEP-ключа і перерахувати для нього нове значення ICV.

- WEP Інкапсуляція

Ключ WEP і вектор ініціалізації об'єднуються для створення початкового числа WEP, яке подається в PRNG ARC4 для створення потоку ключів. Процес ство

рення для двох довжин описано нижче:

- WEP-64 - біти 0–39 ключа WEP відповідають бітам 24–63 WEP, а біти 0–23 IV відповідають бітам 0–23;

- WEP-128 - біти 0–103 ключа WEP відповідають бітам 24–127 WEP, а біти 0–23 від IV відповідають бітам 0–23; ICV (цінність перевірки цілісності) обчислюється на даних простого тексту та додається до даних прямого тексту перед шифруванням. Інкапсуляція даних проходить наступним чином (Малюнок):

1. Контрольна сума від поля «дані» обчислюється за алгоритмом CRC32 і додається в кінець кадру;

2. Дані з контрольною сумою шифруються алгоритмом RC4, які використовують в якості ключа криптоалгоритму;

3. Проводиться операція XOR над вихідним текстом і шифротекстом;

4. На початок кадру додається вектор ініціалізації і ідентифікатор ключа;

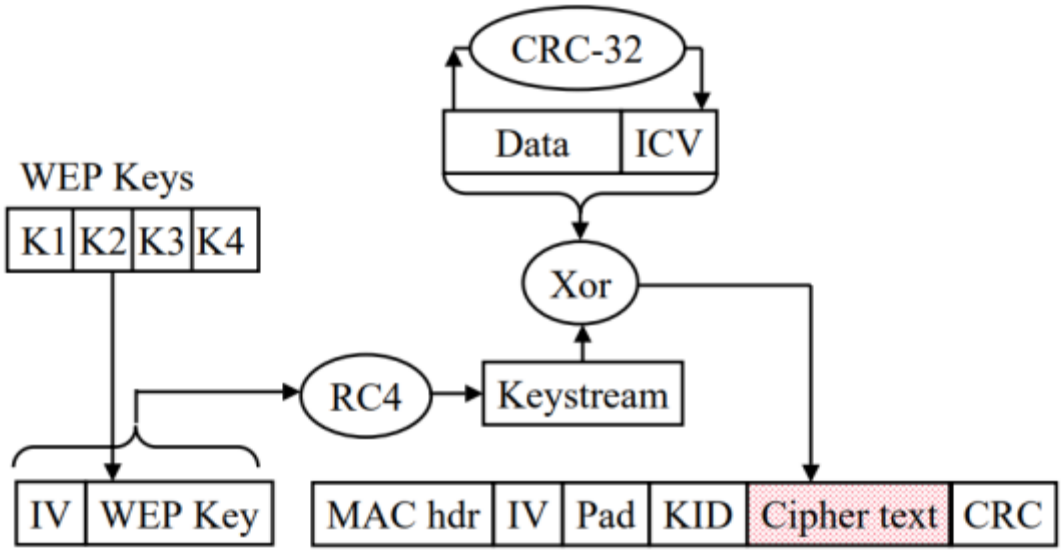

Рисунок 2.2 - WEP інкапсуляція.

- WEP декапсуляція

WEP дотримується наведеної нижче процедури для декапсуляції отриманого за

шифрованого кадру 802.11 WEP:

- WEP витягує вектор ініціалізації (IV) та ідентифікатор ключа з отриманого пакету для отримання відповідного ключа WEP. Якщо використовуються ключі зіставлення клавіш, то буде використовуватись ключ зіставлення клавіш, а ідентифікатор ключа ігнорується;

- Система розшифрування WEP створює потік ключів і застосовує потік ключів на зашифрованомупакеті для отримання простого тексту MPDU;

- ICV перераховується та порівнюється з ICV, з'єднаним у MPDU. Якщо невідповідність ICV - кадр опускається, а верхньому шару надається вказівка як помилка дешифрування;

- Проблеми в шифруванні WEP

У проводовій мережі - через те, що станції підключаються за допомогою кабелів, дані досить безпечні самі по собі. Однак, коли середовище передачі є повітряним, усі передачі даних чуються кожною станцією в мережі. Дані також можуть обнюхуватися хакерськими станціями, які можуть спробувати і розшифрувати пакети.

WEP був розроблений, щоб забезпечити безпеку, еквівалентну дротовій мережі. Однак, WEP не вдалося забезпечити те саме, що реалізація безпеки WEP була серйозно хибною. Проблеми алгоритму WEP носять комплексний характер і криються в цілій серії слабких місць:

- механізм обміну ключами (а точніше, практично повну його відсутність);
- малих розрядних ключа і вектори ініціалізації (Initialization Vector - IV);
- механізм перевірки цілісності переданих даних;
- способі аутентифікації і алгоритмі шифрування RC4.

- Вирішення проблем

Проблеми WEP були усунені в ключі шифрування TKIP через збільшення довжини IV до 48 біт. Крім того, якщо поле IV номера вичерпано, новий ключ TKIP потрібно обміняти з Точкою доступу. Виснаження IV довжини зайняло б дуже

велику кількість часу - завдяки 48-бітовій довжині та іншим параметрам (наприклад, тайм-аут клавіші PTK) потраплятиме до вичерпання IV довжини.

Перший стандарт шифрування Wired Equivalent Privacy був дискредитований знаходженням вразливостей в алгоритмі розподілу ключів RC4. Це трохи загальмувало розвиток ринку бездротових Wi-Fi мереж і викликало створення Інститут інженерів з електротехніки та електроніки (IEEE) групи 802.11i для розробки нового стандарту безпеки, що враховує відомі уразливості WEP, що забезпечує 128-бітове шифрування AES і автентифікацію для захисту переданих даних.

2.2.2 Стандарт WPA

WPA означає бездротовий захищений доступ. Стандарт WPA був введений Альянсом Wi-Fi. Стандарт WPA запровадив TKIP як просування на WEP для забезпечення кращої безпеки. WPA також представила автентифікацію користувача верхнього рівня для пристроїв 802.11. Описано два способи автентифікації користувача

1. Попередній ключ (рукостискання EAPOL);

2. 802.1X рукостискання верхнього шару EAP / EAPOL для автентифікації користувача;

Обидва вищевказані механізми автентифікації включають автентифікацію користувача, а також генерують набір ключів шифрування, які можуть бути використані для захисту даних. Асоціація WLAN та механізм автентифікації можуть бути розбиті на три фази:

1. Станція WLAN та точка доступу асоціюються одна з одною та визначають, чи використовується механізм автентифікації за допомогою загальнодоступного ключа / 802.1X

2. Обраний механізм автентифікації створює "головний ключ" в кінці фази 2.

3. Головний ключ використовується в чотирьох сторонньому рукостисканні EAPOL, отриманому тимчасовими ключами для шифрування даних в кінці фази

- Механізм шифрування TKIP

Протокол шифрування TKIP був введений для виправлення помилок, виявлених при шифруванні WEP, до моменту, коли був розроблений більш безпечний механізм шифрування (AES). Отже, мережі, що підтримують TKIP, стали Стаціонарною мережею переходу. Алгоритм TKIP застосував модифікації до існуючого алгоритму WEP для вирішення вразливостей WEP і тим самим вирішив існуючі на той час проблеми.

Схема шифрування TKIP не вимагала додаткових вимог до апаратного забезпечення та могла бути реалізована над обладнанням WEP. Отже, схема шифрування TKIP широко застосовувалася протягом певного періоду часу до появи надійних мереж безпеки.

TKIP використовує той самийформат, що і формат кадру WEP Encryption з додатковим полем розширеної вектору ініціалізації (IV) (4 байти) та полем MIC (8 байт).

- TSC0- TSC5 - лічильник послідовностей TKIP (довжина 6 байтів) - TSC0 і TSC1 утворюють IV послідовний номер для змішування TKIP фази 2 та TSC2-TSC5 використовуються в хешуванні ключа фази 1;

- Біт Ext IV включений, щоб вказати, чи є Extended IV чи ні. Для TKIP цей біт завжди встановлюється на 1;

- Key ID - Ключовий індекс;

- WEPSeed - встановлено на (TSC1 | 0x20) & 0x7f;

- MIC - перевірка цілісності Майкла;

Лічильник послідовності TKIP використовується для запобігання атакам відтворення. Якщо TSC вичерпується до нуля, ключ TKIP потрібно оновити.

- TKIP інкапсуляція

Процес інкапсуляції TKIP.

1. Обчислення TKIP MIC захищає поля даних MSDU та відповідні поля SA, DA та пріоритет. Обчислення MIC виконується на впорядкованому конкатенації полів даних SA, DA, Priority та MSDU. MIC додається до поля даних MSDU. TKIP відкидає будь-які прокладки MIC перед додаванням MIC.

2. При необхідності IEEE Std 802.11 фрагментує MSDU з MIC на один або кілька MPDU. TKIP присвоюємонотонно зростаюче значення TSC кожному MPDU, дбаючи про те, щоб усі MPDU, створені з одного і того ж MSDU, мали однакове значення розширеного IV.

3. Для кожного MPDU TKIP використовує функцію змішування ключів для обчислення насіння WEP.

4. TKIP представляє насіння WEP як ключ WEP IV і ARC4 і передає їх разом із кожним MPDU в WEP для генерації ICV та для шифрування MPDU простого тексту, включаючи весь або частину MIC, якщо він присутній. WEP використовує насіння WEP як ключ за замовчуванням WEP, ідентифікований ідентифікатором ключа, асоційованим з тимчасовим ключем.

2.2.2.4. Декапсуляція TKIP

1. Перед тим, як WEP декапсулює отриманий MPDU, TKIP витягує номер послідовності TSC та ідентифікатор ключа з WEP IV та розширеного IV. TKIP відкидає отриманий MPDU, який порушує правила послідовності(тобто кадр, лічильник послідовностей TKIP не монотонно збільшує більш високе значення.

2. TKIP представляє насіння WEP як ключ WEP IV та ARC4 і передає їх разом з MPDU на декапсуляцію WEP.

3. Якщо WEP вказує, що перевірка ICV вдалася, реалізація повторно збирає MPDU в MSDU. Якщо дефрагментація MSDU проходить успішно, приймач перевіряє MIC TKIP. Якщо дефрагментація MSDU виходить з ладу, MSDU відкидається.

4. Крок підтвердження MIC повторно обчислює MIC над полями даних MSDU SA, DA, Priority та MSDU (але не поле MK TKIP). Потім обчислений результат TIC MIC порівнюється побіжно з отриманим MIC.

5. Якщо отримані та локально обчислені значення MIC однакові, перевірка проходить успішно, і TKIP доставляє MSDU до верхнього шару. Якщо дві різняться, то перевірка не вдається; одержувач повинен відмовитися від MSDU та вжити відповідних заходів протидії.

TKIP використовує MIC (Michael Integrity Check) у надісланому пакеті, щоб перевірити, чи передається пакет справжньою WLAN-станцією, пов'язаною з мережею. Ми розберемося з потребою у TKIP MIC та форматі кадру та обчисленнях.

MIC TKIP запобігає нападам підробки. MIC - це 64-бітове (8 байт) значення. MIC сам по собі слабкий, а отже, шифрується та надсилається разом із MSDU. Оскільки ICV (Integrity Check Value) обчислюється на MPDU у шарі

MAC, перевірка Цілісності забезпечує захист верхнього рівня для різних типів атак, які пройшли перевірку ICV.

Перелік атак, від яких MIC здатний захистити, наведено нижче:

- Атаки біт-гортання;

- Дані (корисне навантаження) усікання, з'єднання та сплайсинг;

- Атаки фрагментації; - Ітеративні напади на відгадування проти ключа; - Перенаправлення шляхом зміни поля MPDU DA або RA;

- Атаки видавання себе за допомогою модифікації поля MPDU SA або TA;

MIC ускладнює успіх будь-якої з цих атак. MIC обчислюється за адресою призначення (DA), адресою джерела (SA), пріоритетом MSDU, 3 зарезервованими байтами та самою MSDU.

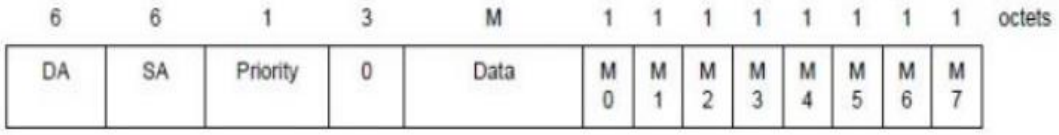

Рисунок 2.3 - СтруктураMIC.

Він додається до MSDU в кінці MSDU і весь MSDU + MIC шифрується. Це дозволяє виявляти атаки шару MAC. MSDU з приєднаним MIC може бути розділеним та надісланим у вигляді декількох MPDU. MIC сам не може забезпечити повний захист від підробок, тому TKIP також включає захист від повторного відтворення .

- Захист від відтворення TKIP

TKIP забезпечує 48-бітовий (6 байт) монотонно збільшуючи лічильник передачі послідовностей (TSC), який він додає до кожного пакету. Якщо приймається який-небудь пакетTKIP, у якому значення TSC менше або дорівнює поточному значеннюлічильника відтворення - кадр мовчки відкидається.

Стандарт 802.11 визначає набір правил захисту від відтворення TKIP і надається (від стандарту) нижче:

- Кожен MPDU повинен мати унікальне значення TKIP TSC;

- Кожен передавач повинен підтримувати один TSC (48-бітний лічильник) для кожного PTKSA, GTKSAта STKSA;

- TSC повинен бути реалізований як 48-бітний монотонно зростаючий лічильник, ініційований до 1, коли відповідний тимчасовий ключ TKIP ініціюється або оновляється;

- Формат WEP IV містить 16 LSB 48-розрядних TSC, як визначено функцією змішування TKIP (Фаза 2, STEP3). Залишок TSC переноситься в розширене IV поле;

- Одержувач повинен підтримувати окремий набір лічильників відтворення TKIP

TSC для кожного PTKSA, GTKSA та STKSA;

- Виявлення відтворення TKIP відбувається після перевірки MIC та будь-якого перевпорядкування, необхідного при обробці ACK. Таким чином, одержувач затримує просування лічильника відтворення TKIP TSC до тих пір, поки MSDU не пройде перевірку MIC, щоб запобігти зловмисникам вводити MPDU з дійсними ICV і TSC, але недійсними MIC;

- Для кожного PTKSA, GTKSA та STKSA приймач повинен підтримувати окремий лічильник відтворення для кожного пріоритету кадру та використовувати TSC, відновлений з отриманого кадру, для виявлення відтворених кадрів. Повторний кадр виникає, коли TSC, вилучений з отриманого кадру, менший або рівний поточному лічильнику відтворення для пріоритету кадру. Передавач не повинен упорядковувати кадри з різними пріоритетами, не гарантуючи, що приймач підтримує необхідну кількість лічильників повтору. Передавач не повинен впорядковувати кадри в межах лічильника відтворення, але може переупорядковувати кадри через лічильники відтворення. Однією з можливих причин переупорядкування кадрів є пріоритет IEEE 802.11 MSDU;

- Одержувач повинен відкинути будь-який MPDU, отриманий поза порядком, ізбільшить значення dot11RSNAStatsTKIPReplays для цього ключа; - Для MSDU, що надсилаються за допомогою функції Block Ack, переупорядкування отриманих MSDU відповідно до приймача Block Ack виконується до виявлення повторного відтворення;

У 2004 альянс Wi-Fi 18 випустили новий стандарт, який набрав більшу попу

лярність на сьогоднішній день, стандарт WPA2, який представляє собою поліпшення стандарту WPA. Основна різниця між стандартами WPA і WPA2 полягає в технології шифрування: у WPA - TKIP і у WPA2 - AES. Стандарт WPA2

дозволяє забезпечити більш високий рівень захисту бездротової мережі, так як TKIP дозволяє створювати ключі довжиною тільки до 128 біт, а AES - вже до 256 біт. Можна дійти до висновку, що WPA був перехідним протоколом безпеки, на якого не покладали великих сподівань. Він хоч і був кращим за WEP, але теж мав свої недоліки, які на жаль ніхто не усунув, бо на зміну йому прийшов новий протоколWPA2.

2.2.3 Стандарт WPA2

Стандарт IEEE 802.11i, також відомий як Wi-Fi Protected Access 2 (WPA2), є поправкою до 802.11 стандарт із зазначенням механізмів захисту бездротових мереж. Проект стандарту був ратифікований на початку літа 2004 р. Він замінює попередні технічні умови безпеки, конфіденційність провідної еквівалентної конфіденційності (WEP), яка виявила серйозні недоліки в безпеці. Захищений доступ Wi-Fi (WPA) раніше був представлений як проміжне рішення щодо невпевненості в WEP. WPA реалізував лише підмножину IEEE 802.11i. WPA2 використовує специфічний режим Розширеного стандарту шифрування (AES), відомого як протокол автентифікації коду ланцюга блоку шифрування контр режимного режиму (CBC-MAC) (CCMP). CCMP забезпечує як конфіденційність даних (шифрування), так і цілісність даних. Використання розширеного стандарту шифрування (AES) є більш безпечною альтернативою шифру потоку RC4, який використовується WEP та WPA.

Стандарт WPA2 має два компоненти, шифрування та автентифікація, які мають вирішальне значення для безпечної бездротової локальної мережі. Елемент шифрування WPA2 передбачає використання AES (Advanced Encryption Standard), але TKIP (Temporal Key Integrity Protocol) доступний для зворотної сумісності з існуючим обладнанням WAP. Елемент автентифікації WPA2 має два режими: Персональний та Підприємницький.

Персональний режим вимагає використання PSK (попередньо діленого ключа) і не вимагає, щоб користувачі мали окрему автентифікацію.

У режимі Enterprise, який вимагає індивідуальної автентифікації користувачів на основі стандарту автентифікації IEEE 802.1X, використовується розширений протокол EAP (протокол розширюваної автентифікації), який пропонує п'ять стандартів EAP на вибір:

- EAP-MD5;

- безпека рівня EAP-транспортного рівня (EAP-TLS);

- захищеність транспортного шару з підтримкою EAP (EAP-TTLS);

- захищений протокол автентифікації виклику рукостискання EAP vo / EAPMicrosoft;

- v2 (PEAPvo / EAP-MSCHAPv2);

- захищена карта EAP v1 / EAP-Generic (PEAPv1 / EAPGTC) та модуль посвідчення абонента EAP-абонента Глобальної системи мобільних комунікацій (EAPSIM);

EAP-MD5 використовує MD5 алгоритм для обчислення хеш-значення пароля,

які відправляються на сервер і на його стороні звіряються зі збереженим хеш-значенням. Протокол EAP-FAST дозволяє авторизуватися за логіном і паролем, а PEAP-GTC - за спеціальним токеном. Протоколи PEAP-MSCHAPv2 і EAP-TLS проводять авторизацію по клієнтським сертифікатами.

Максимальний захист мережі Wi-Fi забезпечує тільки WPA2-Enterprise і цифрові сертифікати безпеки в поєднанні з протоколом EAP-TLS або EAP-TTLS. Сертифікат - це заздалегідь створені файли на сервері RADIUS і клієнтському пристрої. Клієнт і сервер автентифікації взаємно перевіряють ці файли, тим самим гарантується захист від несанкціонованих підключень з чужих пристроїв і помилкових точок доступу. Протоколи EAP-TTL / TTLS входять в стандарт 802.1X і використовують для обміну даними між клієнтом і RADIUS інфраструктуру відкритих ключів (PKI). PKI для авторизації використовує секретний ключ (знає користувач) і відкритий ключ (зберігається в сертифікаті, потенційно відомий всім). Поєднання ці ключів забезпечує надійну автентифікацію.

WPA2 встановлює захищений комунікаційний контекст у чотири фази. На першому етапі сторони, AP та клієнт, домовляться про політику безпеки (метод автентифікації, протокол для одноадресного трафіку, протокол для багатоадресної передачі та метод попередньої автентифікації) для використання, що підтримується AP та клієнтом. На другій фазі (застосовується лише для режиму підприємства).

- Автентифікація WPA2

Однією з найважливіших змін, внесених до стандарту WPA2, є відокремлення автентифікації користувачів від забезпечення цілісності та конфіденційності повідомлення, тим самим забезпечуючи більш масштабовану 61 та надійну архітектуру безпеки, придатну для домашніх мереж або корпоративних мереж з рівними можливостями.

Автентифікація в персональному режимі WPA2, що не вимагає сервера автентифікації, виконується між клієнтом та AP, генеруючи 256-бітний PSK з простої тексту пропуску (від 8 до 63 символів). PSK спільно з ідентифікатором службового набору та довжиною SSID утворюють математичну основу для PMK (Pair-mud Master Key), який буде використаний пізніше при генерації ключів.

Автентифікація в режимі WPA2 Enterprise покладається на стандарт автентифікації IEEE 802.1X. Основними компонентами є заявник (клієнт), що приєднується до мережі, автентифікатор (AP виступає автентифікатором), що забезпечує контроль доступу, і сервер автентифікації (RADIUS), який приймає рішення про авторизацію. Автентифікатор (AP) розділяє кожен віртуальний порт на два логічні порти, один для обслуговування та інше для автентифікації, складання PAE (Port Access Entity). PAE автентифікації завжди відкритий, тоді як служба PAE відкрита лише після успішної автентифікації сервером RADIUS. Автентифікатор перетворює повідомлення EAPoL у повідомлення RADIUS, а потім пересилає їх їх на сервер RADIUS. Сервер автентифікації, який повинен бути сумісний з типами EAP заявника, отримує та обробляє запит автентифікації. Після завершення процесу автентифікації заявник та автентифікатор мають секретний MK (головний ключ).

- Механізм шифрування AES

Схема шифрування AES була введена в 802.11i для використання в надійних мережах безпеки. Використовуваний механізм шифрування AES - це "CTR з протоколом CBC-MAC (CCMP)". CCMP заснований на CCM алгоритму шифрування AES. CCM поєднує CTR для конфіденційності даних та CBC-MAC для автентифікації та цілісності. CCM захищає цілісність як поля даних MPDU, так і вибраних частин заголовка MPEU 802.11 IEEE. "Розмір блоку, який використовується в AES, становить 128 біт, а ключ також

- 128 бітова довжина ключа. Формат CCMP MPDU

- 8 байт заголовка CCMP та 8 байтів MIC додано до MPDU для шифрування AES;

- Номер пакету (PN) становить 6 байт

- PN0 найменш значущий байт і PN5 - найзначніший байт;

- Поле Ext IV повідомляє приймач, що додаткові 8 байт заголовка додаються до MPDU завдякиCCMP. Для CCMP - поле Ext IV встановлено у 1;

- Поле "Ідентифікатор ключа" - містить ідентифікатор ключа, який використовується при капсулюванні CCMP зарезервовані біти встановлюються на нуль;

- AES інкапсуляція

Процес шифрування AES включає шифрування частини даних MPDU. Блок-схема інкапсуляціїCCMP Наведені нижче кроки виконуються для інкапсуляції частини кадру даних та створення зашифрованого AES кадру для передачі:

- Збільшення PN, щоб отримати свіжий PN для кожного MPDU, щоб PN ніколи не повторювався для одного і того ж тимчасового ключа. Зауважимо, що повторно передані MPDU не змінюються при повторній передачі.

- Використовування поля в заголовкуMPDU для побудови додаткових даних автентифікації (AAD) для CCM. Алгоритм CCM забезпечує захист цілісності для полів, включених до AAD. Поля заголовка MPDU, які можуть змінюватися при повторному переданні, відключаються, маскуючись до 0 при обчисленні AAD.

AAD побудований із заголовка MPDU. Параметри в заголовку MPDU, які різняться - певні IE, такі як поле управління HTT і поле тривалості, не є частиною побудови AAD. З тієї ж причини - певні параметри в полі Frame Control маскуються до нуля. ДовжинаAAD також змінюється залежно від наявностіполя керування QoS та полів A4.

- Декапсуляція AES

Кроки, що беруть участь у процесі декапсуляції, описані нижче:

1. Зашифрований MPDU аналізується для побудови значень AAD та nonce;
2. AAD формується ззаголовка MPDU зашифрованого MPDU;
3. Значення Nonce будується з полів A2, PN та Nonce Flags;

4. MIC витягується для використання при перевірці цілісності CCM;

5. Обробка реципієнта CCM використовує текстові дані шифруваного ключа, AAD, не відтак, MIC та MPDU для відновлення даних простого тексту MPDU, а також для перевірки цілісності даних простого текстуAAD та MPDU;

6. Отримані заголовки MPDU та дані простого тексту MPDU від обробки отримувачаСКМоб'єднуються у формуMPDU простого текст;

7. Обробка дешифрування запобігає відтворенню MPDU, перевіряючи, що ПН у MPDU перевищує лічильник відтворення, який підтримується для сеансу;

- Вразливості WPA2

Хоч і WPA2 був новітнім протоколом захисту даних в безпровідних мережах, який вирішував всі проблеми і недоліки своїх попередників, він все ж 65 таки мав і свої вади, які виявлялись далеко не в перші роки його використання. Одними з відомих вразливостей були:

- Атака Hole196 – за допомогою цієї атаки зловмисник, що авторизований в мережі, міг розшифровувати дані інших користувачів цієї мережі застосовуючи свій закритий ключ. Атака проводилась без застосування брут-форсу чи злому ключів.

- Також, ця система була вразлива до взлому словниками і брутфорсом. Тобто можна було підібрати пароль чи записати деякі пакети даних. Атака проводилась офлайн за допомогою програми та файлом з нарахуванням хендшейку. В основному вона була націлена на захоплення «рукостискання» (Handshake), тобто захоплення початкового обміну пакетами.

Але ті вразливості були не дуже суттєвими в порівняні з наступною. У 2017 році в протоколі WPA2 була виявлена серйозна вразливість, що отримала назву KRACK (K ey R einstallation A tta ck), яка дає можливість зловмиснику атакувати 4-х стороннє рукостискання протоколу WPA2, тобто ініціювання WPA2-з'єднання. Це рукостискання відбувається кожного разу, коли клієнт хоче приєднатися до захищеної Wi-Fi мережі WPA2, щоб підтвердити, що клієнт і точка доступу мають правильні облікові дані, тобто пароль Wi-Fi, перед тим, як клієнт приєднається до мережі. Під час того ж 4-х стороннього рукостискання встановлюється свіжий ключ шифрування, який використовується для шифрування подальшого трафіку. Маніпулюючи цим рукостисканням, зловмисник

може обманути жертву перевстановши вже використаний ключ шифрування, тоді як ключ повинен бути встановлений і використаний лише один раз. Перевстановлення ключа шифрування змушує скинути два лічильника (відомі як "nonces"), використовувані протоколом шифрування, і це дозволяє атакувати на протокол, наприклад, повторення, розшифрування або підробка пакетів. Потенційний зловмисник, який перебуває у фізичній близькості від захищеної мережі Wi-Fi і здійснює цю атаку, відому як "людина-в- 66 середині". Зловмисник може по суті перехоплювати та розшифровувати інтернет-трафік без володіння обліковими даними захищеної мережі Wi-Fi (тому зміна пароля Wi-Fi не допоможе). Ключова атака переустановки проілюстрована на рисунку 2.4.

Рисунок 2.4 - Ключова атака переустановки (KRACK)

Ці вразливості, поряд з усіма раніше відомими недоліками протоколу WPA2 наштовхнув Wi-Fi Alliance на розробку чогось нового, що могло б не зважати на ці проблеми. Так в середині літа 2018 року ратифікувався новий протокол захисту – WPA3.

Висновки до другого розділу:

У даному розділі було розглянуто основні вразливості мереж безпровідного доступу. Також розглянуто основні протоколи захисту мереж безпровідного

доступу, що забезпечують цілісність інформації, такі як WEP;WPA;WPA2; Виходячи з загальних положень і спираючись на сукупність всіх перелічених фактів в цьому розділі можна сказати, що на даний момент найбільш розповсюджений протокол WPA2.

Найбільш вживаним і основним протоколом на теперішній час являється WPA2, а особливо його два підтипи:

- WPA2;
- WPA2 Enterprise;

В наступному розділі буде розглянуто протокол безпеки WPA2 Enterprise, та як він захищає корпоративну мережу від зловмисників, що бажають заволодіти даними користувачів цієї мережі. Буде показано основні атаки та як протокол

справляється з ними.

ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ПРОТОКОЛУ WPA2 ENTERPRISE

Різниця між WPA2 Personal і WPA2 Enterprise полягає в тому, звідки беруться ключі шифрування, які використовуються в механізмі алгоритму AES. Для приватних (домашніх, дрібних) застосувань використовується статичний ключ (пароль, кодове слово, PSK (Pre-Shared Key)) мінімальною довжиною 8 символів, яке задається в настройках точки доступу, і у всіх клієнтів даної бездротової мережі однаковим. Компрометація такого ключа вимагає негайної зміни пароля у всіх, хто лишився користувачів, що реально тільки в разі невеликого їх числа. Для корпоративних застосувань, як випливає з назви, використовується динамічний ключ, індивідуальний для кожного працюючого клієнта в даний момент. Цей ключ може періодичний оновлюватися по ходу роботи без розриву з'єднання, і за його генерацію відповідає додатковий компонент - сервер авторизації, і майже завжди це RADIUS-сервер.

Таблиця. 3.1.Всі можливі параметри безпеки протоколу WPA2 Enterprise

Властивість	WPA 2 (Enterprise)
Ідентифікація	Користувач, комп’ютер
Авторизація	EAP або загальний ключ
Цілісність	CRT/CBC-MAC (Counter mode Cipher

	Block Chaining Auth Code — CCM) Part of AES
Шифрування	CCMP (AES)
Розподілення ключів	Похідна від PMK
Вектор ініціалізації	48-біт номер пакету (PN)
Довжина ключа, біт	До 256
Інфраструктура	RADIUS

3.1 Небезпека корпоративних мереж

Якщо говорити про безпеку персональних даних в персональній мережі і в корпоративній мережі, то перевагу отримає остання, так як ці мережі більш захищенні від зломів та перехоплень даних, що передаються. Але не потрібно розслаблятись, адже не кожна мережа надійна. Зловмисник, з метою викрадення ваших персональних даних зможе проникнути і в корпоративну мережу. В його арсеналі є не тільки хороший рівень кваліфікації, а й хороший набір спеціалізований інструментів, таких як:

- Wi-Fi адаптери для роботи на різних частотних діапазонах;
- Мікрокомп’ютери для створення підробленої точки доступу;
- Спрямовані антени;
- Обладнання для аналізу мережі;

- Різне ПО, що дозволяє проводити аналіз безпеки Wi-Fi мереж;

Спочатку зловмисника зацікавить інформація про механізми безпеки, що використовуються в механізмах автентифікації і алгоритмах шифрування корпоративної мережі. Вся зібрана ним інформація в майбутньому буде використана для проведення злому обраної ним мережі. Існує таке поняття як «контрольована зона», де використання Wi-Fi мереж буде безпечним і ця мережа буде доступна тільки для працівників компанії. Якщо «контрольованої зони» не має, то злом корпоративної мережі є можливим. Адже якщо обмеження по потужності сигналу на маршрутизаторах відсутні, то доступ до мережі може здійснюватися з прилеглих до будівлі територій. Багато великих компаній нехтують цим і наражають своїх співробітників і саму компанію на небезпеку.

Зловмисник не буде втрачати таку можливість для проведення різних атак на мережу за межами «контрольованої зони». Так як йому ніхто не заважатиме і він буде не помітним, то він може застосовувати не тільки швидкі атаки, а й 76 довготривалі атаки – підбор ключа безпеки. Зловмисник для взлому може використовувати різні типи атак, а саме такі:

- Підроблена точка доступу;
- Перехід з гостьової мережі в корпоративну;
- Несанкціоновані точки доступу;
- Словарні ключі безпеки;
- Використання механізму WPS;
- Не захищена автентифікація;

Всі ці атаки призводять до того, що зловмисник так чи інакше проникає в корпоративну мережу і може зловживати персональними даними користувачів, даними самої компанії та іншими ресурсами. Детальніше вплив кожної атаки на мережу і як з цим боротися розглянемо в наступних пунктах.

3.1.1 Підроблена точка доступу

Всі ґаджети, що працюють в корпоративній мережі коли підключаються до безпровідної мережі автоматично запам’ятовують її назву (SSID мережі). Наші люди ліниві і вони не люблять кожного разу по новому підключатись до мережі, тому користуються небезпечним налаштуванням «Автоматичне підключення до мережі». Хоч ця функція і полегшує життя користувачів, але вона несе за собою деяку потенційну загрозу. Коли пристрій буде в межах доступу до корпоративної мережі, ґаджет автоматично підключиться. Саме в такий момент зловмисник створює підроблену ТД, після чого ґаджети співробітників, що знаходяться в зоні підробленої ТД, будуть відправляти запити на автентифікацію автоматично.

Рисунок 3.1 - Атака із застосуванням підробленої ТД

І якщо в корпоративній мережі використовується протокол PEAPv0 / EAPMsCHAPv2, а в користувача не перевіряється сертифікат ТД, то зловмисник з легкістю може проводити атаку з підробленою ТД. Він акцентується на перехоплення пари «Challende + Response», які застосовуються коли проводиться запит на автентифікацію. Отримані дані можуть слугувати для захоплення хеш пароля методом підбору.

Отримавши значення пари «Challenge + Response», зловмисник буде застосовувати суперкомп'ютер для підбору ключів, що засновані на аглоритмах DES і SHA1, щоб отримати хеш пароля. В результаті в нього це вдасться.

Найбільш небезпечним є те, що користувачі можуть навіть не підозрювати, що їх намагаються взломати, адже зловмисник в цьому випадку зовсім не помітний. Він може розмістити підроблену ТД де завгодно – нижній поверх будівлі, кафе, парковка. Як тільки користувач буде в зоні роботи мережі, зловмисник почне діяти і спробує підключити пристрій зі збереженим раніше значенням SSID.

Найкраще рішення в цій ситуації, це не допускати виходу мережі за територію компанії. Але не завжди є можливість так зробити, тому для таких ситуацій рекомендується застосовувати в корпоративних мережах безпечні методи автен-

тифікації, такі як EAP-TLS з використанням клієнтського сертифіката і перевіркою сертифіката сервера. Цей протокол вимагає встановлення клієнтських сертифікатів на кожен новий сеанс. І якщо зловмисник захоче атакувати з використанням підробленої ТД, то він потерпить невдачу.

3.1.2 Перехід з гостьової мережі в корпоративну

Гостьова мережа була спеціально зроблена для гостей, яких приймає компанія. Але співробітники компаній часто користуються цією мережею, навіть не підо

зрюючи, що вони наражають на небезпеку свої дані. Гостьова мережа майже не використовує механізми шифрування. І якщо мережа не ізолює користувачів один від одного, то зловмисник, що зміг отримати доступ до гостьової мережі, запросто має змогу атакувати співробітників компанії. Цей вид атаки часто поєднують з використанням підробленої ТД.

Вирішенням цієї проблеми є простим – потрібно використовувати режим ізоляції користувачів точки доступу та використання надійніших механізмів шифрування. А також заборонити співробітникам компанії використовувати гостьову точку доступу.

3.1.3 Несанкціоновані точки доступу

Часто співробітники використовують інтернет в особистих цілях, але не кожна компанія вони мають можливість доступу до ресурсів, що задовольняють ці потреби. Саме тому співробітники для цього використовують смартфони чи розгортають на ньому безпроводову ТД, до якої підключають робочу станцію. В такому випадку вони користуються інтернет-ресурсами через несанкціоноване з'єднання. При успішній атаці на такі бездротові мережі зловмисник здатний отримати доступ до ресурсів цієї мережі, а також проводити атаки на користувачів цієї точки доступу.

Після перехоплення значень рукостискання користувача і ТД можна отримати змогу проводити локально атаки на підбір пароля. Застосовуючи підібраний пароль дізнаємось, що зовнішній IP-адрес пристрою належить одній з стільникових компаній. В зв’язку з цим було здійснено успішний вхід в додаток «Особистий кабінет» без пароля, і виявилось що це корпоративний обліковий запис.

При цьому через цей доступ можна встановлювати переадресацію дзвінків, відправляти SMS і т. д.

Рішенням цієї проблеми є проведення періодичних перевірок з виявлення несанкціонованих точок доступу в мережі. У разі виявлення негайно відключати їх. Також пропонується проведення тренінгів в компанії для співробітників з метою покращення обізнаності в питані інформаційної безпеки.

3.1.4 Словарні ключі безпеки

Це одна з найпопулярніших вразлвостей в багатьох безпровідних мережах. Ключі безпеки, що використовуються мають недостатню довжину або вони є дуже простими, тому з легкістю можуть бути підібрані зловмисником. Він може перехопити рукостискання для атакованої ТД і мати змогу без підключення до мережі підбирати пароль. Успішний підбір пароля може бути здійснений в короткі терміни.

В невеликих компаніях пароль іноді співпадає з назвою самої компанії або іншими схожими даними. Для зловмисника це як цукерку в дитини відібрати. Він використовує за допомогою програм CeWL і RSMangler може з легкістю здійснити «персоналізовану» атаку на підбір. Саме в цьому випадку буде створено словник спеціально для підбору пароля атакованої компанії. Це є досить простою процедурою.

```
                                Aircrack-ng 1.2 rc4

[00:00:00] 8/9822768 keys tested (102.97 k/s)

Time left: 1 day, 2 hours, 45 minutes, 1 second                 0.00%

                        KEY FOUND! [ 12345678 ]


Master Key     : 9B E0 20 EF 21 4F 5D 7D 1C 7A 06 93 F1 85 86 6F
                 4B D9 D1 F1 5A 70 2F 16 05 F9 2E 71 9C 81 DF 88

Transient Key  : EB B3 2E 39 CE F2 F3 65 6A A3 D6 54 85 73 93 E2
                 29 0F 9E CE BA 66 2D 83 37 3B 76 49 86 D7 1A AF
                 1D 8F 9A DA 61 08 96 9A 20 6C A5 07 FD 29 1A E4
                 6E 49 A1 C3 E0 AB 63 7F 79 0F A1 F4 B1 DC 52 BD

EAPOL HMAC     : 6E 6C 38 2C 89 D3 C5 BE 79 55 D5 B5 5C 8B FE 2D
```

Рисунок 3.2 - Підбір пароля для доступу бездротової мережі.

Рішення проблеми просте – використання надійних і складних паролів, та зміна паролів раз в квартал.

3.1.5 Використання механізму WPS

Ще один випадок, коли людина наражає себе на небезпеку обираючи зручність, а не надійність. WPS (Wi-Fi Protected Setup) – це механізм, який був призначений для спрощення процесу налаштування бездротової мережі. При використанні цього механізму в мережі ім'я і тип шифрування задаються автоматично, а для підключення до ТД застосовується деякий PIN-код. В більшості випадків він складається тільки з цифр і інколи цей код може бути написаний прямо на роутері. В багатьох роутерів цей механізм налаштування 82 активований з самого початку. Тому зловмисник може підібрати PIN-код і отримати доступ до мережі. Для цього підбору є спеціальне ПО, що допомагає знайти такі точки доступу і проводити на них атаки. Таке ПО є у вільному доступі, тому кожен бажаючий зловмисник може скачати його собі і займатись зломами мереж.

Рисунок 3.3 - Успішний підбір PIN-коду точки доступу

Рішенням даної проблеми є відключення механізму WPS в налаштуваннях точки доступу.

3.1.6 Не захищена автентифікація

Іноді розгортання безпровідної мережі може виконуватись по фільтрації MAC-адрес ґаджетів, що підключаються. В таких випадках мережа наражає себе на атаку KRACK.

Наприклад є безпровідна мережа для доступу до якої реалізована автентифікація з використанням веб-інтерфейсу, доступного по протоколу HTTPS. Після

успішної автентифікації зберігався MAC-адрес підключеного ґаджету для ідентифікації пакетів в мережі. При наступному підключенні користувача автентифікація відбувалася по MAC-адресу.

Зловмисник, застосовуючи підроблену ТД, передає запити від користувачів до дійсної точки доступу через власне обладнання. Після цього ґаджет одного з співробітників підключається до підробленої ТД, і вже згодом користувач повторно ввів в підроблену форму автентифікації свої облікові дані, які одразу ж були перехопленні зловмисником. Далі весь обмін між користувачем і ТД буде проходити через зловмисника. Це дає йому змогу записати MAC-адрес підробленої ТД в таблицю автетентифікованих пристроїв і прослуховувати трафік співробітника непомітно для нього. Також доступ до мережі дозволив звертатись до інших мережевих ресурсів.

Для рішення цієї проблеми потрібно використовувати більш безпечні методи автентифікації. (див. Розділ «Підроблена точка доступу»).

3.2 Надання рекомендацій для захисту зі сторони мережі

У корпоративних мережах можливі два сценарії установки підробленої ТД:

- Підроблена ТД функціонує як незалежна від мережі точка;
- ПідробленаТД підключається прямо до комутатора/контролеру локальної мережі ;

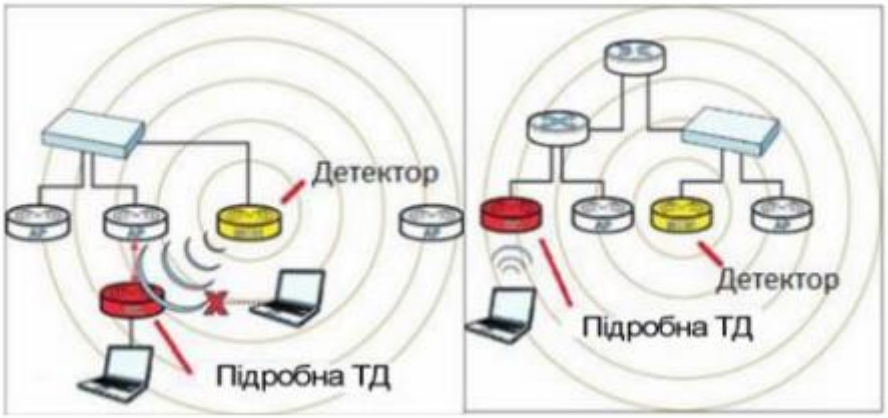

Рисунок 3.4 - Підроблена ТД є незалежною; Підроблена ТД підключена до внутрішньої мережі.

На контролері безпровідної мережі налаштовуються списки довірених ТД на основі їх Mac-адрес. Ті адреси, які не входять до цього списку, для безпеки відкидаються. Більш ефективним рішенням є настроювання однієї із ТД у режим моніторингу. ТД сканує радіоефір і шукає підозрілі точки. Якщо ідентифікована ТД не підключена до локальної мережі, то детектор заважає їй працювати, а саме розсилає широкомовні пакети, щоб клієнти не могли підключитися до підробленої ТД (Рисунок 3.5).

Рисунок 3.5 - Заходу захисту від підроблених ТД, яка не підключена до провідної мережі

Якщо підключена провідним з'єднанням, то з'являється можливість заблокувати її роботу через порт комутатора (Рисунок 3.6).

Рисунок 3.6 - Заходу захисту від підроблених ТД, яка підключена до провідної мережі.

На сьогодні найкращими технологіями для захисту безпровідних мереж володіє компанія Cisco. Вона підтримує технологію WIPS (Wireless Intrusion Prevention System), що виявляє підроблені ТД . Діагностування підозрілої ТД проводиться на основі SSID. Процес керування такими точками доступу здійснюється в 3 етапи:

1. Виявлення. Спеціальна ТД переводиться в режим моніторингу й сканує ефір, збираючи такі дані, як SSID, Mac-адреси точки і її клієнтів, IP-адреси. Отримані дані заносяться на контролер.

2. Класифікація. Точки-детектори порівнюють дані про підроблену ТД, отримані по бездротовому каналу, з тими, що отримані по провідному каналу. Якщо Mac-адреса підробленої точки був виявлений у провідній мережі, то така підроблена точка розглядається як критична. Cisco має спеціальний протокол RLDP, який допомагає визначити, чи підключена підроблена ТД до провідної мережі, підключаючись до неї прямо в якості клієнта й посилаючи її дані по протоколу RLDP на CPI.

3. Усунення. Визначається місце розташування ТД та створюються перешкоди. Проходить процес відключення портів цієї ТД.

3.2.1 Надання рекомендацій для захисту зі сторони клієнта

Клієнтський пристрій можна захистити такими способами:

• відключати автоматичні підключення до мереж Wi-Fi. Кожен раз після користування ТД нажимати кнопку «Забути дану мережу», щоб пристрій не підключився до неї знову.

• включення фільтрації підключень програмними засобами. Наприклад, в ОС Windows дане налаштування можна зробити за допомогою вбудованої утиліти netsh.

В ОС Linux схоже налаштування можна провести за допомогою вбудованої утиліти iptables, однак блокування можливе тільки по Mac-Адресам.

• використання сторонніх утиліт. Наприклад, утиліт, які дозволяють самостійно виявити підозрілих ТД, таких як Waidps, Evilapdefender, Smart Wi-Fi Toggler.

• підключатися тільки до мереж, захищених по протоколах EAP.

• відключення бездротового адаптера. Метод є самим радикальним, однак найбільш діючим.

Висновок до третього розділу:

У цьому розділі було розглянуто шість типів атак, та наведення прикладу їх дії, а саме:

- Підроблена точка доступу;
- Перехід з гостьової мережі в корпоративну;
- Несанкціоновані точки доступу;
- Словарні ключі безпеки;
- Використання механізму WPS;
- Не захищена автентифікація; Також було наведено рішення до кожної з вразливостей, для запобігання можливих атак в майбутньому. Наведено рекомендації для захисту даних для:
- Зі сторони мережі;
- Зі сторони користувача;

У зловмисника є безліч варіантів, щоб проникнути в корпоративну мережу. Якби кожна компанія виконувала всі рекомендації, дотримувалась парольної політики, а співробітники в свою чергу з відповідальністю ставились до

політики конфіденційності, і не нехтували б рекомендаціями, то більшість вразливостей можна було б уникнути.

ВИСНОВКИ

У роботі розглянуто захист мереж безпровідного доступу на базі технології Wi-Fi з протоколом безпеки WPA2 Enterprise.

Мета, яка була поставлена перед виконанням роботи, виконана, а отримані результати в ході виконання дипломної роботи відповідають сформульованим завданням і повністю задовольняють їх. Для досягнення мети були зроблені такі дії:

У першому розділі було розглянуто безпровідні мережі передачі інформації. Визначено, що безпровідна локальна мережа WLAN має найбільший масштаб розгортання, саме тому її було обрано для подальшого розгляду. Детальним аналізом цієї мережі були опрацьовані такі пункти:

- Ознайомлено з чотирма топологіями розгортання мережі безпровідного доступу;
- Були опрацьовані стандарти мережі Wi-Fi;
- Розглянуто основний механізм доступу та рівні мережі; Завдяки своїй простоті, дешевизни послуг і зручністю користування, безпровідні локальні мережі Wi-Fi мають широке застосування у різноманітних сферах. Завдяки цій технології працюють як і домашні мережі, так і великі корпоративні.

2) У другому розділі були розглянуті типи атак на мережі безпровідного доступу. Особливу увагу було приділено протоколам безпеки, що протидіють цим вразливостям:

- WEP;
- WPA;
- WPA2;

3) У третьому розділі було розглянуто відмінність між протоколом WPA2 та WPA2 Enterprise. Були наведені можливі типи атак на корпоративну мережу, їх розгортання та застосування при зломі. Також після кожної з атак було наведено рішення, що сприяло б уникненню або виправленню існуючої вразливості. Також було надано рекомендації для подальшого захисту від атак на корпоративну мережу, а саме для:

- Захист зі сторони мережі;

- Захист зі сторони користувача;

Було виявлено, що дотримання і виконання цих рекомендацій суттєво зменшить ризик на небезпеку персональних даних як самих користувачів, так і компанію.

Отже, я вважаю, що поставлена мета виконана.

ПЕРЕЛІК ПОСИЛАНЬ

1. Mathy Vanhoef and Frank Piessens. Predicting, decrypting, and abusing wpa2/802.11 group keys. In 25th USENIX Security Symposium, USENIX Security 16, 2016 – 673c.

2. Tanenbaum A. Computer Networks / A. Tanenbaum, D. Wetherall. – New Jersey: Pearson, 2012. – 959 c. – (5th Edition).

3. Mathy Vanhoef and Frank Piessens. Release the kraken: new KRACKs in the 802.11 standard. In Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS). ACM, 2018.

4. V Міжнародна науково-практична конференція "SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY". Збірник матеріалів конференції. 8-10 січня 2020 року – Ліверпуль.2020. – 803 с.

5. ВИКОРИСТАННЯ ГІБРИДНИХ БЕЗПЛАТНИХ МЕРЕЖ ДОСТУПУ НА ОСНОВІ ТЕХНОЛОГІЙ LI-FI І WI-FI ДЛЯ РОЗВИТКУ ЕФЕКТИВНОСТІ ОБСЛУГОВУВАННЯ. IV Міжнародна науковопрактична конференція "SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS". Збірник матеріалів конференції. 16-17 березня 2020 року – Харків. 2020. – 180 с.

6. АНАЛІЗ РОБОТИ ПРОТОКОЛУ ЗАХИСТУ БЕЗПРОВОДОВИХ МЕРЕЖ WPA2. І Міжнародна науково-практична конференція “MODERN SCIENCE: PROBLEMS AND INNOVATIONS”. Збірник матеріалів конференції. 5-7 квітня 2020 року – Стокгольм. 2020. – 229 с.

7. АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3. XIV Міжнародна науково-технічна конференція «Перспективи телекомунікацій»; ПТ2020: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2020. – С. 98-102. ISSN(print) 2663-502X

8. Угрозы для беспроводной корпоративной сети WPA2-Enterprise и способы защиты [Електронний ресурс]. – 2017. – Режим доступу до ресурсу:https://uni.dtln.ru/digest/ugrozy-dlya-besprovodnoy-korporativnoyseti-wpa2-enterprise-i-sposoby-zashchity

9. WPA2-Enterprise. Как создать безопасную сеть? [Електронний ресурс]. – 2018. - Режим доступу до ресурсу: https://wifi-solutions.ru/zashitakorporativnoy-seti-s-wpa2-enterprise/

10 WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети. [Електронний ресурс]. – 2012. - Режим доступу до ресурсу:

https://habr.com/ru/post/150179/
11. DSSS - Direct Sequence Spread Spectrum.[Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.telecomabc.com/d/dsss.html 92
16. Стандарт локальних мереж ieee 802.11 wi fi. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://beloshop.ru/uk/ethernetstandard-ieee-80211-wi-fi/
12. Some WLAN Network Topologies – BSS, IBSS, Mesh BSS and P2P [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.hitchhikersguidetolearning.com/2017/09/17/some-wlannetwork-topologies-bss-ibss-mesh-bss-and-p2p/
13. Стандарт IEEE 802.11 для широкосмугового безпровідного доступу [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: http://www.ce-studbaza.ru/schriebe.php?id=1040
14. 802.11 b g n методи перевірки. Способи збільшення швидкості з'єднання бездротової мережі Wi-Fi [Електронний ресурс]. – 2016 – Режим доступу до ресурсу: https://reactor-web.ru/uk/80211-b-g-nverification-methods.html
15. Wireless LAN (WLAN) [Електронний ресурс]. – 2017. – Режим доступу до мережі: http://www.hitchhikersguidetolearning.com/wireless-lan-wlanarticles/
16. Wi-Fi [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Wi-Fi.
17. Wi-Fi сети: проникновение и защита. 3) WPA. OpenCL/CUDA. Статистика подбора [Електронний ресурс]. - 2014. – Режим доступу до ресурсу: https://m.habr.com/ru/post/226431/
18. Захист мереж безпроводового доступу на базі технології wi-fi з протоколом wpa2-enterprise [Електронний ресурс]. – Режим доступу до ресурсу: http://tk-its.kpi.ua/sites/default/files/2020-07/Pidpalyi_bakalavr.pdf