МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Система забезпечення захисту інформації в бездротових технологіях»

Виконавець: _____ Анна ШАПОВАЛОВА
(підпис)

Керівник: _____ Георгій КОНАХОВИЧ
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Шаповалової Анни Володимирівни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Система забезпечення захисту інформації в бездротових технологіях»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: Проаналізувати стандарти мереж бездротового доступу Wi-Fi. 2) Проаналізувати можливі типи загроз і вразливостей та протоколи інформаційної безпеки, що борються з ними в мережах Wi-Fi.
4. Зміст пояснювальної записки: Особливості функціонування стандартів IEEE 802.11 в бездротових технологіях, аналіз загроз та уразливостей бездротових систем зв’язку, технології та методи захисту бездротових мереж
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: Класифікація бездротових технологій за дальністю дії, порівняння QAM в стандартах Wi-Fi 5 та Wi-Fi 6, схема атаки типу «Людина посередині», схема DDoS-атаки

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Особливості функціонування стандартів IEEE 802.11 в бездротових технологіях	12.09.2022-05.10.2022	Виконано
4	Аналіз загроз та уразливостей бездротових систем зв’язку	06.10.2022-15.10.2022	Виконано
5	Технології та методи захисту бездротових мереж	17.10.2022-28.10.2022	Виконано
6	Аналіз методів для генерування паролів	29.10.2022-06.11.2022	Виконано
7	Охорона праці	07.11.2022-12.11.2022	Виконано
8	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Георгій КОНАХОВИЧ
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Анна ШАПОВАЛОВА
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Система забезпечення захисту інформації в бездротових технологіях» містить 84 сторінки, 12 рисунків, 4 таблиці, 20 використаних джерел.

ПРОТОКОЛ, АВТЕНТИФІКАЦІЯ, WEP, WPA, СТАНДАРТ, ШИФРУВАННЯ, ЗАХИСТ, ПАРОЛЬ.

Об’єкт дослідження –. процес забезпечення безпеки бездротових технологій.

Предмет дослідження –. методи забезпечення безпеки в бездротових технологіях.

Мета кваліфікаційної роботи –. підвищення захищеності та надійності бездротових мереж шляхом покращення політик паролю.

Метод дослідження –. метод порівняння, метод синтезу і аналізу, метод класифікації, метод розрахунку.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ……..……... 8
ВСТУП ……..…….…….... 9
РОЗДІЛ 1. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СТАНДАРТІВ IEEE 802.11 В БЕЗДРОТОВИХ СИСТЕМАХ…….……12
1.1. Поняття та застосування технології бездротової мережі Wi-Fi…….12
1.2. Класифікація бездротових мереж……12
1.3. Класифікація стандартів бездротового зв'язку……14
1.3.1. Стандарти сімейства IEEE 802.11……..14
1.3.2. Стандарт 802.11ac……15
1.3.3. Стандарт 802.11ax……16
1.3.4.Wi-Fi EasyMesh……19
1.3.5.Технологія WiMAX……19
1.3.6.Технологія Zigbee…….20
1.3.7.Технологія Bluetooth і BluetoothLowEnergy……21
ВИСНОВКИ ДО РОЗДІЛУ 1……22
РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ ТА УРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ СИСТЕМ ЗВ'ЯЗКУ……..……...23
2.1. Основні типи атак на бездротову мережу……23
2.1.1. Атака типу «Людина посередині»…….23
2.1.2. DDoS атаки…….25
2.1.3. Фальшива точка доступу…….……...……26
2.1.4. Атаки на мережеве обладнання…….…….26
2.2. Уразливості впровадження незашифрованого тексту…….27
2.3. Небезпеки для мобільних пристроїв…….30
ВИСНОВКИ ДО РОЗДІЛУ 2……34
РОЗДІЛ 3. ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ……..35
3.1. Огляд основних технологій захисту бездротових мереж……...……35

3.1.1. Протокол безпеки WEP……...……35
3.1.2. Стандарт IEEE 802.11X……..……37
3.1.3. Стандарт безпеки WPA……...38
3.1.4. Стандарт безпеки WPA2…….……42
3.1.5.Стандарт безпеки WPA3…….……43
3.2. Порівняльна характеристика стандартів безпеки……46
3.3. Методи захисту бездротових мереж зв’язку……48
ВИСНОВКИ ДО РОЗДІЛУ 3……50
РОЗДІЛ 4. АНАЛІЗ МЕТОДІВ ДЛЯ ГЕНЕРУВАННЯ ПАРОЛІВ……51
4.1. Проблеми парольних політик…….51
4.2. Огляд методів для генерування паролів……53
4.3. Порядок покращення методу генерування паролів…….....55
4.4.Зберігання паролів……...……60
ВИСНОВКИ ДО РОЗДІЛУ 4……60
РОЗДІЛ 5. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА……61
5.1. Вплив електромагнітного забруднення на живі організми……..……..61
5.2. Захист від електромагнітного забруднення…….64
5.3. Проблема електронного сміття…….66
ВИСНОВКИ ДО РОЗДІЛУ 5……68
РОЗДІЛ 6. ОХОРОНА ПРАЦІ……..69
6.1. Аналіз умов праці……..69
6.2. Перелік та аналіз шкідливих та небезпечних виробничих чинників……72
6.4. Розробка заходів з охорони праці…….……74
6.5. Пожежна безпека……..76
6.6. Розрахункова частина……..78
ВИСНОВКИ ДО РОЗДІЛУ 6……79
ВИСНОВКИ ……..…….....80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……..……...…82

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard

CRC – Cyclic Redundancy Check

DDoS – distributed denial of servise

DNS – Domain Name System

DSSS – Direct Sequence Spread Spectrum

EAP – Extensible Authentication Protocol

FHSS – Frequency-Hopping Spread Spectrum

ICV – Integrity Checksum Value

IV – Initialization Vector

MIC – Message Integrity Check

MIMO – Multiple Input Multiple Output

OFDM – Orthogonal frequency-division multiplexing

PSK – Pre - Shared Key

RADIUS – Remote Authentication Dial - In User Server

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

UPnP – Universal Plug and Play

VPN – Virtual Private Network

WEP – Wired Equivalent Privacy

WLAN – wireless local area network

WMAN – Wireless Metropolitan Area Network

WPA – Wi-Fi Protected Access

WPAN – wireless personal area network

ЕОМ – Електронно-обчислювальна машина

ЕМП – Електромагнітне поле

ЛЕП – Лінія електропередач

ПК – Персональний комп’ютер

ВСТУП

Актуальність теми. В сучасному світі пристрої бездротових технологій набирають популярності. Кількість бездротових працюючих пристроїв скоро буде рівним кількості людей на землі, оскільки на кожна людина має близько 3-4 пристроїв бездротової мережі, до прикладу мобільні телефони, планшети, ноутбуки та інші. Ці пристрої дуже впливають на наше життя, оскільки в них міститься багато конфіденційних інформації та даних таких як: цифрові документи, доступ до банківських рахунків, електронний цифровий підпис та інші важливі ресурси. Саме тому, питання щодо забезпечення захисту (доступності та цілісності) бездротових систем зв'язку є надзвичайно актуальними. У все більш взаємопов'язаному середовищі інформація піддається зростаючій кількості та різноманітності ризиків. Такі загрози, як шкідливий код, комп'ютерний злом і атаки на відмову в обслуговуванні, стали більш поширеними. Це ускладнює впровадження та підтримку відповідних засобів захисту. Крім того, зловмисники щоразу придумують все нові способи атак на пристрої.

Дослідженню проблеми захищеності бездротових систем зв'язку присвячені роботи Ю.В. Борсуковського, В.Л. Бурячка, П.М. Складанного, В. І. Ніконова, , А.В. Чунарьової, L. Badman, R. Bartz, F. Garzia, L. Hermens та багатьох інших.

За висновками їхніх робіт можна сказати, що одними з головних проблем захищеності бездротових систем зв'язку є: чутливість паролів до різних типів підбору, низька обізнаність користувачів в налаштуванні та некомпетентне використання технічних засобів, наявність досить великої кількості небезпечного ПЗ. Тому всі вище перехована вразливості загрожують не тільки особистим користувачам, а й організаціям.

Мета і завдання дослідження. Мета дипломної роботи полягає в підвищенні захищеності та надійності бездротових мереж шляхом шляхом покращення політик паролю.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Проаналізувати стандарти мереж бездротового доступу Wi-Fi.
2. Проаналізувати основні типи загроз і вразливостей для бездротових систем зв’язку
3. Визначити можливі загрози для мобільних пристроїв.
4. Оглянути та проаналізувати основні протоколи та методи захисту бездротових систем зв’язку
5. Проаналізувати методи для створення та генерування паролів.
6. Вдосконалити один з розглянутих методів генерування паролів.
7. Розглянути способи зберігання паролів.

Об’єктом дослідження є процес забезпечення безпеки в бездротових технологіях.

Предметом дослідження є методи забезпечення безпеки в бездротових технологіях.

Методи досліджень. Для досягнення поставлених завдань в роботі було використано теоретичні методи: аналітичний огляд аналіз наукової літератури, навчально-методичної документації, методи дослідження та порівняння, метод синтезу і аналізу, розрахунок.

Наукова новизна отриманих результатів.

Покращений метод створення випадкових паролів для систем бездротового зв'язку. Тому що його реалізація враховує можливість зіставлення паролів у словникових системах та використовує уніфікований підхід для генерації більш стабільних паролів на основі довжини та набору символів . Може забезпечити порівняно збільшення рівня захищеності систем бездротового зв’язку стандарту IEEE 802.11 від можливої спроби злому в $2{,}53 \cdot 10^4$ разів.

Для зберігання паролів пропонується мати ідентифікаційну картку з QR-кодом, яку можна зберігати у своєму гаманці. Для отримання доступу до своїх паролів (переглядати їх безпосередньо), знадобиться ідентифікаційна картка та сканування її за допомогою захищеного паролем смартфоном.

Практичне значення отриманих результатів.

Метод генерування ускладнених паролів в бездротового технологіях, дозволяє сформувати стійкий до підбору пароль. Крім того дозволяє зменшити час на створення паролю та ймовірність його злому. Для забезпечення більшої безпеки зберігання паролів пропонується мати ідентифікаційну картку з QR-кодом, яку можна зберігати у своєму гаманці. Для отримання доступу до своїх паролів, знадобиться ідентифікаційна картка та сканування її за допомогою захищеного паролем смартфоном. Крім того, картка з qr-кодом є більш довговічною, ніж нотатка, тому її можна зберігати в гаманці чи сумочці, де вона фізично закрита та її важко вкрасти.

РОЗДІЛ 1
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СТАНДАРТІВ IEEE 802.11 В БЕЗДРОТОВИХ ТЕХНОЛОГІЯХ

1.1. Поняття та застосування технології бездротової мережі Wi-Fi

Wi-Fi – технологія бездротової мережі, що ґрунтується на стандартах IEEE 802.11. Wi‑Fi є торговою маркою некомерційної Wi-Fi Alliance. Термін «Wi-Fi» виник у 1990-х роках зі слів «Wireless» плюс «Fi», подібно до Hi-Fi. Wireless Fidelity у перекладі бездротова точність.

Раніше терміном «Wi-Fi» позначали лише технології, що працювали в діапазоні частот 2.4ГГц, проте зараз поширив своє застосування і в інших технологіях бездротових мереж.

Мережа Wi-Fi застосовується для зв’язку і обміну даними між вузлами, при цьому дана система обміну інформацією є дуже гнучкою та подібною до еквівалентної дротової системи, що розташовується в будівлі або відкритій місцевості. Крім того, дана система відзначається можливістю організації публічних точок доступу в місцях великого скупчення людей, до прикладу торгові центри, аеропорти та інші, а також організація тимчасових бездротових систем.

1.2. Класифікація бездротових мереж

В телекомунікаціях стрімко розвиваються бездротові мережі передачі інформації. Ринок має достатньо широкий асортимент обладнання бездротового доступу, а саме для побудови бездротових мереж Wi-Fi, GSM, WiMAX і глобальних мереж.

Для об'єднання великих мереж або на величезні дистанції використовується обладнання зі спрямованими антенами або підсилювачі.

При розгляді бездротових мереж передачі інформації можна виділити основні чотири види, які можна побачити на рисунку 1.

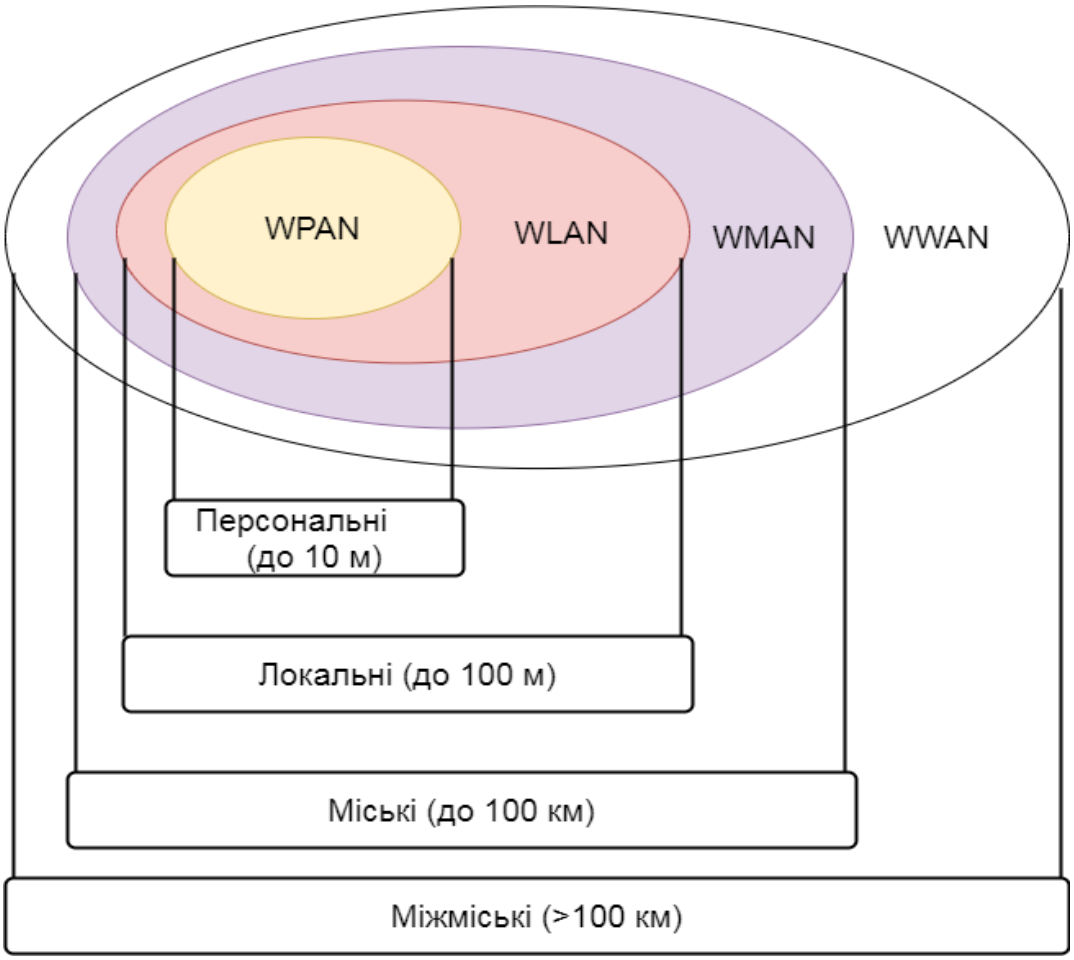


Рис. 1.1. Класифікація бездротових технологій за дальністю дії

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

2. Бездротові локальні мережі (WLAN – wireless local area network) – радіус дії до 100 метрів, але при використанні підсилювачів і напрямлених антен дальність дії може сягати до понад кількох сотень метрів. Їх ще називають Wi-Fi мережами. Головна функція таких систем – розгортання бездротових мереж усередині

приміщень, проте є можливість їх застосування на відкритих майданчиках. Основна послуга – доступ в Internet або корпоративну мережу.

3. Бездротові міські мережі (WMAN - Wireless Metropolitan Area Network) - радіус дії базової станції – до 10 км. З використанням обладнання, яке відноситься до класу фіксованого широкосмугового бездротового доступу (Fixed Broadband 13 Wireless Access, FBWA) здійснюється побудова розподілених бездротових операторських мереж масштабом з місто або величезних корпоративних мереж. До прикладу можна навести технологію WiMAX.

4. Бездротові глобальні мережі WWAN. Глобальні бездротові мережі передачі інформації відображені здебільшого супутниковими системами зв'язку. Сюди можна віднести технологію GPRS [2].

1.3. Класифікація стандартів бездротового зв’язку

1.3.1. Стандарти сімейства IEEE 802.11

Стандарт 802.11a: це був перший стандарт Wi-Fi у серії 802.11. Випущений у 1999 році, він визначив канал бездротової мережі, що працює в діапазоні 5 ГГц, використовуючи ортогональне частотне мультиплексування зі швидкістю передачі даних до 54 Мбіт/с. У той же час використання досить високої несучої частоти обумовлює меншу дальність дії пристроїв, що використовують даний стандарт.

Стандарт 802.11b використовує ту саму частоту 2,4 ГГц, що й оригінальний стандарт 802.11. Він підтримує максимальну теоретичну швидкість 11 Мбіт/с і радіус дії 50 м. Через досить невелику швидкість передачі, цей стандарт має низький рівень безпеки. Зловмиснику може знадобитися менше години для розшифрування ключа мережі та проникнення до локальної мережі.

Стандарт 802.11g використовує ту саму технологію OFDM, що була представлена в 802.11a. Як і 802.11a, він підтримував максимальну теоретичну швидкість 54 Мбіт/с. Але, як і 802.11b, він працював на переповненій частоті 2,4 ГГц (і тому мав ті ж проблеми з перешкодами, що й 802.11b). Завдяки стандарту 802.11g споживачі отримали значне підвищення швидкості та рівня захисту Wi-Fi. У

той же час споживчі бездротові маршрутизатори ставали кращими, з більшою потужністю та кращим покриттям, ніж попередні покоління.

Завдяки стандарту 802.11n Wi-Fi став ще швидшим і надійнішим. Він підтримував максимальну теоретичну швидкість передачі 300 Мбіт/с (і міг досягати до 450 Мбіт/с при використанні трьох антен).

Стандарт 802.11n використовує MIMO (багато входів і множинний вихід), де кілька передавачів/приймачів могли працювати одночасно на одному або обох кінцях зв'язку з одним пристроєм. Це забезпечило значне збільшення даних без потреби у вищій пропускній здатності чи потужності передачі. 802.11n працює як у діапазонах 2,4 ГГц, так і в 5 ГГц [1].

Для наглядності та розгляду потенціалу і функціональної спроможності зазначених вище стандартів бездротових мереж передачі інформації наведено таблицю, в якій наведені такі параметри як, швидкість передачі даних в кожній технології, дальність дії, частотний діапазон та технологія модуляції, використовувана певним стандартом.

Таблиця 1.1

Порівняльна таблиця стандартів Wi-Fi

Стандарт	Максимальна швидкість передачі, Мбіт/с	Дальність дії, м	Технології шифрування	Частотний діапазон	Технологія модуляції
802.11a	54	10-100	WEP	5ГГц	OFDM
802.11b	11	30-300	WEP	2,4ГГц	DSSS
802.11g	54	30-300	WEP, WPA, WPA2	2,4ГГЦ	OFDM
802.11n	540	50-400	WEP, WPA, WPA2, AES	2,4ГГЦ/ 5ГГц	OFDM

У реальних умовах швидкість передачі та площа зони покриття мережі залежать від створених іншими пристроями ступенями завантаження мережі Wi-Fi, наявності перешкод (і матеріалів, з яких вони виготовлені) та інших факторів.

Багато клієнтських утиліт, що поставляються виробниками разом з Wi-Fi-адаптерами, а також утиліти операційної системи Windows, при підключенні по Wi-Fi відображають саме «теоретичну» пропускну здатність, а не реальну швидкість передачі даних, вводячи користувачів в оману.

Тому, максимальна реальна пропускна здатність виявляється приблизно в 3 рази нижче, ніж та, що вказана в специфікаціях до пристрою або відповідному стандарту IEEE групи 802.11 (стандарти технології Wi-Fi).

1.3.2. Стандарт 802.11ac

Стандарт 802.11ac високошвидкісний Wi-Fi зі швидкістю від 433 Мбіт/с до кількох Гбіт/с. Щоб досягти такої продуктивності, 802.11ac:

- Працює виключно в діапазоні 5 ГГц;
- Підтримує до восьми просторових потоків (у порівнянні з чотирма потоками 802.11n);
- Ширина каналу до 80 МГц.

Використовується технологія під назвою формування променю. За допомогою формування променю антени в основному передають радіосигнали, тому вони спрямовані на певний пристрій.

Іншим значним досягненням 802.11ac став багатокористувацький MIMO (MU-MIMO). Хоча MIMO спрямовує кілька потоків до одного клієнта, MU-MIMO може спрямовувати просторові потоки до кількох пристроїв одночасно. Хоча MU-MIMO не збільшує швидкість жодного клієнта, він може збільшити загальну пропускну здатність усієї мережі [3].

1.3.3. Стандарт 802.11ax

Стандарт Wi-Fi останнього покоління – Wi-Fi 6. Найбільше, що варто знати про найновіший стандарт, це те, що Wi-Fi 6:

- Має покращення, подібні до 5G;
- Пропонує вищу швидкість передачі даних і ємність до 9,6 Гбіт/с;
- Пропонує кращу підтримку спектру 2,4 ГГц і 5 ГГц;
- Пропонує збільшення багатокористувацьких, багаторазових входів, кількох виходів (MU-MIMO) з 4 x 4 до 8 x 8;
- Загалом обіцяє кращу та швидшу роботу;
- Дозволяє підключати ще більше пристроїв.

На відміну від попередніх стандартів, Wi-Fi 6 дозволяє одному маршрутизатору обслуговувати більше антен. Це означає, що один маршрутизатор може підключатися до кількох пристроїв. Wi-Fi 6 розроблено, щоб зробити бездротовий Інтернет кращим удома та в громадських місцях [4].

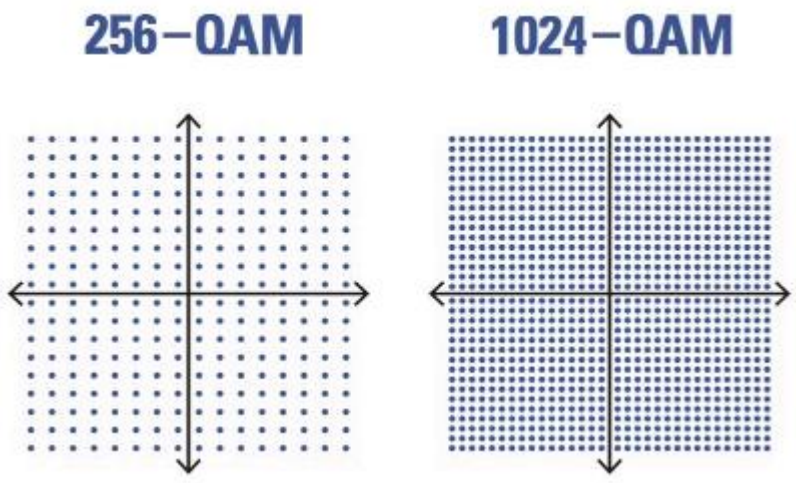


Рис. 1.2. Порівняння QAM в стандартах Wi-Fi 5 та Wi-Fi 6

В 1024-QAM збільшена довжина кожного символу кодування з 8 біт (в 256-QAM на стандарті Wi-Fi 5) до 10 біт, це в свою чергу збільшує швидкість передачі даних та ефективність використання спектра щонайменше на 25%, оскільки кожен пакет міститиме більше даних.

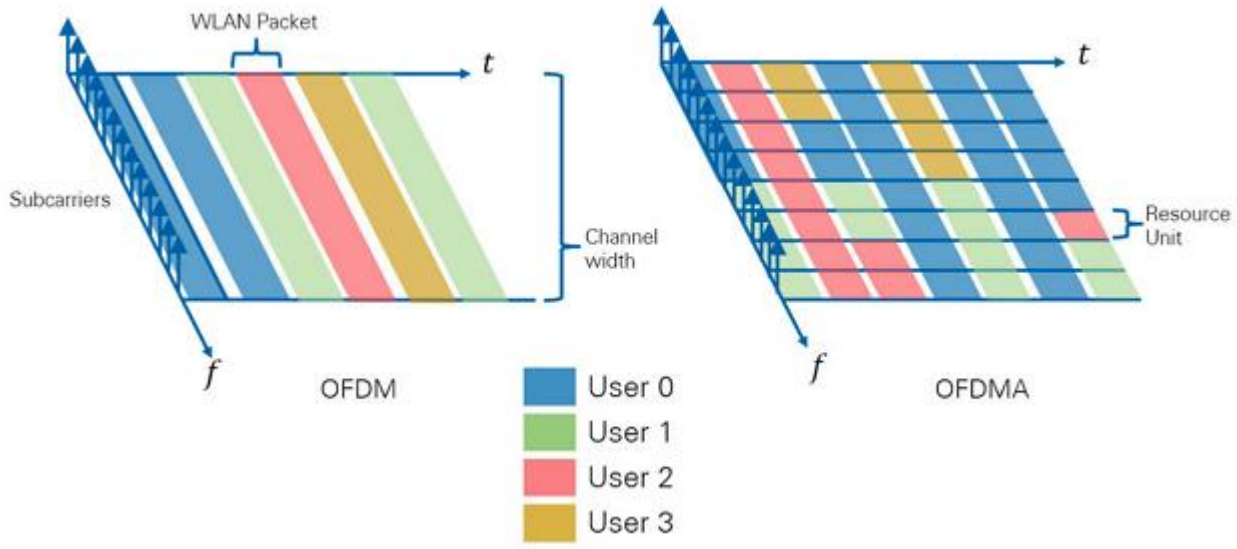


Рис. 1.3. Порівняння OFDM та OFDMA

У Wi-Fi 6 також додано режим OFDMA (Orthogonal Frequency Division Multiple Access, множинний доступ з ортогональним частотним розділенням каналів) для покращення спектральної ефективності. OFDMA забезпечує можливість встановлення з'єднання між точкою доступу та кількома користувачами одночасно, а також використання одного і того.

Даний стандарт передбачає, що пристрої, які його підтримують зможуть в чотири рази швидше скачувати інформацію та в 6 разів швидше передавати її на віддалений сервер у порівнянні з попередніми стандартами.

Таблиця 1.2

Порівняння стандартів Wi-Fi 5 та Wi-Fi 6

Параметр	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)
Частота	5 ГГц	2.4 ГГц та 5 ГГц
Пропускна здатність	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80, 160 МГц
Доступ	OFDM	OFDMA

Закінчення таблиці 1.2

Антени	MU-MIMO (4*4)	MU-MIMO (8*8)
Модуляція	256QAM	1024QAM
Швидкість передачі	3.5 Гбіт/с	9.6 Гбіт/с
Максимальна кількість точок доступу	4	8

1.3.4. Wi-Fi EasyMesh

Для розширення зони покриття бездротового роутера на великій території (квартира, котедж, офіс, виставковий зал), як правило, додатково встановлюються точки доступу або повторювачі.

Незважаючи на розширення зони покриття, таке рішення має наступні недоліки:

- Зниження продуктивності мережі через неправильне планування мережі
- З’являється потреба в налаштуванні кілька бездротових пристроїв
- Знижена швидкість, велика затримка та можливість втрати зв’язку, коли клієнт перемикається між точками доступу.

Функція EasyMesh дозволяє будувати високопродуктивні інтелектуальні розподілені бездротові мережі на основі маршрутизаторів з підтримкою централізованого управління. Нині існує можливість об’єднати до 6 маршрутизаторів – 1 контролер і 5 агентів в Mesh мережі.

1.3.5. Технологія WiMAX

Технологія WiMAX — це технологія бездротового широкосмугового зв’язку, заснована на стандарті IEE 802.16, що забезпечує високу швидкість передачі даних на великій території. Вона дозволяє передавати дані зі швидкістю від 30 до 40 Мбіт на секунду.

Система зв'язку WiMAX забезпечує BWA (широкосмуговий бездротовий доступ) до 50 кілометрів для фіксованих станцій, а також для мобільних станцій від 5 до 15 км. WiMAX замінює DSL-послуги та кабелі, надаючи універсальний доступ до Інтернету. Архітектура, яка використовується в WiMAX, — це «точка-багатоточка», що є ідеальною технікою для операторів, щоб забезпечити широкосмуговий зв’язок у місцях, де дротове з’єднання є дорогим і складним. З’єднання WiMAX також можна спрямувати або з’єднати мостом до стандартної дротової або бездротової локальної мережі.

Робота WiMAX подібна до Wi-Fi, але на високих швидкостях і більшій відстані для кількох користувачів. Це бездротове широкосмугове з’єднання здатне надавати послуги навіть у важкодоступних місцях і здатне долати фізичні межі зазвичай дротової інфраструктури.

1.3.6. Технологія ZigBee

ZigBee — це бездротова технологія, розроблена як стандарт підключення відкритого глобального ринку для задоволення унікальних потреб недорогих і малопотужних бездротових мереж передачі даних IoT. Стандарт підключення ZigBee працює на основі радіоспецифікації фізичної плати IEEE 802.15.4 і працює в неліцензійних радіодіапазонах, включаючи 2,4 ГГц, 900 МГц і 868 МГц.

Протокол ZigBee 3.0 призначений для передачі даних через радіочастотне середовище з високим шумом, яке є поширеним у комерційних і промислових додатках. Версія 3.0 базується на існуючому стандарті зв’язку ZigBee, але уніфікує профілі додатків для певного ринку, щоб дозволити всім пристроям бути бездротовим підключенням до однієї мережі, незалежно від їх ринкового призначення та функції. Підключення мереж ZigBee 3.0 до IP-домену відкриває можливість бездротового моніторингу та керування за допомогою радіопристроїв, таких як смартфони та планшети в LAN або WAN, включаючи Інтернет, і втілює справжній Інтернет речей.

Функції протоколу ZigBee включають:

- Підтримка кількох мережевих топологій, таких як точка-точка, мережі «точка-багато точок» і Mesh
- Низький робочий цикл – забезпечує тривалий термін служби батареї
- Низька затримка
- Розширений спектр прямої послідовності (DSSS)
- До 65 000 вузлів на мережу
- 128-бітове шифрування AES для безпечного з'єднання даних
- Уникнення зіткнень, повторні спроби та підтвердження

1.3.7. Технологія Bluetooth і Bluetooth Low Energy

Bluetooth і Bluetooth Low Energy (BLE) — бездротові технології, які використовуються для передачі даних на короткі відстані. Технологія часто використовується в невеликих пристроях, які підключаються до телефонів і планшетів користувачів. Наприклад, технологія використовується в багатьох акустичних системах.

Bluetooth працює за принципом FHSS (Frequency-Hopping Spread Spectrum). Цей принцип полягає в тому, що передавач розбиває дані на пакети та передає їх за допомогою псевдовипадкового алгоритму скачкоподібної переналаштування частоти (1600 раз в секунду).

BLE поєднує в собі зручність класичного Bluetooth і додає значно нижче енергоспоживання. Таким чином, він може конкурувати з ZigBee за час автономної роботи. BLE не може конкурувати з ZigBee з точки зору розміру мережі, але для підключення одного пристрою до пристрою це можна порівняти. BLE лише нещодавно почав набирати обертів. Цю технологію вперше представив виробник смартфонів Nokia у 2006 році, але вона не стала частиною стандарту Bluetooth до 2010 року. Використовується в таких апаратних засобах, як фітнес-трекери, смарт-годинники та інші підключені пристрої для бездротової передачі даних без значного зниження заряду акумулятора в телефоні користувача [6].

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі було розглянуто класифікацію бездротових мереж. Серед яких найбільш популярною та використовуваною є (WLAN - wireless local area network), іншою назвою яких є Wi-Fi. Головна функція таких систем – розгортання бездротових мереж усередині приміщень, проте є можливість їх застосування на відкритих майданчиках. Основна послуга – доступ в Internet або корпоративну мережу.

Також було розглянуто основні стандарти бездротового зв'язку серед яких стандарти сімейства IEEE 802.11. Для наглядності та розгляду потенціалу і функціональної спроможності стандартів бездротових мереж передачі інформації наведено таблицю, в якій наведені такі параметри як, швидкість передачі даних, дальність дії, частотний діапазон та технологія модуляції. Стандарт IEEE 802.11n має найкращі характеристики у порівнянні з іншими стандартами., саме тому він є найбільш застосованим для організації в житлових будинках та на відкритій місцевості.

Крім того, було проаналізовано роботу таких стандартів як Wi-Fi 5 та Wi-Fi 6. На відміну від попередніх стандартів, Wi-Fi 6 дозволяє одному маршрутизатору обслуговувати більше антен, пропонує вищу швидкість передачі даних і ємність та загалом обіцяє кращу та швидшу роботу.

Було розглянуто технологію BLE, яка поєднує в собі зручність класичного Bluetooth і додає значно нижче енергоспоживання. Таким чином, дана технологія може конкурувати з технологією ZigBee за час автономної роботи. Проте BLE не може конкурувати з ZigBee з точки зору розміру мережі.

РОЗДІЛ 2
АНАЛІЗ ЗАГРОЗ ТА УРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ СИСТЕМ ЗВ’ЯЗКУ

2.1. Основні типи атак на бездротову мережу

Значні проблеми безпеки бездротових систем зв’язку, незважаючи на їхні численні переваги, є одним із головних їхніх недоліків. У зв'язку з цим вони значно поступаються дротовому з'єднанню. Це пов'язано з тим, що для злому дротової мережі, зловмиснику потрібен прямий доступ до кабелю, який набагато складніше отримати, ніж перехопити радіосигнал за допомогою спеціальних пристроїв. Крім того, часто бездротові мережі працюють навіть без базового захисту паролем.

Отримання доступу до локальної бездротової мережі дає зловмисникам можливість викрадення конфіденційної інформації та персональних даних, поширення шкідливих програм, та інших маніпуляцій.

Існує кілька основних типів атак, які загрожують безпеці бездротової комп'ютерної мережі:

- DDoS-атаки;
- помилкова точка доступу;
- «людина посередині»;
- атаки на мережеве обладнання.

Кожен із цих типів може використовуватися хакерами в певних умовах в залежності від мети атаки.

2.1.1. Атака типу «Людина посередині»

«Людина посередині», або Man-in-the-Middle, одна з найбільш типових атак. Цей спосіб найчастіше використовується для підключення до точок доступу, які не захищені паролем. Так як сигнал в таких мережах транслюється без шифрування, зловмисник може легко перехопити його, лише за допомогою звичайного ноутбука або комп'ютера з адаптером Wi-Fi. Однак, є ймовірність, що хакер може

підключитися до захищеної паролем мережі за допомогою спеціальної програми для злому паролів методом підбору.

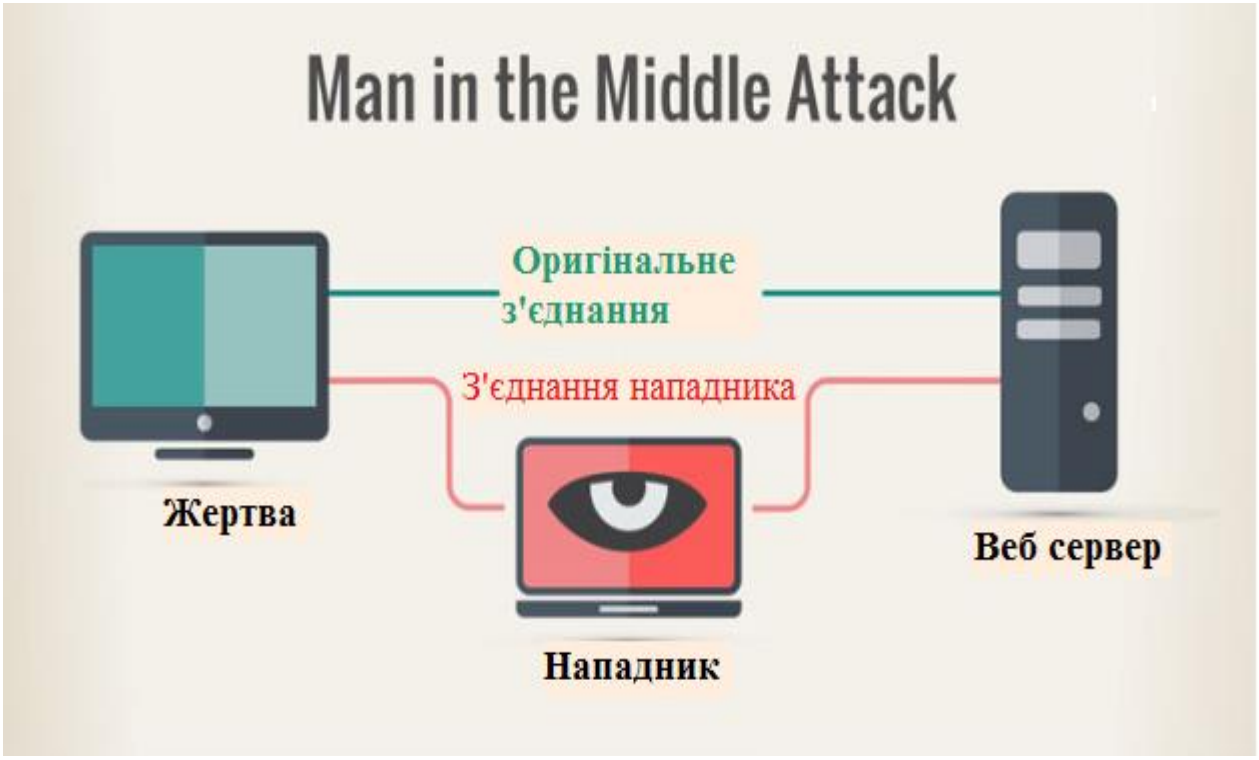


Рис. 2.1. Схема атаки типу «Людина посередині»

«Прослуховування» також називають пасивною атакою. Виконується за допомогою спеціального програмного забезпечення, яке після отримання доступу до локальної мережі відображає весь трафік користувача на комп'ютері зловмисника. Це може бути історія відвідування сайтів, введені логіни та паролі, дані пластикових карток та інша конфіденційна інформація. Маніпуляційні атаки називають активними. У цьому випадку хакер отримує можливість не тільки крадіжки особистих даних користувача, а й маніпуляції його пристроєм через бездротову мережу. Наприклад, за допомогою спеціального програмного забезпечення на комп'ютер користувача можна відправити команду перенаправлення браузера від імені точки доступу на певну сторінку в Інтернеті. На цій сторінці комп'ютер заражається вірусами або іншим шкідливим програмним забезпеченням [9].

2.1.2. DDoS атаки

Ще один поширений тип загрози, який слід враховувати. Стандарти безпеки бездротової мережі – DDoS-атаки або відмова обслуговування. Мета зловмисників – порушити роботу локальної мережі, де він не може бути повністю використаний. Напад можна здійснити на програмному і апаратному рівнях. У першому випадку використовують хакери наявні вразливості програмного забезпечення. Атака на апаратному рівні здійснюється шляхом заповнення системи запитами, що призводить до її виснаження ресурсів (дисковий простір, час ЦП, пропускна здатність і тощо).

DDoS-атаки на програмному рівні найчастіше здійснюються через уразливості в протоколах. Вони можуть призвести до повної втрати продуктивності підключеного до мережі пристрою. Наприклад, може зависати комп'ютер, змінюватися конфігурації в операційній системі або вона може бути пошкоджена.

При атаці на апаратному рівні зловмисник прагне досягти збою каналу зв'язку. Це досягається шляхом посилки масиву потоки безглуздих даних, які перевантажують канал, або створення потужних перешкод. Перешкоди створюються за допомогою спеціальних електромагнітних генераторів випромінювання.

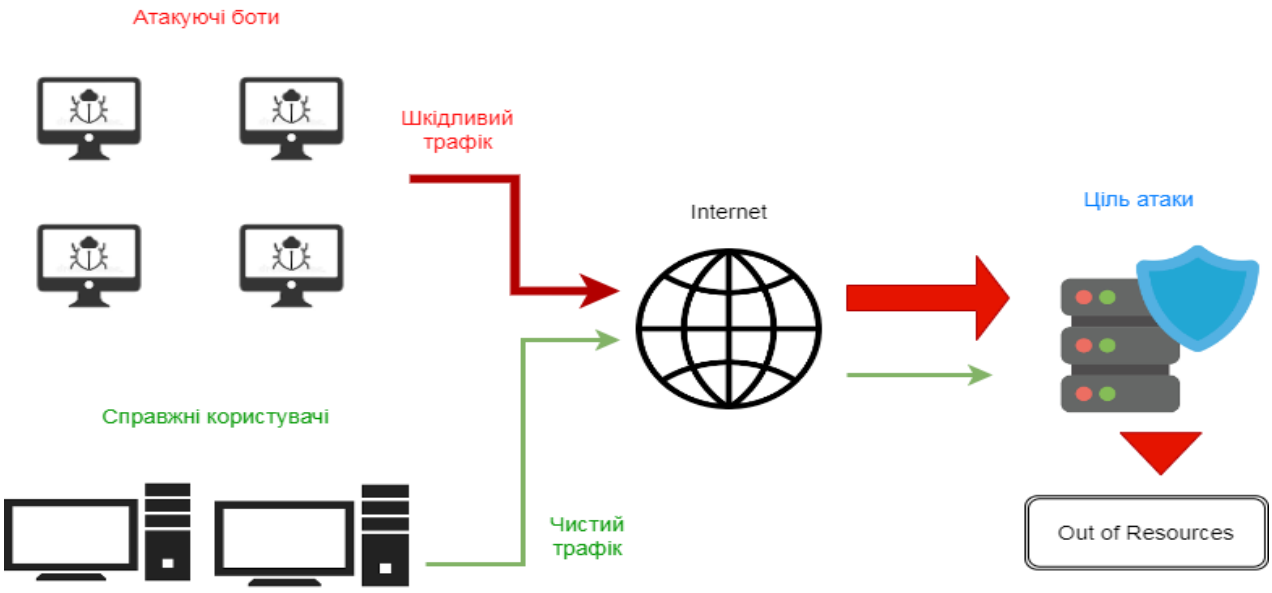


Рис. 2.2. Схема DDoS-атаки

Відмова в обслуговуванні програми стає можливою, якщо вразливі місця програми призводять до отримання контролю над машиною (наприклад, через переповнення буфера обміну). Програма стане недоступною через брак ресурсів або збій. Уразливість програми також може бути використана для порушення продуктивності інших компонентів системи, таких сервер автентифікації.

Відмова в обслуговуванні мережі базується на особливостях стека протоколів TCP/IP. Якщо атака виконується одночасно з великої кількості хостів, то говорять про розподілену атаку на відмову в обслуговуванні - DDoS-атаку (Distributed Denial of Service). У деяких випадках виникає DDoS-атака при звичайній дії в Інтернеті, наприклад, популярний інтернет-ресурс містить посилання на сайт, розміщений на не дуже продуктивному сервері (так званий ефект косої точки). Великий наплив користувачів призводить до перевищення допустимого навантаження на сервер, і він дуже швидко стає недоступним або важкодоступним в результаті перевантаження.

2.1.3. Фальшива точка доступу

Цей тип атаки використовується зловмисниками в місцях, де є громадські точки доступу, наприклад, в кінотеатрі, в транспорті і т. д. Хакер через смартфон або ноутбук створює точку доступу без пароля, яка маскується під легітимну.

Користувачі при спробі підключитися до публічної Wi-Fi бачать у списку доступних мереж підроблену точку доступу та підключаються до неї. Як результат зловмисник перехоплює весь переданий трафік, в тому числі конфіденційні дані.

Часто зловмисники за допомогою помилкових точок можуть придушити легальний сигнал точки доступу за допомогою спеціального обладнання. Це значно збільшує кількість жертв, що були підключені.

2.1.4. Атаки на мережеве обладнання

Неправильно налаштовані точки доступу та інше мережеве обладнання з недостатньо ефективним захистом часто стає каналом для проникнення хакерів в локальну бездротову мережу. До того ж бездротові мережі з часом переходять на

дротові. Тому злом мережевого обладнання становить загрозу для безпеки дротових мереж і є дуже важливим правильне налаштування мережевих пристроїв відповідно до рекомендацій виробника [7].

2.2. Уразливості впровадження незашифрованого тексту

Кілька недоліків реалізації можна використати для легкого впровадження кадрів у безпечну мережу Wi-Fi. Зокрема, зловмисник може ввести незашифрований кадр Wi-Fi, виконавши ретельне конструювання цього кадру. Наприклад, цим можна зловживати для перехоплення клієнтського трафіку, змусивши клієнта до використання зловмисного сервера DNS, (хоча перехоплений трафік може мати інший рівень захисту). У відношенні до маршрутизаторів, цим також можна зловживати для обходу NAT/брандмауера, дозволяючи зловмиснику згодом атакувати пристрої в локальній мережі Wi-Fi (наприклад, атака на застарілу машину з Windows 7).

Деякі пристрої Wi-Fi приймають будь-який незашифрований кадр, навіть якщо пристрій підключено до безпечної мережі Wi-Fi. Це означає, що зловмиснику не потрібно робити нічого особливого. Це уразливість торкнулася двох із чотирьох перевірених маршрутизаторів, кілька пристроїв IoT і кілька смартфонів [8].

Крім того, багато модулів Wi-Fi Windows помилково приймають кадри з відкритим кодом тексту, коли вони розбиті на декілька (незашифрованих) фрагментів.

До того ж , деякі пристрої приймають агреговані кадри з відкритим текстом, схожі на повідомлення рукостискання. Зловмисник може скористатися цим, надіславши агрегований кадр, початок якого нагадує повідомлення рукостискання, а другий підкадр містить пакет, який зловмисник хоче запровадити. Уражений пристрій спочатку інтерпретує цей кадр як повідомлення рукостискання, але згодом обробить його як агрегатний фрейм. У певному сенсі одна частина коду думатиме, що кадр — це повідомлення рукостискання, і прийме його, навіть якщо він не

зашифрований. Натомість інша частина коду розглядатиме його як агрегований фрейм і обробить пакет, який зловмисник хоче ввести.

Наостанок, деякі пристрої сприймають фрагменти трансляції як нормальні нефрагментовані кадри. Проблемніше те, що деякі пристрої можуть отримувати фрагменти трансляції навіть в незашифрованому вигляді. Зловмисник може використовувати це для введення пакетів, інкапсулюючи їх у другий фрагмент широкомовного кадру з відкритим текстом.

Першим недоліком дизайну є функція агрегації кадрів Wi-Fi. Це збільшує швидкість і пропускну здатність мережі для об'єднання малих кадрів у більший агрегований кадр. Для реалізації цієї функції заголовок кожного кадру містить прапорець, який вказує, чи містять транспортовані (зашифровані) дані один або об'єднаний кадр. Це показано на малюнку нижче:

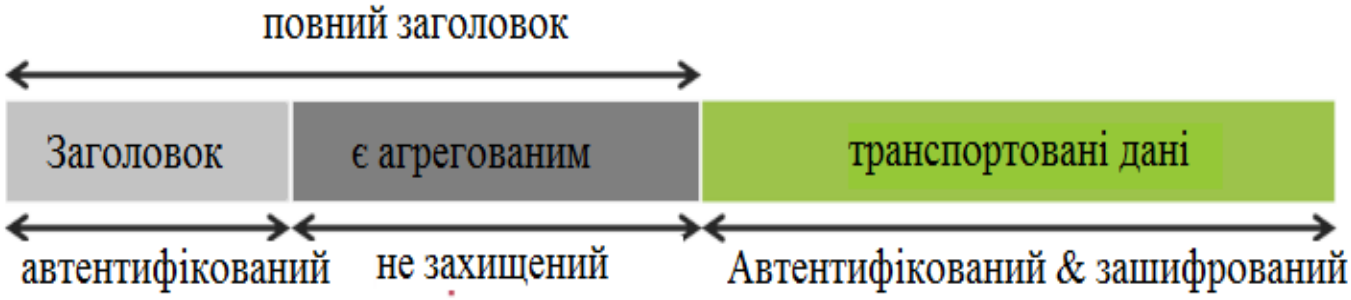


Рис. 2.3. Процес агрегації кадрів Wi-Fi

На жаль, цей «агрегований» прапор не автентифікований і може бути змінений зловмисником, це означає, що жертва може бути обманом оброблена зашифрованими транспортними даними ненавмисно. Зловмисник може зловживати цим для впровадження довільних мережевих пакетів, обманом змушуючи жертву підключитися до свого сервера, а потім установлює позначку «агреговано» для ретельно вибраних пакетів. Майже всі протестовані пристрої були вразливі до цих нападів. Можливість вставляти пакети, у свою чергу, може бути використана для перехоплення трафіка жертви, змушуючи її використовувати шкідливий DNS сервер. Цей недолік конструкції можна виправити шляхом перевірки дійсності прапора «агрегований». Стандарт Wi-Fi вже містить функцію аутентифікації для

цього прапора, а саме вимога кадрів SPP A-MSDU, але цей захист не має зворотної сумісності та не підтримується на практиці. Ймовірність нападу також можна зменшити шляхом використання спеціального патча, хоча нові атаки можуть залишитися можливими.

Другий недолік дизайну - функція фрагментації кадру Wi-Fi. Ця функція покращує надійність з'єднання, розбиваючи великі кадри на менші фрагменти. Причому кожен фрагмент, що належить одному кадру зашифровано тим самим ключем. Однак одержувачі не зобов'язані робити перевірку і мають самі зібрати фрагменти, розшифровані за допомогою інших ключів. У рідкісних випадках цим можна зловживати для ексфільтрації даних. Це досягається змішуванням фрагментів, зашифрованих різними ключами.

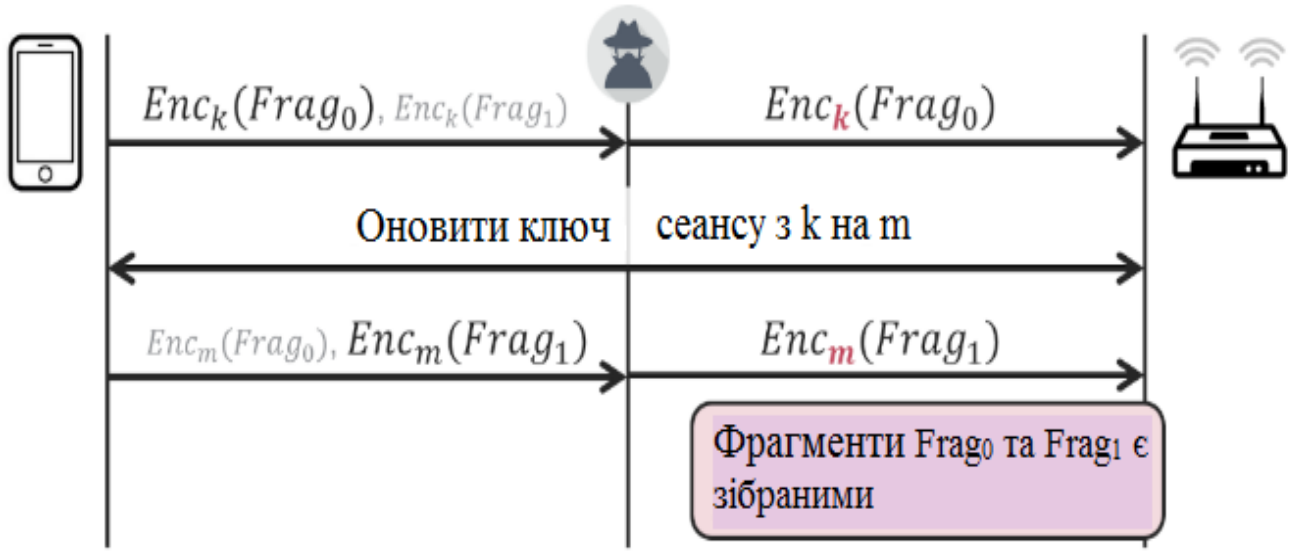


Рис. 2.4. Функція фрагментації кадру Wi-Fi

На наведеному вище малюнку перший фрагмент, отриманий точкою доступу розшифровується за допомогою ключа, відмінного від другого фрагмента. Тим не менш жертва знову збере обидва фрагменти. На практиці це дозволяє зловмиснику фільтрувати вибрані дані клієнтів. Цей недолік конструкції можна виправити шляхом зворотної сумісності. Та лише шляхом повторного збирання фрагментів, які

були розшифровані за допомогою того самого ключа. Так як напад можливий лише в рідкісних випадках така атака вважається теоретичною атакою.

Третім недоліком конструкції також є функція фрагментації Wi-Fi. Проблема полягає в тому, що коли клієнта відключено від мережі Wi-Fi, пристрій може не видаляти незмонтовані фрагменти з пам'яті. Цим можна зловживати схожими на точки доступу мережами, такими як eduroam і govroam, а також проти корпоративних мереж, де користувачі не довіряють один одному. У цих випадках деякі дані, надіслані жертвою, можуть бути вкрадені. Це досягається шляхом введення шкідливого фрагмента в пам’ять (тобто кеш фрагменти) точки доступу. Коли жертва підключається до точки доступу та надсилає фрагментований кадр, вибрані фрагменти буде об’єднано (тобто повторно зібрано) із вбудованим фрагментом зловмисника.

2.3. Небезпеки для мобільних пристроїв

На сьогодні кількість людей, що користуються мобільними пристроями зростає щоденно, разом із тим збільшується кількість атак на них, та знаходяться все нові способи злому та крадіжок персональної інформації та інших даних на смартфоні.

Однією з найпоширенішою небезпекою для мобільних пристроїв можна назвати соціальну інженерію. Соціальна інженерія – це використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації. Суть цього методу полягає в тому, що зловмисник намагається отримати цікаву для нього інформацію шляхом встановлення контакту з особою, яка так чи інакше володіє необхідною інформацією (під час телефонної розмови, поштового листування, конфіденційної розмови в кафе тощо). Зі стрімким розвитком соціальних мереж цей спосіб доступу до конфіденційної інформації став дуже популярним.

Фішинг — це форма соціальної інженерії. Метою такого шахрайства є отримання ідентифікаційних даних користувача. Це включає викрадення паролів,

номерів кредитних карток, банківських рахунків та іншої конфіденційної інформації. Фішинг здійснюється за допомогою підроблених повідомлень електронною поштою від банків, провайдерів, платіжних систем та інших організацій про те, що з якихось причин одержувачу терміново необхідно передати/оновити персональні дані. Причини можуть бути різними. Це може бути втрата даних, збій системи тощо. Зазвичай фішингові сайти працюють недовго (в середньому 5 днів). Оскільки антифішингові фільтри швидко отримують інформацію про нові загрози, фішерам доводиться реєструвати все більше сайтів. Їх зовнішній вигляд збігається з офіційним сайтом, під яким шахраї намагаються підробити їх сайт. Найчастіше жертвами фішингу стають користувачі електронних платіжних систем, аукціонів, електронної пошти, а крім того, користувачі соціальних мереж (twitter, facebook тощо) [12].

Spear Phishing (спрямований фішинг). Це поєднання поширених методів фішингу та соціальної інженерії, спрямованих проти однієї особи чи цільової групи. Щоб атака була успішною, вона повинна бути дуже добре підготовлена, щоб не викликати підозри. Зловмисник збирає максимум інформації про конкретну особу (групу осіб). Дуже часто такі атаки спрямовані проти фінансових установ. Зловмисник використовує зібрану особисту інформацію та готує електронний (іноді паперовий) лист таким чином, щоб він виглядав достовірним і змушував людину відповісти та надати свої конфіденційні дані (логіни та паролі).

Останнім часом для організації та реалізації DDoS-атаки на мережевий ресурс дуже часто використовується механізм соціальної інженерії, коли зловмисники провокують користувачів ресурсу на певні дії, пов’язані з розсилкою повідомлень (так званих «листів щастя» або « чарівні літери», уявні попередження про шкідливі програми, події та необхідність сповістити про це інших користувачів тощо). У цьому випадку чесні користувачі, якщо грають за правилами зловмисників (тобто надсилають повідомлення, отримані зловмисниками), мимоволі стають співучасниками DDoS-атаки на мережевий ресурс.

Найкращий захист від фішингу та інших атак соціальної інженерії — це вміння виявляти підозрілі фішингові електронні листи та SMS-повідомлення та

взагалі не відкривати їх. Зменшення кількості людей, які мають доступ до конфіденційних даних або систем, також може допомогти захистити від атак соціальної інженерії, оскільки це зменшує кількість точок доступу, через які зловмисники можуть отримати доступ до критично важливих систем або інформації.

Ще однією небезпекою є використання загальнодоступних мереж Wi-Fi, які як правило, менш безпечні, ніж приватні мережі, тому що немає способу дізнатися, хто налаштував мережу, як (або чи) вона захищена за допомогою шифрування, або хто зараз отримує до неї доступ або контролює її.

Наприклад, кіберзлочинці часто встановлюють мережі Wi-Fi, які виглядають справжніми, але насправді є фасадом для захоплення даних, які проходять через їхню систему (атака «людина посередині»).

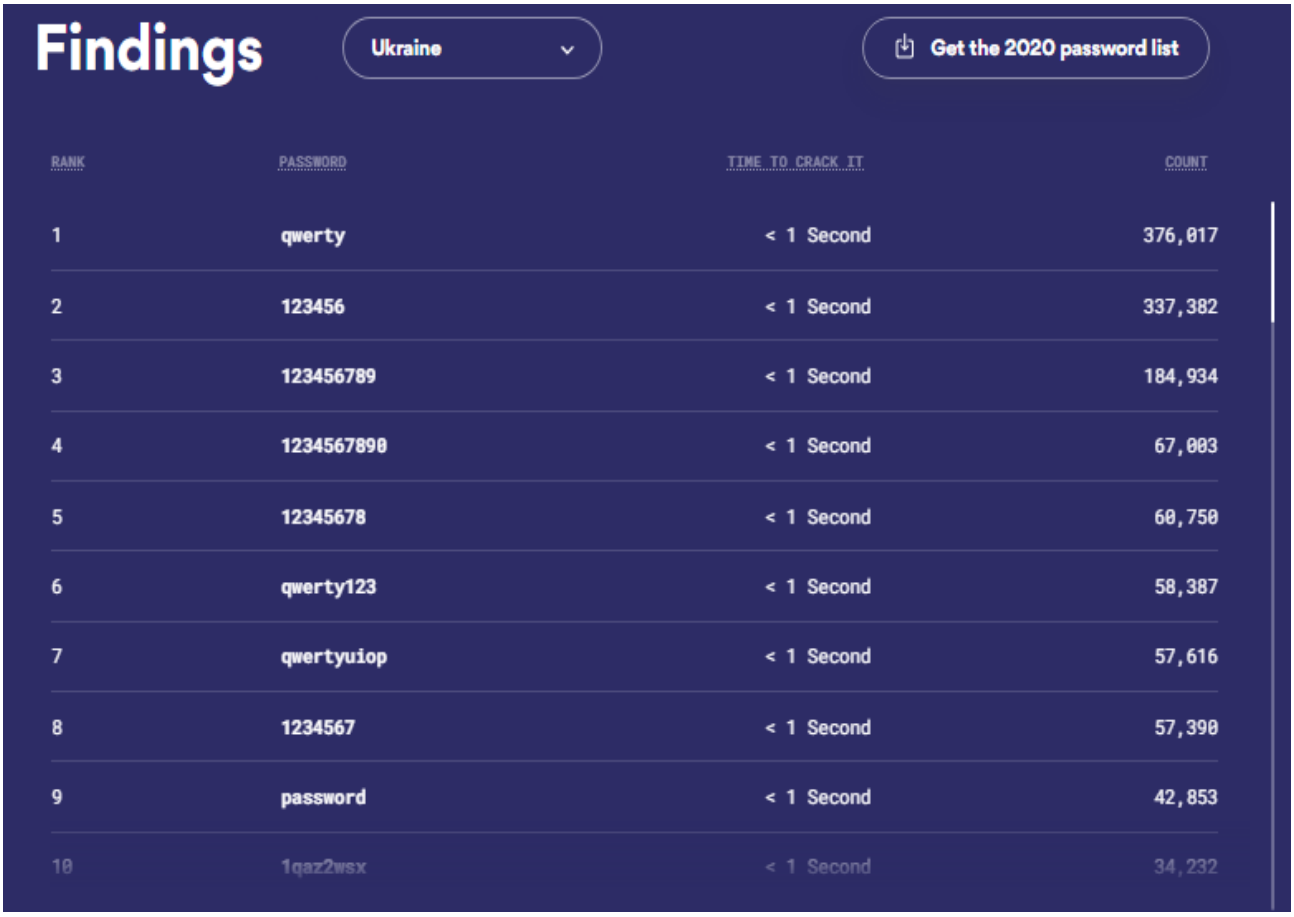
Найкращий спосіб захисту від загроз через загальнодоступні мережі Wi-Fi — це використання VPN для доступу до систем або файлів на пристрої. Це забезпечить конфіденційність і безпеку сеансу, навіть якщо при використанні громадської мережі для доступу до систем. Також не рекомендується при підключенні до публічної мережі передати будь-яку конфіденційну або фінансову інформацію.

Мабуть, однією з най розповсюдженою загрозою не тільки для мобільних, а й пристроїв в цілому є використання ненадійних паролів, що може привезти до злому пристрою та як наслідок втрати особистих даних.

Як показало дослідження Balbix у 2020 році, 99% опитаних людей повторно використовували свої паролі між робочими обліковими записами або між робочими та особистими обліковими записами. На жаль, паролі, які використовуються повторно, також дуже часто є слабкими. Наприклад, дослідження Google у 2019 році показало, що 59% опитаних людей використовували ім’я або день народження у своєму паролі [10].

Розробник сервісів для безпеки в Інтернеті Nord Security опублікувала рейтинг найпоширеніших користувацьких паролів 2021-го року, як в Україні, так у світі [11].

На рисунку нижче показано найпопулярніші паролі, які були використані користувачами з України. Зазначається, що перелічені нижче паролі можна зламати за 1 секунду.



RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	qwerty	< 1 Second	376,017
2	123456	< 1 Second	337,382
3	123456789	< 1 Second	184,934
4	1234567890	< 1 Second	67,003
5	12345678	< 1 Second	60,750
6	qwerty123	< 1 Second	58,387
7	qwertyuiop	< 1 Second	57,616
8	1234567	< 1 Second	57,390
9	password	< 1 Second	42,853
10	1qaz2wsx	< 1 Second	34,232

Рис. 2.5. Рейтинг найбільш використовуваних паролів в Україні

Пароль із 12 знаків, включаючи комбінацію великих і маленьких літер, цифр та символів, вважаються більш надійними для захисту своїх аккаунтів. Використання більше ніж одного фактора автентифікації (багатофакторна автентифікація або MFA) для доступу до мобільних програм також допоможе зменшити ризик того, що зловмисники зможуть отримати доступ до ваших систем, оскільки їм потрібно буде підтвердити свою особу за допомогою додаткових факторів автентифікації для входу.

Нарешті, впровадження автентифікації без пароля допоможе повністю усунути ризики, пов’язані з паролем. Наприклад, у випадку викрадення мобільного пристрою або незаконного доступу до нього сканування обличчя як

основного (або додаткового) фактора автентифікації може запобігти несанкціонованому доступу.

ВИСНОВКИ ДО РОЗДІЛУ 2

В даному розділі було розглянуто основні загрози та вразливості для бездротових мереж. Загрози пов'язані з тим, що для злому дротової мережі, зловмиснику потрібен прямий доступ до кабелю, який набагато складніше отримати, ніж перехопити радіосигнал за допомогою спеціальних пристроїв. Крім того, часто бездротові мережі працюють навіть без базового захисту паролем.

Серед основних типів атак, які загрожують безпеці бездротової комп'ютерної мережі можна виділити: DDoS-атаки; помилкова точка доступу; «людина посередині»; атаки на мережеве обладнання.

Були розглянуті та досліджені найпоширеніші загрози безпеки з якими стикаються користувачі мобільних пристроїв. Однією з найпоширенішою небезпекою для мобільних пристроїв можна назвати соціальну інженерію. Найкращий захист від фішингу та інших атак соціальної інженерії — це вміння виявляти підозрілі фішингові електронні листи та SMS-повідомлення та взагалі не відкривати їх. Зменшення кількості людей, які мають доступ до конфіденційних даних або систем може допомогти захистити від атак.

Однією з най розповсюдженою загрозою не тільки для мобільних, а й пристроїв в цілому є використання ненадійних паролів, що може привезти до злому пристрою та як наслідок втрати особистих даних. Використання більше ніж одного фактора автентифікації (багатофакторна автентифікація або MFA) для доступу до мобільних програм допоможе зменшити ризик того, що зловмисники зможуть отримати доступ до ваших систем. Крім того, впровадження автентифікації без пароля допоможе повністю усунути ризики, пов’язані з паролем.

Ще однією небезпекою є використання загальнодоступних мереж Wi-Fi. Найкращий спосіб захисту від загроз через загальнодоступні мережі Wi-Fi — це використання VPN для доступу до систем або файлів на пристрої.

РОЗДІЛ 3
ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

3.1. Огляд основних технологій захисту бездротових мереж

Протоколи безпеки Wi-Fi застосовують технологію шифрування для безпеки мереж і захисту даних. Бездротові мережі не рідко є менш безпечними, у порівнянні з дротовими, тому бездротові протоколи безпеки мають вагоме значення для безпеки в Інтернеті. Найпоширенішими протоколами безпеки Wi-Fi на сьогодні є WEP, WPA та WPA2.

3.1.1. Протокол безпеки WEP

WEP (Wired Equivalent Privacy) є найстарішим і найпоширенішим протоколом безпеки Wi-Fi. WEP є частиною стандарту IEEE 802.11, розробленого для забезпечення більшої безпеки трафіку, що надсилається через бездротові мережі. У 1997 році, коли базовий стандарт 802.11 був ратифікований, в IEEE був схвалений механізм WEP, в якому головним засобом забезпечення безпеки в бездротових мережах є шифрування. Він був створений, щоб допомогти запобігти успішним кібератакам, таким як атаки типу «людина посередині». WEP працює на другому рівні моделі OSI із використанням для шифрування 40-бітного ключа, який є недостатньо захищеним [13].

Ключові проблеми та слабкі місця алгоритму WEP полягають у:

- механізми обміну ключами (а саме, в його відсутності);
- досить малих розрядностях ключів та вектора ініціалізації (IV);
- механізмі перевірки цілісності переданих даних;
- способі аутентифікації і алгоритмі шифрування RC4 .

Далі розглянемо процес шифрування WEP, що здійснюється у два етапи.

На першому етапі підраховується контрольна сума (Integrity Checksum Value - ICV) із застосуванням алгоритму Cyclic Redundancy Check (CRC - 32), що в

подальшому додається в кінець незашифрованого тексту і служить для перевірки його цілісності прийнятою стороною.

На другому етапі здійснюється безпосередньо шифрування . Ключ для WEP - шифрування - загальний секретний ключ, який що відомий обом сторонам бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом з випадковим 24 - бітним IV є вхідною послідовністю для генератора псевдовипадкових чисел, що базується на шифрі Вернама для генерації рядка випадкових символів, що називається ключовим потоком (key stream).

Дана операція виконується з ціллю уникнути методів злому, заснованих на статистичних властивостях відкритого тексту.

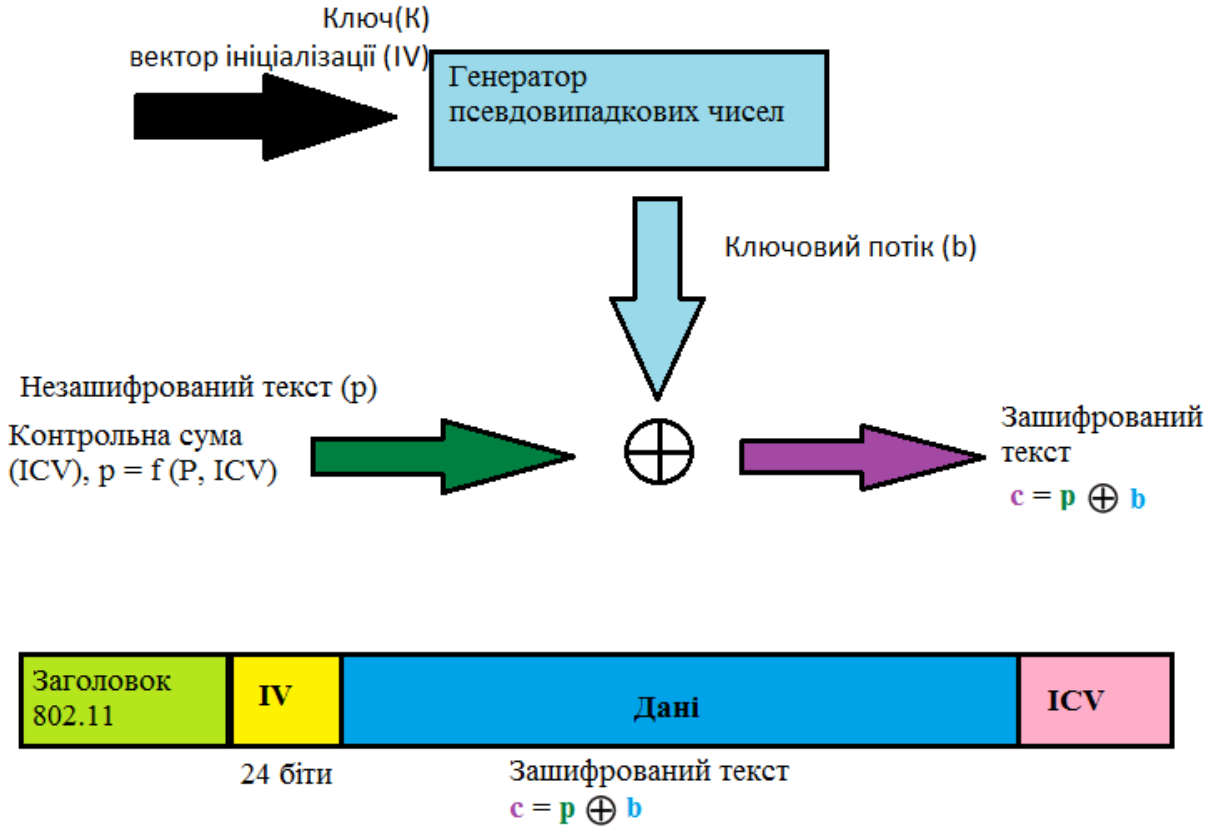


Рис. 3.1. Схема шифрування за протоколом WEP

Зашифроване повідомлення (рис. 3.1) утворюється шляхом здійснення операції XOR (додавання за модулем 2) над незашифрованим повідомленням з ICV і ключовим потоком. В переданий пакет у відкритому вигляді додається IV, для того

щоб отримувач зміг його прочитати. Після приймання інформації на іншій стороні, проводиться зворотна дія (p = c + b).

Використовуючи код Вернама до вхідної послідовності, одержувач обчислює значення b, що складається з ключа К (який заздалегідь відомий) і IV, який прийшов разом з цим же повідомленням у відкритому вигляді. Для кожного чергового пакета процес повторюється з новим обраним значенням IV.

З числа властивостей алгоритму RC4 можна виділити: використання того самого значення ключа і вектора ініціалізації призводить до отримання однакового значення b, тому використання операції XOR до двох текстів, які зашифровані RC4 з використанням однакового значення b є не що іншим, як операцію XOR до двох початкових текстів.

Отже, можна отримати незашифрований текст, що є результатом операції XOR між двома іншими оригінальними текстами. Процедура їх вилучення є нескладною. Наявність оригінального тексту і IV дає змогу обчислити ключ, що надалі дозволить читати всі повідомлення даної бездротової мережі.

3.1.2. Стандарт IEEE 802.11X

Етапом у розвитку методів захисту бездротових мереж є виникнення стандарту IEEE 802.11X, спільно з IEEE 802.11. На відміну від протоколу WEP, стандарт IEEE 802.11X використовує динамічні 128 - бітові ключі, періодично змінні в часі. Секретний ключ передається в зашифрованому вигляді після обов’язкового проходження етапу аутентифікації. Дія ключа є обмеженою у часі і є дійсним тільки на момент сеансу. Якщо сеанс закінчився, то для користувача створюється новий секретний ключ та повторно висилається.

802.1X ґрунтується на:

- EAP (Extensible Authentication Protocol). Протокол розширеної аутентифікації. Застосовується разом з RADIUS сервером у великих мережах.
- TLS (Transport Layer Security). Протокол транспортного рівня, що забезпечує цілісність і шифрування переданих даних між сервером і клієнтом, їх взаємну аутентифікацію, попереджає перехоплення і підміна повідомлень.

- RADIUS (Remote Authentication Dial - In User Server). Сервер аутентифікації користувачів за логіном і паролем .

Для шифрування даних, як і в протоколі WEP, використовується алгоритм RC4 з невеликими відмінностями.

У зазначеному стандарті були виправлені недоліки технологій безпеки, вживаних в 802.11, - це можливість злому WEP і залежність від технологій виробника.

3.1.3. Стандарт безпеки WPA

Wi- Fi Protected Access (WPA) - протокол безпеки, що використовується для забезпечення безпеки в бездротових мережах. Він був створений на заміну WEP, в якого були виявлені доволі слабкі місця.

Розрізняють два види WPA :

- WPA- PSK (Pre-shared key). Для входу в мережу та генерації ключів використовується ключова фраза. Найкращий із можливих варіантів для домашньої або невеликої офісної мережі.
- WPA- 802.1x . (Enterprise). Вхід в мережу здійснюється через сервер аутентифікації. Добре підходить для мережі великої компанії.

WPA - це тимчасовий стандарт, що з'явився внаслідок домовленостей виробників устаткування, допоки не буде введено в дію стандарт IEEE 802.11i . Фактично, WPA = 802.1X + EAP + TKIP + MIC, де:

- WPA - технологія захищеного доступу до бездротових мереж;
- EAP - протокол розширеної аутентифікації (Extensible Authentication Protocol),
- TKIP - протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol),
- MIC - технологія перевірки цілісності повідомлень (Message Integrity Check).

Ключовими тут є нові модулі TKIP і MIC. Стандарт TKIP використовує автоматично підібрані 128 - бітові ключі, які утворюються випадковим чином, при

тому що загальне число можливих варіантів сягає 500 мільярдів. Складна система алгоритму підбору ключів і їх заміна через кожні 10 Кбайт (10 тис. переданих пакетів) роблять систему більш безпечною.

Технологія перевірки цілісності повідомлень MIC застерігає від зовнішнього проникнення і модифікації інформації. Доволі складний математичний алгоритм дає змогу порівняти дані відправлені з однієї точки і отриману в іншій. Дані вважаються помилковими, коли були виявлені зміни та підсумок порівняння відрізняється, такі дані викидаються та не беруть участь у подальших розрахунках.

У порівнянні з WEP, де для контролю цілісності переданих даних застосовувався алгоритм CRC- 32, TKIP використовує MIC, де криптографічна контрольна сума обчислюється як сумування трьох полів (адреса джерела, адреса призначення і поле даних). Оскільки класичні MIC- алгоритми (наприклад, HMAC - MD5 або HMAC - SHA1) для існуючого бездротового обладнання були дуже складними і вимагали великих обчислювальних витрат, то спеціально для використання в бездротових мережах Нільсом Фергюсоном (Niels Ferguson) був розроблений алгоритм Michael. Для шифрування він застосовує 64-бітний ключ і виконує дії над 32-бітними блоками даних. MIC включається в зашифровану частину фрейму між полем даних і полем ICV

Ще однією функцією, котрої не було WEP є нумерація пакетів, що забезпечує цілісність даних в протоколі TKIP. В якості номеру береться IV, що тепер носить назву TKIP Sequence Counter (TSC) із довжиною 48 біт, це вдвічі більше у порівнянні з 24 бітами, як було в WEP (рис. 3). Підвищення довжини IV до 48 біт дає можливість уникнути колізії векторів і дає гарантію, що вони не повторяться у наступні тисячі років.

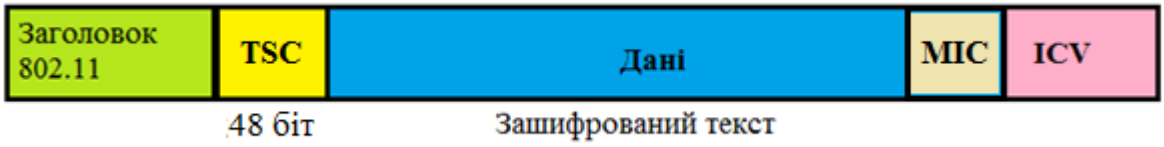


Рис. 3.2. Структура пакета протоколу TKIP

Головною рисою, що відрізняє TKIP від WEP є механізм управління ключами, який дає змогу час від часу змінювати ключі і дозволяє проводити обмін ними між усіма учасниками мережевої взаємодії: саплікантом, аутентифікатором і сервером аутентифікації. Спеціалізовані ключі генеруються на різних етапах взаємодії та у процесі роботи. Проте, TKIP зараз не дуже підходить для реалізації шифрування, оскільки набирають популярності нові алгоритми, засновані на технології Advanced Encryption Standard (AES), що вже досить давно застосовується в VPN та є більш захищеними.

Аутентифікація потребує, щоб користувач показав підтвердження того, що він має дозвіл на вхід в мережу. Для цього права користувача перевіряються по базі даних зареєстрованих користувачів. Для роботи в мережі користувач повинен обов'язково пройти через механізм аутентифікації.

RADIUS – це спеціальний централізований сервер аутентифікації, в якому міститься база даних та система перевірки для великих мереж. Сервер RADIUS спершу здійснює перевірку інформацію користувача, яка підлягає аутентифікації (чи відповідає вмісту своєї бази даних про ідентифікатори і паролі користувачів) або його цифровий сертифікат, а після цього здійснює динамічну генерацію ключів шифрування точкою доступу і клієнтською системою для кожного сеансу зв'язку.

Але, оскільки застосування WPA стосується усіх категорій користувачів бездротових мереж, стандарт має спрощений режим, котрий не потребує застосування більш складних механізмів. Даний режим має назву Pre-Shared Key (WPA - PSK) – суть якого полягає у використанні одного паролю на кожен вузол бездротової мережі (до прикладу точки доступу, бездротові маршрутизатори, клієнтські адаптери, тощо). Клієнт матиме доступ в мережу тільки у випадку збігання паролів [15].

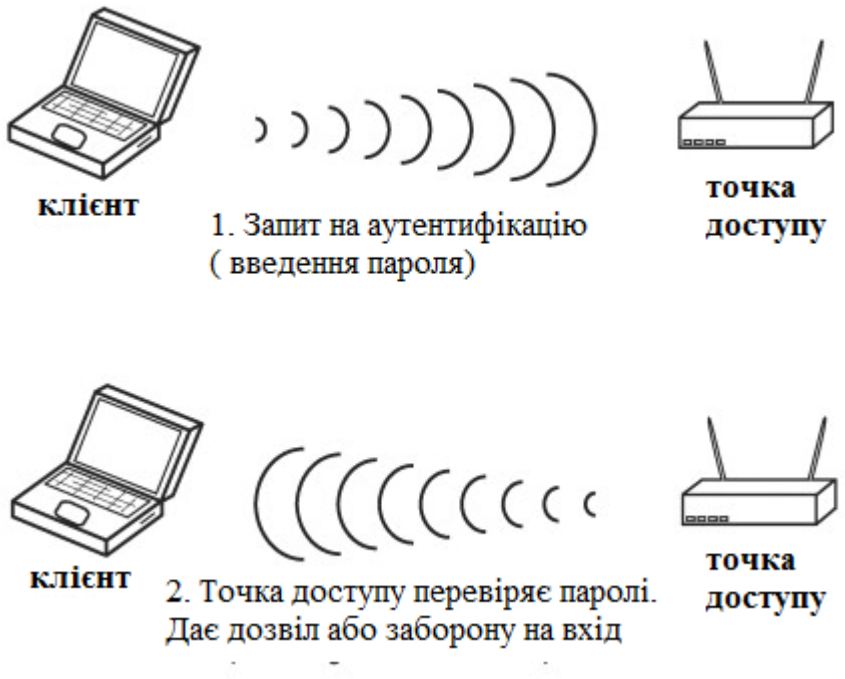


Рис. 3.3. Аутентифікація PSK.

EAP методи аутентифікації:

- Message Digest 5 (MD5) - процедура односторонньої аутентифікації сапплікanта сервером аутентифікації, використовує хеш-суму MD5, ім’я користувача і пароля в якості підтвердження для сервера RADIUS. Даний метод не підтримує управління ключами та створення динамічних ключів. Саме томі він не застосовується в стандарті 802.11i і WPA.
- Transport Layer Security (TLS) - процедура аутентифікації, що використовує цифрові сертифікати X.509 в рамках інфраструктури відкритих ключів (Public Key Infrastructure - PKI). EAP-TLS має динамічного створення ключів і взаємну аутентифікацію між сапплікантом і сервером аутентифікації. Як недолік даного методу можна виділити необхідність підтримки інфраструктури відкритих ключів.
- Tunneled TLS (TTLS) - EAP має розширені можливості EAP- TLS. EAP-TTLS використовує безпечне з'єднання, встановлене в результаті TLS - квитування для обміну додатковою інформацією між сапплікантом і сервером аутентифікації.

3.1.4. Стандарт безпеки WPA2

На відміну від WPA, використовується більш стійкий алгоритм шифрування AES. За аналогією з WPA, WPA2 також ділиться на два типи: WPA2-PSK і WPA2-802.1x.

Для забезпечення цілісності та конфіденційності даних застосовуються більш нові та перевірені механізми такі як:

- Протокол CCMP (Counter -Mode - CBC - MAC Protocol), заснований на режимі Counter Cipher - Block Chaining Mode (CCM) алгоритму шифрування AES. CCM об'єднує два механізми: Counter (CTR) для забезпечення конфіденційності та Cipher Block Chaining Message Authentication Code (CBC - MAC) для аутентифікації.
- Протокол WRAP (Wireless Robust Authentication Protocol), заснований на режимі Offset Codebook (OCB) алгоритму шифрування AES.
- Протокол TKIP для забезпечення зворотної сумісності з обладнанням, яке випускалося раніше.
- Взаємна аутентифікація та доставка ключів на основі протоколів IEEE 802.1x/EAP.
- Безпечний Independent Basic Service Set (IBSS) для підвищення безпеки в мережах Ad-Hoc.
- Підтримка роумінгу.

Однак WPA2 має свої вразливості. Головною вразливістю, що несе за собою серйозну небезпеку є можливість несанкціонованого доступу до корпоративної бездротової мережі. Це є можливим за умови введення векторних атак на окремі точки доступу Wi-Fi Protected Setup (WPS). Тому слід здійснювати відключення WPS для всіх точок доступу вектора атак у WPA2, для попередження здійснення атак. Крім того, WPA2 має такі вразливості, як Transport Layer Security. За допомогою атаки з пониженням версії зловмисники можуть здійснювати напади на такі вразливості.

Здебільшого такі загрози зазвичай були розраховані на корпоративні бездротові системи. Крім того, домашні бездротові системи з простими паролями

або паролями за замовчуванням можуть нести небезпеку та бути атакованими. Облікові записи, що мають переваги, до прикладу облікові записи адміністратора, зобов’язані мати складніші та довгі паролі. Більше того рекомендується періодично змінювати всі паролі [15].

3.1.5. Стандарт безпеки WPA3

WPA3 забезпечує найсучасніші протоколи безпеки. Ґрунтуючись на широкому успіху та прийнятті безпеки Wi-Fi, WPA3 додає нові функції для спрощення безпеки Wi-Fi, забезпечення більш надійної автентифікації, забезпечення підвищеної криптографічної надійності даних та підтримки стійкості критично важливих мереж.

Усі мережі WPA3:

- Використовують новітні методи безпеки;
- Забороняють застарілі протоколи;
- Вимагають використання захищених кадрів керування (PMF).

Оскільки мережі Wi-Fi відрізняються за цілями використання та потребами безпеки, WPA3 містить додаткові можливості спеціально для персональних і корпоративних мереж. Користувачі WPA3-Personal отримують посилений захист від спроб вгадування пароля, а користувачі WPA3-Enterprise тепер можуть скористатися перевагами протоколів безпеки вищого рівня для конфіденційних мереж даних [14].

WPA3-Personal надає кращий захист окремим користувачам, забезпечуючи більш надійну автентифікацію на основі пароля, навіть якщо користувачі вибирають паролі, які не відповідають стандартним рекомендаціям щодо складності. Цю можливість увімкнено через одночасну автентифікацію рівняння (SAE). Технологія стійка до офлайн-словникових атак, коли зловмисник намагається визначити мережевий пароль, підбираючи можливі паролі без подальшої взаємодії з мережею.

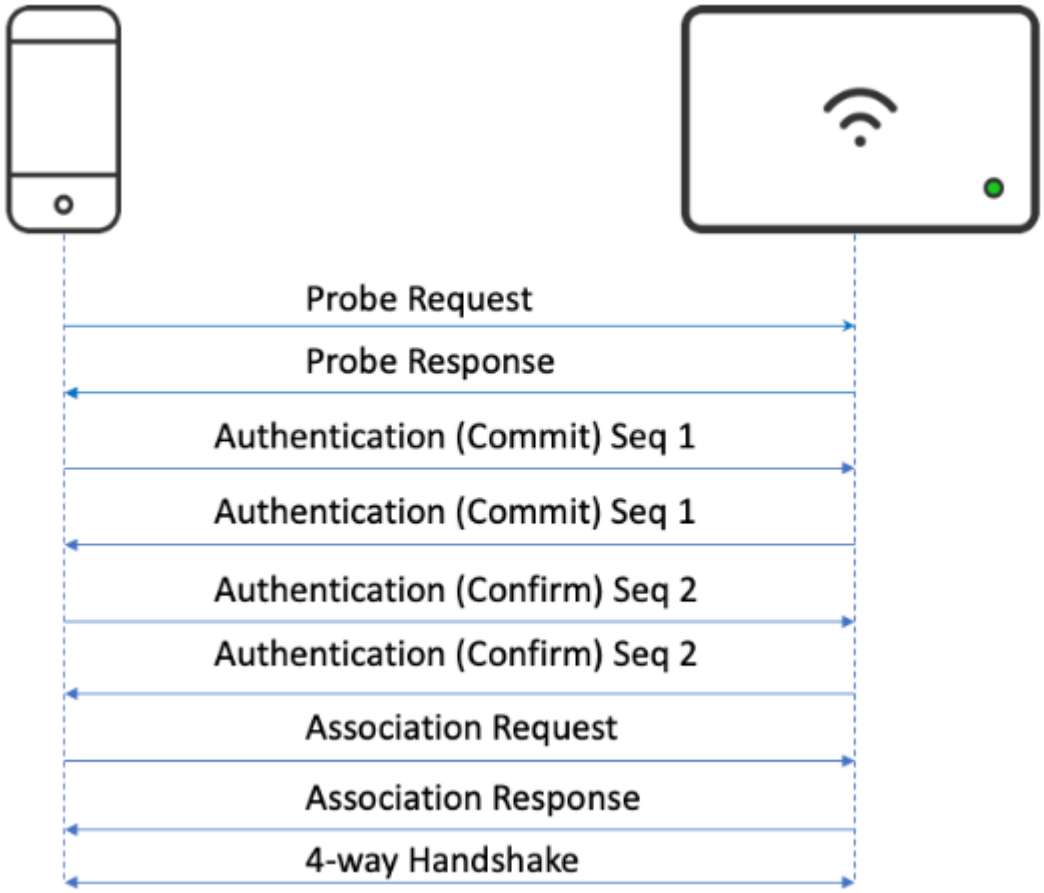


Рис. 3.4. Аутентифікація SAE

1. Запит зонду. Регулярний запит до AP після маяка.

2. Відповідь зонда. Звичайна відповідь на ДПА.

3. Автентифікація (Здійснення) від STA до AP. Цей пакет є кадром автентифікації 802.11. Закріплення включатиме послідовний номер 1 автентифікації SAE зі скаляром і елементом, не пов'язаним із паролем, який буде використано. Це використовується для створення PMK (парного головного ключа) на STA.

4. Автентифікація (Здійснення) від AP до STA Використовується для створення PMK на точці доступу.

5. Автентифікація (підтвердження) від STA до AP Цей пакет є кадром автентифікації 802.11. Підтвердження включає послідовний номер 2 із повідомленням підтвердження з ключем, згенерованим для перевірки AP.

6. Автентифікація (підтвердження) від AP до STA Підтвердження включає послідовний номер 2 із повідомленням підтвердження зі згенерованим ключем, що повідомляє STA, що ключ правильний, або відхиляє автентифікацію.

7. Звичайний запит на асоціацію

8. Регулярна відповідь асоціації

9. 4-стороннє рукостискання з використанням PMK, створеного методом SAE. Після цього кроку можна буде передавати регулярні дані

Особливості WPA3-Personal:

- Природний вибір пароля: дозволяє користувачам вибирати паролі, які легше запам’ятати;
- Простота використання: забезпечує покращений захист без змін у способі підключення користувачів до мережі;
- Передача секретності: захищає трафік даних, навіть якщо пароль було зламано після передачі даних.

WPA3-Enterprise будується на основі WPA2-Enterprise з додатковою вимогою використання захищених фреймів керування для всіх підключень WPA3. Особливості WPA3-Enterprise:

- Автентифікація: кілька методів Extensible Authentication Protocol (EAP);
- Автентифіковане шифрування: мінімальний 128-бітний стандартний режим лічильника розширеного шифрування з автентифікацією повідомлень у ланцюжку шифрованих блоків (AES-CCMP 128);
- Виведення та підтвердження ключа: мінімум 256-бітний режим автентифікації хешованого повідомлення (HMAC) із безпечним алгоритмом хешування (HMAC-SHA256);
- Надійний захист фрейму керування: мінімум 128-бітний код автентифікації повідомлень на основі протоколу цілісності широкомовної/багатоадресної передачі (BIP-CMAC-128).

3.2. Порівняльна характеристика стандартів безпеки

Таблиця 3.1

Порівняльна характеристика стандартів безпеки

Стандарт захисту	Переваги	Недоліки
WEP	- Краще, ніж протокол безпеки відсутній взагалі	- Має уразливості системи безпеки - Використовує тільки 64-бітні та 128-бітні ключі для шифрування - Шифрування з фіксованим ключем - Важкий у налаштуванні
WPA	- Позбувається вразливих місць стандарту бездротової безпеки WEP - Метод шифрування TKIP є кращим за шифрування з фіксованим ключем, як в протоколі WEP - 256-бітний ключ для шифрування	- TKIP можна застосовувати при відкритті на пристроях WEP - Вразливості безпеки схожі до WEP
WPA2	- Виправляє багато мінусів безпеки попередніх стандартів - Застосовує найбільш надійний метод шифрування: AES - Wi-Fi Alliance рекомендує цей стандарт для використання на всіх сертифікованих продуктах	- Містить незначні вразливості безпеки - Потребує дуже великої обчислювальної потужності

Закінчення таблиці 3.1

WPA3	- Безпечніший зв'язок у громадських місцях - Протокол практично усунув проблеми атаки KRACK - Забезпечує більш надійний, але простий процес автентифікації - Дає можливість використовувати більш короткі електронні ключі	- Висока вартість - Повністю не усуває ризиків атаки. -

З огляду на таблицю 3.1 наведену вищу, можна побачити, що від WEP до WPA3 кожен тип протоколу безпеки є вдосконаленням і покращенням в порівнянні з попереднім. Крім того, можна зробити висновки що протокол WEP не рекомендуються використовувати взагалі, оскільки він має низький рівень захисту та багато проблем із безпекою, через які ключі легко зламати. Що стосується методу шифрування, WPA все ще використовує незахищений потоковий шифр RC4 WEP, але забезпечує додатковий захист через TKIP.

На відміну від WPA та WPA2, які використовують недосконале 4-стороннє рукостискання для включення бездротових з’єднань, яке є джерелом уразливості KRACK, у WPA3 діє одночасна автентифікація рівних рукостискань, що автентифікує пристрій у мережі, для захисту з’єднання від атак. WPA3 замінює PSK на SAE, більш безпечний спосіб початкового обміну ключами. У той же час розмір ключа сеансу WPA3 збільшується до 128-біт у режимі WPA3-Personal і до 192-біт у WPA3-Enterprise, що робить пароль важчим для злому, ніж попередні стандарти безпеки Wi-Fi.

Порівнюючи всі вищезгадані стандарти, можна сказати, що WPA3 показує найвищу безпеку та ефективність серед цих чотирьох типів стандартів безпеки Wi-Fi, особливо для корпоративних мереж і громадських місць. Проте усі переваги WPA3 реалізуються лише у випадку, коли мережа перебуває в режимі WPA3 і розгортання цієї мережі почнеться лише за наявності більшої кількості пристроїв

кінцевих користувачів WPA3. Тому поки не варто розглядати WPA3 як основний протокол захисту безпровідних мереж. Найбільш вживаним і основним протоколом на сьогодні залишається WPA2.

3.3. Методи захисту бездротових мереж зв'язку

Не можна недооцінити важливість безпеки бездротової мережі. З поширенням мобільних пристроїв і популярністю публічних точок доступу Wi-Fi ймовірність витоку даних та інших загроз останнім часом дуже сильно зросла. На сьогодні, у звичайних користувачів і адміністраторів мереж є всі необхідні засоби для надійного захисту Wi-Fi, і за відсутності явних помилок (людський фактор) завжди можна забезпечити високий рівень безпеки, відповідний цінності інформації, що знаходиться в такій мережі. Основні ж методи, як слід використовувати при організації і налаштуванні бездротової Wi-Fi- мережі наступні.

Двофакторна автентифікація забезпечує додатковий рівень безпеки до процесу входу. Користувачі повинні вводити ім'я користувача та пароль, а також код, створений програмою автентифікації. Це ускладнює неавторизований доступ до мережі. Крім того можливість використання автентифікації без пароля , як-от хмарний радіус, забезпечить ще більш надійний захист. Оскільки у випадку якщо стороння особа отримає пароль, вона зможе отримати доступ до мережі. Використовуючи хмарні технології, можна бути впевненим, що лише авторизовані користувачі матимуть доступ до мережі.

Використання надійного пароля є одним із найважливіших передових методів безпеки бездротової мережі. Надійний пароль містить як мінімум вісім символів і містить поєднання великих і малих літер, цифр і символів. Паролі слід час від часу змінювати, щоб забезпечити їх безпеку.

Шифрування даних є ще однією важливою умовою для безпеки бездротової мережі. Шифрування даних дозволяє розшифрувати та прочитати інформацію лише авторизованим користувачам. Це допомагає захистити конфіденційну інформацію від доступу неавторизованим особам. Шифрування можна реалізувати кількома

способами, включно з використанням програмного забезпечення для шифрування, обладнання або послуг.

Вимкнення широкомовної передачі SSID – це ще одна найкраща умова безпеки бездротової мережі. Коли трансляція SSID увімкнена, це дозволяє будь-кому в зоні дії бездротової мережі бачити назву мережі. Мета полягає в тому, щоб ускладнити доступ неавторизованих осіб до мережі. Ідентифікатор SSID усе ще можна побачити, якщо хтось перебуває в зоні дії мережі та використовує сканер бездротової мережі, але до нього буде важко отримати доступ.

Використання фільтрації MAC. MAC-адреси — це унікальні ідентифікатори, призначені пристроям, які підключаються до мережі. Дозволяючи підключатися до мережі лише пристроям із певними MAC-адресами, ви можете допомогти запобігти неавторизованому доступу.

Увімкнення безпеки WPA3. WPA3 — найновіший і найбезпечніший протокол безпеки бездротового зв’язку. Він забезпечує сильніший захист, ніж WPA2, і його слід використовувати, коли це можливо. Обираючи маршрутизатор, важливо переконатися, що він підтримує цей останній протокол безпеки. Попередні протоколи було легше зламати, тому важливо щоб WPA3 було увімкнено.

Використання VPN . VPN шифрує весь трафік між пристроєм і сервером VPN, що ускладнює прослуховування з’єднання. Це особливо важливо під час використання публічних мереж Wi-Fi, оскільки вони часто менш безпечні, ніж приватні.

Вимкнення віддаленого адміністрування. Коли віддалене адміністрування ввімкнено, це дозволяє будь-кому з належними обліковими даними отримати доступ до сторінки конфігурації маршрутизатора та внести зміни в мережу. Це може становити загрозу безпеці, оскільки дозволяє неавторизованим особам отримати доступ до мережі.

Використання брандмауера допомагає захистити мережу, блокуючи вхідний трафік, який не авторизований. Universal Plug and Play (UPnP) — це протокол, який дозволяє пристроям автоматично виявляти та підключатися один до одного. Тому, його слід відключити. Крім того, слід вимкнути непотрібні служби, це допоможе

зменшити поверхню атаки мережі. Поширені непотрібні служби включають такі речі, як Telnet, SSH і HTTP.

ВИСНОВКИ ДО РОЗДІЛУ 3

В даному розділі було розглянуто основні стандарти безпеки бездротових мереж такі як: WEP, WPA, WPA2, та WPA3. Проаналізувавши характеристики та особливості вищезазначених протоколів безпеки можна зробити висновки, що протокол WEP має низький рівень захисту та багато проблем із безпекою, через які ключі легко зламати, тому його використовувати не варто.

Порівнюючи всі вищезгадані стандарти, можна сказати, що WPA3 показує найвищу безпеку та ефективність, особливо для корпоративних мереж і громадських місць. WPA3 має ряд переваг такі як: подовження шифрування до 192 біт (WPA3-Enterprise) для підвищення надійності паролів; більш безпечне рукостискання (SAE), що забезпечує секретність пересилання та набагато більшу безпеку даних у відкритій мережі; можливість користувачам вибирати паролі, які легше запам’ятати. Проте усі переваги WPA3 можна реалізувати лише у випадку, коли мережа перебуває в режимі WPA3 і розгортання цієї мережі почнеться лише за наявності більшої кількості пристроїв кінцевих користувачів WPA3. Тому поки не варто розглядати WPA3 як основний протокол захисту безпровідних мереж. Найбільш вживаним і основним протоколом на сьогодні залишається WPA2.

Були наведені основні методи захисту бездротових мереж серед яких: двофакторна автентифікація, використання надійного пароля, шифрування даних, вимкнення широкомовної передачі SSID, використання фільтрації MAC, увімкнення безпеки WPA3, використання VPN, вимкнення віддаленого адміністрування, використання брандмауера та вимкнення непотрібних служб.

РОЗДІЛ 4
АНАЛІЗ МЕТОДІВ ДЛЯ ГЕНЕРУВАННЯ ПАРОЛІВ

4.1. Проблеми парольних політик

Політика паролів встановлює правила, яким мають відповідати паролі для служби, наприклад довжину та тип дозволених і заборонених символів. Крім того, політика паролів може вказувати, на те що запис заборонено до використання , оскільки термін міститься в словнику небажаних термінів. На сьогодні, проблема парольних політик є надзвичайно актуальною. Як показує практика: чим більша мережа і чим цінніша інформація там знаходиться, тим більше охочих здійснити атаку на неї заради матеріальної вигоди. Політика паролів не має можливості вирішити основну проблему з паролями – їх величезну кількість. Оскільки кількість додатків, що використовуються, є дуже великою, це означає, що створити та запам’ятати унікальні складні паролі для кожного з них просто неможливо. Навіть якщо політика паролів дотримується, сам пароль за сучасними стандартами може бути недостатньо надійним, щоб уникнути його зламу.

Розглянемо найпоширеніші методи злому паролів.

Атака за словником — це техніка вгадування пароля за допомогою часто використовуваних слів. Як правило, користувачі придумують паролі за двома правилами: хобі чи близькі люди; пароль, який легко запам'ятати.

У цій атаці хакери використовують спеціально підібраний список слів, що містять повсякденні слова, які жертва може використовувати. Такий список складається на етапі збору інформації. У цьому методі хакер систематично вводить кожне слово в словник, щоб зламати пароль. Однак ви можете бути захищені від атаки за словником, використовуючи комбінацію випадкових слів зі словника, наприклад. Крім того, найкраще поєднувати його з цифрами та символами для більшої складності та кращої безпеки. У типовій атаці за словником WPA/WPA2 PSK зловмисник використовує ПЗ, що здійснює вивід 256-бітового ключа для

кожної парольної фрази разом з іншими параметрами, описаними у розділі Створення РТК.

Під час атаки методом грубої сили зловмисник намагається зламати пароль, надсилаючи різні комбінації, доки не буде знайдено правильну. Зловмисник використовує програмне забезпечення, щоб автоматизувати цей процес і запускати вичерпні комбінації паролів за значно менший проміжок часу. За останні кілька років таке програмне забезпечення було активізовано завдяки прогресу апаратного забезпечення та технологій. В таблиці нижче наведено час, необхідний для злому пароля в залежності від кількості символів та місткості пароля [17].

Таблиця 4.1

Час необхідний для злому пароля

Кількість символів	Містить тільки цифри	Малі літери	Великі і малі цифри	Цифри, великі і малі літери	Цифри, великі і малі літери, символи
4	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
5	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
6	Миттєво	Миттєво	Миттєво	1 сек	4 сек
7	Миттєво	Миттєво	24 сек	1 хвилина	5 хвилин
8	Миттєво	4 сек	21 хвилина	1 година	7 годин
9	Миттєво	2 хвилини	18 годин	3 дні	3 тижні
10	Миттєво	57 хвилин	1 місяць	6 місяців	5 років
11	3 сек	1 день	5 років	40 років	350 років
12	23 сек	3 тижні	290 років	3 тис. років	33 тис. років
13	3 хвилини	1,5 року	15 тис. років	100 тис. років	2 млн. років

Закінчення таблиці 4.1

14	38 хвилин	50 років	750 тис. років	8 млн. років	200 млн. років
15	6 годин	1 тис. років	42 млн. років	550 млн. років	14 млрд. років

Атака із застосуванням райдужної таблиці. Коли ваші паролі зберігаються на сервері, вони шифруються в безглузді рядки символів замість того, щоб зберігатися як звичайний текст. Цей процес називається хешуванням і запобігає зловживанню вашим паролем. Щоразу, коли ви вводите свій пароль для входу, він перетворюється на хеш-значення та порівнюється з попередньо збереженим. І якщо значення збігаються, ви входите в систему. Тепер, оскільки паролі перетворюються на хеші, хакери намагаються отримати автентифікацію, зламавши хеш пароля. І вони роблять це за допомогою таблиці Rainbow — списку попередньо обчислених хешів можливих комбінацій паролів. Хакери можуть шукати веселкову таблицю, щоб зламати хеш, що призведе до злому вашого пароля. Таким чином, він знаходить хеш пароля з бази даних і усуває необхідність його зламувати. Крім того, не потрібно шукати сам пароль. Якщо хеш збігається, злом успішний [16].

4.2. Огляд методів для генерування паролів

Для створення надійного пароля слід дотримуватися наступних рекомендацій:

- Мінімум 12 символів: потрібно вибрати достатньо довгий пароль. Немає мінімальної довжини пароля, , але зазвичай паролі мають бути довжиною мінімум від 14 до 16 символів. Довший пароль був би ще кращим.
- Містить цифри, символи, великі та малі літери: використовуйте поєднання різних типів символів, щоб зробити пароль важчим для зламу.
- Не є словниковим словом або словосполученням словникових слів: тримайтеся подалі від очевидних словникових слів і комбінацій словникових слів.

Будь-яке слово саме по собі погане. Будь-яке поєднання кількох слів, особливо якщо вони очевидні, теж погано.

- Не варто робити очевидні заміни: також не використовуйте звичайні заміни — наприклад, «H0use» не є сильним лише тому, що ви замінили о на 0.

Хоч такі паролі і будуть надійні та стійкі до злому, запам’ятати такої довжини та складності паролі може бути досить складно. Так як пароль є ключем для підключення до бездротових мереж зв’язку, то питання їх надійності є дуже значущим, з погляду на захищеність користувачів [17].

Складання абсолютно випадкових послідовностей є важким завданням для людини. Отже, слід застосувати більш простий варіант для створення паролів. Наприклад створити пароль зі словосполучень слів, що мають хоч якийсь зв'язок між собою, тоді пароль запам'ятати буде простіше.

Як приклад можна використовувати в паролях антоніми чи синоніми до слів при цьому розбавляти їх різними комбінаціями знаків та цифр. Використовувати формули та вислови; вигадані адреси електронних пошт; зробити візуалізацію якогось процесу.

Правила використання букв, цифр і символів при різних довжинах паролів. Якщо довжина паролю від 8 до 11, спеціальні символи можна не використовувати. Від 12 до 15 використовуються букви різного регістру та цифри. Від 16 до 19 цифри можна не використовувати. При довжині паролю більш ніж 20 символів обмеження відсутні. Якщо пароль є дуже легким для запам'ятовування, то це означає, що його можна легко зламати.

Сигнали точки доступу в дальній зоні виявляються нижче рівня шуму приймача. Виявлення передавачів Wi-Fi шляхом послідовного сканування вузькосмуговими приймачами неможливо.

Виходячи з того, що практично кожен об'єкт оточений безліччю мереж Wi-Fi, відрізнити законних клієнтів мереж та сусідніх мереж від порушників, на жаль, дуже складно. канал.

У великих містах загальнодоступні мережі Wi-Fi мають досить великі зони покриття, щоб не було необхідності використовувати мобільні точки прийому

поблизу об'єктів. Неавторизовані пристрої можуть підключатися до доступних мереж Wi-Fi та використовувати їх для надсилання інформації. Через Інтернет, де це потрібно.

Wi-Fi є одним з варіантів прихованої передачі великих обсягів інформації, коли об'єкти мають обмежений доступ до носіїв інформації та обмежений доступ до Інтернету.

Йому необхідно підключитись до найближчої мережі Wi-Fi, але законні користувачі не знають про це.

Більшість атак починаються з розвідки, яка включає сканування мережі, збір і аналіз пакетів (багато службових пакетів у мережах Wi-Fi передаються відкрито).

При цьому дуже складно з'ясувати, хто є законними користувачами, хто намагається підключитися до мережі, хто займається збором інформації.

Після розвідки приймається рішення щодо подальших кроків наступу. Ви можете зменшити вразливість для розвідки, розмістивши точки доступу для забезпечення необхідного покриття. Це покриття мінімально перевищує контрольовану зону.

Розглянемо найбільш поширені способи генерування паролів.

Метод написання слів з іншою розкладкою з наступною заміною. Так як основна кількість слів, що часто вживаються якоюсь мовою застосовуються для утворення словників паролів, цей спосіб є дуже не надійним. Злочинець спосіб підбору зможе визначити пароль за досить швидкий час.

Метод випадкового рядка. Метод випадкового рядка також можна назвати клавіатурним затиранням, тобто випадкове натискання на клавіатуру. Словники з такими можливими комбінаціями теж існують, тому цей спосіб генерування паролів, є також сумнівним.

Метод паролів, що визначаються людиною. Суть цього методу полягає в створенні матриці з символами та в подальшій заміні цих символів використовуючи певний алгоритм. Цей спосіб можна використовувати як захист для онлайн-сервісів. Проте для бездротових систем зв'язку може бути ненадійним. Також процес виконання цього методу може бути дуже довгим по часу.

Метод створення паролів з використанням асоціацій та подальша вибіркова заміна букв на символи. Даний метод є затратним у часі і разом з тим існують словники, що містять подібні слова. Виходячи з цього, метод не є надійним.

Метод створення паролів з використанням кількох слів, які мають логічне поєднання та подальша вибіркова заміна. Цей метод може мати кращий результат. Але стійкість цього методу є під питанням. Час на створення паролів може бути довшим.

Метод генерування паролів шляхом застосування гральних кубиків та вибір слів з таблиці. Даний метод є менш затратним по часу, проте до цього методу є можливе застосування словників з підбору. Звідси надійність методу є не дуже високою.

З використанням спеціальних алгоритмів та додатків в ОС для створення випадкових паролів результат може бути кращім та більш складним, а затрати по часу створення є меншими. Ймовірність того, що зловмисник згенерує такий самий пароль є невеликою, хоча це можливо.

Метод парольної фрази. Метод парольної фрази створить дуже надійний пароль, який також є одним із найлегших для запам’ятовування. За допомогою цього методу ви створюєте випадковий набір слів і об’єднуєте їх разом. Слова мають бути випадковими, різноманітними та не об’єднуватися в логічні фрази.

4.3. Порядок покращення методу генерування паролів

Крок 1. Визначення стійкості та швидкості підбору паролів з їх обґрунтуванням.

Сучасний комп’ютер звичайного користувача за звичних умов роботи при застосуванні всіх центральних процесорів може сягати до 6500 паролів на секунду. Припустимо, що за одну секунду роботи CPU може перебрати біля 8 000 паролів із заданої сукупності. Це зроблено для зручності обчислення.

Вибір пароля може бути в сотні чи тисячі разів швидшим завдяки використанню графічних процесорів у графічних картах (GPU) і GPU фермах (наприклад, 12 графічних карт, що працюють у тандемі).

Можлива кількість вгадувань пароля за допомогою вгадування CPU, GPU та ферми GPU:

Кількість можливих варіантів підбору паролю за 1 секунду при використанні CPU - 10^4, за 1 хвилину - 6×10^5, за 1 годину - $3{,}6 \times 10^7$, за 1 добу - $8{,}64 \times 10^8$ і за 1 рік - $3{,}15 \times 10^{11}$. При використанні GPU за 1 секунду можна підібрати $1{,}5 \times 10^{10}$ варіантів, за 1 хвилину 9×10^{11} варіантів, за 1 годину $5{,}4 \times 10^{14}$ варіантів, за 1 добу $1{,}3 \times 10^{15}$ варіантів і за 1 рік - $4{,}73 \times 10^{17}$ варіантів. Якщо використовувати GPU-ферми, яка складається з 12 GPU за 1 секунду можна підібрати $1{,}8 \times 10^{11}$ варіантів паролю, за 1 хвилину - $1{,}08 \times 10^{13}$ варіантів, за 1 годину - $6{,}48 \times 10^{14}$, за 1 добу - $1{,}56 \times 10^{16}$ варіантів і за 1 рік - $5{,}68 \times 10^{18}$ варіантів паролів.

Якщо в ролі певної комбінації паролів використовується набір можливих мобільних телефонів, то формат +380 YY XXX XX XX (код регіону або мобільного оператора YY, де код оператора 16, або код міста та код оператора 48) Україна, XXX XX XX номер телефону).

Сортування номерів мобільних телефонів за допомогою центрального процесора зайняло 4 з половиною години, а сортування кодів українських регіонів і операторів – близько 14 годин 20 хвилин.

Використовуючи ферми GPU для злому паролів, час відповідної операції можна скоротити як мінімум у 17 мільйонів разів.

У результаті напрошується логічний, хоч і досить очевидний висновок. Чим більший період вибору, тим надійніший вибір пароля, і навпаки.

Крок 2. Визначення набору паролів для політики паролів.

Математично набір паролів політики паролів можна описати як набір певних символів.

- комбінація символів у паролі (комбінація),

Якщо k (довжина вибраного пароля) вибирається з n елементів (кількість можливих символів), порядок не має значення

- розташування символів пароля при виборі k з n елементів

у порядку;

- розташування, що містять повтори символів пароля, коли все є числом

k компоновок з елементів n вибираються і повторюються.

При X<x статистична (емпірична) функція розподілу вибірки паролів у наборі є законом, що змінює частоту подій підбору пароля.

$$\mathcal{F} * (x) = \frac{b(x)}{b} \tag{4.1}$$

де *b(x)* – число можливих варіантів паролю, при $x \leq X$,

X –випадкова величина множини паролів з невідомим розподілом;

b – об'єм вибірки.

Аналогом теоретичної диференціальної функції (густини) розподілу є щільність відносної частоти:

$$f_i = \frac{W_i}{l}, \tag{4.2}$$

де W_i – відносна частота, *l* – інтервал підбору.

Середнє арифметичне спостережуваних значень випадкової величини множини паролів:

$$M * [X] = \frac{\Sigma_{i=1}^{k} n_i x_i}{n} = x_e \tag{4.3}$$

де x_i – значення випадкової величини паролю,

$n = \Sigma_{i=1}^{k} n_i$ – об'єм вибірки.

Моменти вибірки порядків m(статистичні початкові та центральні):

$$M[(X - x_r)^m] = \frac{\Sigma_{i=1}^{k} (x_i - x_r)^m N_i}{N} \tag{4.4}$$

У міру збільшення кількості спостережень у вибірці наборів паролів всі статистичні властивості будуть ймовірно відповідати відповідним числовим властивостям генеральної сукупності цих наборів При $M \to max, P_z \to 0$

Для даних паролів можливі деякі відмінності, за кількістю множини.

Сполучення множини паролів (комбінація). З n елементів вибирають k, порядок не має значення.

$$C_n^k = \frac{n!}{(n-k)! \times k!} \quad (4.5)$$

В цьому випадку:

n=85 - ASCII: 25 прописних літер, 25 заголовних літер, 10 цифр, 25 спеціальних символів; *k=64* - кількість символів у паролі для WPA/WPA2.

Розміщення множини паролів. З n елементів вибирають k в певному порядку.

$$A_n^k = \frac{n!}{(n-k)!} \quad (4.6)$$

де n- кількість можливих символів;

k- довжина обраного паролю.

Розміщення з повтореннями множини паролів. Число всіх розміщень з n по k з повтореннями.

$$A'^k_n = n^k \quad (4.7)$$

де n - кількість можливих символів;

k - довжина обраного паролю.

Можливі різні значення кількості паролів, залежно від вибраного типу захисту мережі та опції обмеження вибору символів. Якщо зловмисники знайомі з методами формування політик паролів (комбінування кількох паролів, повторення кількох паролів тощо), то час збігу пароля, що не повторюється, становить приблизно $6{,}12*10^{100}$ разів, що буде перевагою.

При цьому слід звернути увагу, що кількість паролів у заданому наборі дозволяє оцінити набір паролів лише за їх розміром, але не дозволяє оцінити надійність самих паролів. Скоротити час, необхідний для підбору паролів може часткове збігання з паролями в же існуючих словниках.

Крок 3. Формування змінних правил ускладнення для сполучення множини паролів.

Із сполучення множини паролів *Up* відбирається множина *Uz* , що складається з паролів, які мають в собі два числа від 2 до 8 цифр. З множини *Uz* за певним алгоритмом *d (d1…d8),* за визначенням кількості та довжини чисел, виділяються 8 підмножин *Ul(d)*. З підмножини *Ul(d)* згідно з обраним номером алгоритма *d* визначаються паролі, що згодом сумуються до множини (*Up - Uz*).

Це в свою чергу забезпечує утруднення паролю на три рівні, так як:, при сумуванні нні паролів беруться до уваги лише ті, що складаються з певної кількості цифр (відповідно до певного алгоритму *d*); коли обирається алгоритм *d* для множини паролів, що ускладнюються, воно може бути як змінним, так і незмінним. При використанні порядку ускладнення *d* під час генерування паролів зловмисник не зможе створити такий же алгоритм.

Крок 4. Розрахунок можливої кількості паролів для парольних множин:

$$U_{l(d)} = C_l^m \cdot C_{l-m}^m \cdot C_{l-2m}^m \cdot \ldots \cdot C_{l-(r-1)m}^m \cdot C_{l-rm}^m \qquad (4.8)$$

де *l* – кількість літер алфавіту;

m – кількість літер в слові

Uz обчислюється як сума для кожного значення підмножини $U_{l(d)}$

З цього слідує що, загальна кількість комбінацій можливих слів з двох чисел від двох до восьми цифр складає $2{,}53 \cdot 10^4$ (*Uz*), а кількість можливих комбінацій паролів не зазнає суттєвих змін, та становитиме $5{,}97 \cdot 10^{22}$ (*Up-Uz*).

4.4. Зберігання паролів

Програми для керування паролями пропонують чудову альтернативу використанню функції зберігання паролів. Ось деякі плюси та мінуси використання спеціальної програми для керування паролями.

Переваги використання менеджера паролів:

- Найкраще місце для зберігання паролів — найкращий спосіб безпечного зберігання паролів — надійний додаток для керування паролями. Менеджер паролів дозволяє легко створювати безпечні паролі, керувати ними та отримувати доступ до них.
- Можна використовувати безоплатно — більшість програм для керування паролями пропонують безкоштовний план із базовими функціями, який працює на одному пристрої. Безумовно, можна отримати менеджер паролів, не виймаючи свою кредитну картку.

Мінуси використання програми для керування паролями:

- Потрібен час, щоб знайти потрібний — можливо, вам доведеться витратити час на порівняння варіантів і цін менеджера паролів, щоб вибрати правильний додаток для себе. Велика кількість доступних варіантів може бути надзвичайною, як і вибір між безкоштовним і платним планом.
- Може статися збій — навіть найкращі програми отримують скарги користувачів на випадкові технічні збої, наприклад, блокування доступу до менеджера паролів або відсутність запиту, чи хочуть вони зберегти пароль.
- Потрібен головний пароль — зазвичай для входу в менеджер паролів потрібен довгий, дуже надійний головний пароль. Вам доведеться знайти безпечне місце, щоб сховати цей пароль, і може бути важко отримати доступ до менеджера паролів, якщо він буде втрачений

Для зберігання паролів я пропоную мати ідентифікаційну картку з QR-кодом, яку можна зберігати у своєму гаманці. Для отримання доступу до своїх паролів (переглядати їх безпосередньо), знадобиться ідентифікаційна картка та сканування її за допомогою захищеного паролем смартфоном. Після можна побачити необхідні

паролі. Щойно ви зайдете в телефон і відкриєте налаштовану програму для зчитування пароля QR, ви зможете просто отримати прямий доступ до своїх паролів замість рівня QR-коду. Але, скажімо, додається етап QR-коду, сканування QR-коду для отримання доступу. Тож у вас є пароль телефону та QR-код, який захищає ваш пароль. Важливо, що QR-код необхідно змінювати щомісяця.

ВИСНОВКИ ДО РОЗДІЛУ 4

У цьому розділі було розглянуто найпоширеніші методи злому паролів. Серед яких атака за словником — це техніка вгадування пароля за допомогою часто використовуваних слів. Під час атаки методом грубої сили зловмисник намагається зламати пароль, надсилаючи різні комбінації, доки не буде знайдено правильну. Атака із застосуванням райдужної таблиці. Коли ваші паролі зберігаються на сервері, вони шифруються в безглузді рядки символів замість того, щоб зберігатися як звичайний текст. Цей процес називається хешуванням і запобігає зловживанню вашим паролем.

Розглянуто найбільш поширені способи генерування паролів та порядок покращення методу генерування паролів. Для зберігання паролів запропоновано мати ідентифікаційну картку з QR-кодом, яку можна зберігати у своєму гаманці. Для отримання доступу до своїх паролів (переглядати їх безпосередньо), знадобиться ідентифікаційна картка та сканування її за допомогою захищеного паролем смартфоном. Після можна побачити необхідні паролі. Після того як Ви зайдете в телефон і відкриєте налаштовану програму для зчитування пароля QR, ви зможете просто отримати прямий доступ до своїх паролів замість рівня QR-коду.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день, спостерігається стрімкий розвиток телекомунікаційних систем та мереж, за рахунок збільшення потреб у використанні інформаційних технологій та об’ємів інформації, що передається. Телекомунікаційна інфраструктура передбачає гігабітне підключення, яке об’єднує загальні соціально-економічні інфраструктурні об’єкти такі як: школи, транспортні вузли, державні підприємства та інші.

Разом із тим підвищується ризик виникнення екологічних проблем, таких як електромагнітне забруднення, що має вплив як на живі організми, так і на організм людини.

5.1. Вплив електромагнітного забруднення на живі організми

У останні декілька десятків років використання пристроїв, що випромінюють ЕМП, значно зросло. Початок опанування людиною ЕМП пов'язаний з використанням діапазону довгих хвиль (довжина хвилі 1.10 км.), що було обумовлене розвитком радіозв'язку і радіомовлення в цьому діапазоні. Потім бурхливими темпами почало розвиватися телебачення, і діапазон довжин хвиль, що використовувались почав збільшуватися у сторону їх скорочення. На сьогодні, важко вказати таку область науки, техніки, господарства, де б не використовувалася радіоелектронна апаратура, зокрема випромінююча ЕМП.

До штучних джерел електромагнітного випромінювання відносять:

- лінії електропередач (ЛЕП):
- телевізійні та радіотрансляційні станції:
- радіолокаційні та радіонавігаційні установки;
- трансформатори високої частоти;
- вимірювальні, лабораторні та медичні прилади.

До *природних джерел* належать: Земля, Сонце, Космос. До антропогенних джерел належать радіотелевізійні, радіолокаційні станції, станції мобільного зв'язку, комп'ютери, високовольтні лінії електрозв'язку, електротранспорт, електростанції, , вимірювальні прилади, мікрохвильові печі, телевізори, електроплити.

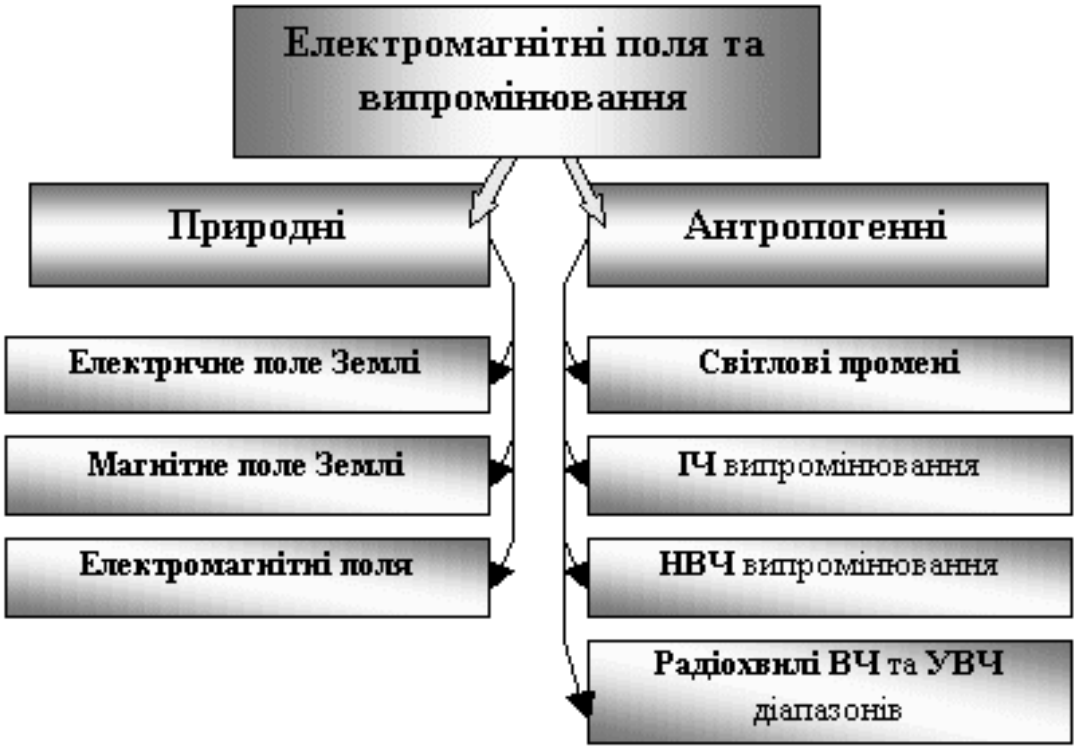


Рис. 5.1. Класифікація електромагнітних полів та вимірювань

Високочастотне поле від телекомунікаційних систем, радарів, високовольтних ліній електропередач вважається найбільш небезпечним. Можна вести дискусію про шкідливість чи безпечність впливу електромагнітного випромінювання, але в більшості Європейських країн, вже запроваджено заборону встановлювати Wi-Fi системи в школах,бібліотеках, лікарнях та інших громадських місцях. Замість того є пропозиція повернутись до дротових технологій.

Електромагнітні випромінювання антропогенного походження розглядають як один з різновидів енергетичних забруднювачів, оскільки вони негативно впливають на організм людини, на живі організми та здійснюють шкідливий вплив на екологічні системи. ЕМП мають енергію і поширюються у вигляді електромагнітних хвиль.

Шкідливий вплив електромагнітних полів на людину та на інші компоненти екосистем є прямо пропорційними потужності поля і часу опромінення. Негативний вплив електромагнітного поля, що формується ЛЕП, може бути виявлений при напруженості поля, яке має значення 1 кВ/м. У людини може спостерігатися порушення роботи ендокринної системи, обмінних процесів, а також порушення функції головного і спинного мозку.

На сьогодні, за даними екологів і лікарів є наявні відомості, що всі діапазони електромагнітного випромінювання впливають на здоров'я і працездатність людей і в майбутньому можуть мати негативні наслідки. Вплив електромагнітних полів на людину через їхню більшу розповсюдженість є у значній мірі небезпечні, у порівнянні з радіацією. Електричні поля промислової частоти перебувають в оточенні людини практично щоденно, через випромінювання від електропроводки, освітлювальних приладів, побутових електроприладів, ліній електропередач та інших. Спостерігається збільшення енергетичного навантаження від електромагнітних випромінювань в повсякденні та промисловості за рахунок розширення мережі джерел фізичних полів електромагнітної природи, і як наслідок зростання їхніх потужностей. Людина не має змоги фізично відчувати електромагнітне поле, яке перебуває в її оточенні, але воно може викликати зниження імунітету, працездатності, а також під його дією може розвиватися синдром хронічної втоми, та збільшуватися ризик виникнення інших захворювань. Насамперед вплив електромагнітних випромінювань є дуже небезпечним для дітей, підлітків, вагітних жінок, особливо вразливих людей та осіб, що мають хронічні захворювання. Інша вразлива група – це люди, професія яких включає в себе довгий час роботи з комп'ютерною технікою та електромагнітним випромінюванням (програмісти, системні адміністратори, оператори ПК, монтажники радіоелектронного обладнання і т. д.).

Принцип дії електромагнітного випромінювання на живі організми досі не вивчений до кінця. Можна виділити кілька припущень, які здатні пояснити біологічну дію електромагнітного поля. В більшості випадків вони зводяться до індиціюванню струмів в тканинах і прямому впливу поля на клітковому рівні, з

першочерговим впливом на мембранні структури. Є ймовірність, що під впливом електромагнітного поля може змінюватися швидкість дифузії через біологічні мембрани, до того ж, стан електронної структури вільних радикалів. Очевидно, що механізми біологічної дії електромагнітного поля мають здебільшого, звичний характер та мають зв’язок зі зміною активності регуляторних систем організму.

Підсумки досліджень, що оцінювали вплив мобільного телефону, комп’ютера і інших сучасних радіоелектронних засобів на різні живі організми як в робочому, так і у вимкненому стані виявились незадовільними і показали досить несприятливий вплив на стан біологічних об’єктів, а саме:

- зменшення рухомої активності і виживання мікроорганізмів;
- збільшення смертності мікроорганізмів;
- погіршення регенерації тканин;
- порушення розвитку ембріону;
- зниження біохімічних реакцій, порушення метаболізму;
- зниження енергетичного потенціалу життєво важливих систем організму.

5.2. Захист від електромагнітного забруднення

З огляду на активне поширення телекомунікаційних мереж, мобільного зв’язку, різноманітних технічних засобів, у групі ризику знаходиться 99,9 % населення Земної кулі. Тому питання захисту від електромагнітного випромінювання стає життєво необхідним. При цьому велика роль виділяється санітарному нагляду за джерелами випромінювання.

Організація санітарного нагляду ґрунтується на санітарних нормах і правилах, що базуються на обов'язкових нормах та основних положеннях гігієнічних вимог до розташування засобів застосування джерел випромінювання.

Під час розробки засобів захисту від впливу ЕМП можна виділити такі аспекти як:

- зменшення інтенсивності опромінювання особисто від самого джерела опромінювання;

- екранування робочого місця або віддалення його від джерела опромінювання;
- застосування засобів індивідуального захисту.

Основні вимоги для засобів захисту від дії ЕМП: не викривляти істотно електромагнітне поле; не знижувати якості технічного обслуговування і ремонту; не знижувати ефективності праці.

Одним з найефективніших способів зменшення інтенсивності випромінювання людей на підприємстві є віддалення робочого місця від джерела випромінювання. Він реалізується за допомогою дистанційного керування і автоматизованого контролю за роботою.

В якості індивідуального захисту від ЕМП найкраще підходить спеціальний одяг – комбінезони, халати та інше. Проте найбільш дієвим способом захисту від електромагнітних випромінювань є встановлення відбиваючих або поглинаючих екранів. Якщо ви мешкаєте або знаходитися в місцевості, де працюють різноманітні джерела випромінювання ЕМП, слід дотримуватися наступних правил:

- не перебувати поблизу їх джерел та випромінювачів;
- не знаходитися, не відпочивати, не використовувати земельні ділянки поблизу ліній передачі електроенергії та трансформаторних підстанцій;
- по можливості уникати близького контакту з працюючими електронними потужними приладами, телевізорами, комп'ютерами, мобільними телефонами;
- при користуванні засобами мобільного зв'язку не намагатися вставити антену передавача в вухо. Набагато краще тримати цей засіб так далеко, щоб тільки було чути вашого кореспондента;
- обмежувати використання одягу з синтетичних тканин; в першу чергу це стосується білизни, шкарпеток та ін. Краще їх замінити тканинами з бавовни та льону;
- у випадку неможливості уникнення впливу ЕМП, треба захищати в першу чергу очі, голову та шию шляхом використання спеціальних поглинаючих або відбиваючих окулярів, халатів, шоломів та різноманітних накидок. Для захисту

житла чи присадибної ділянки, де ви працюєте, можливо також використовувати металеві сітки, що мають щільні ґратки, які необхідно добре заземлити в певних місцях.

5.3. Проблема електронного сміття

На сьогодні, головною екологічною проблемою в сучасному світі можна вважати проблему електронних відходів. Щороку у всьому світі утилізується близько 40 мільйонів тонн електронних відходів, а по факту кожної секунди викидається близько 800 ноутбуків. Однак лише 12,5% з цих відходів в подальшому потрапляють на переробку, решта відправляється на сміттєзвалища або спалюється. При цьому токсичні сполуки, які містяться в комп’ютерних компонентах, забруднюють нашу землю, повітря та воду.

Проте небезпека полягає не тільки в забрудненні навколишнього середовища, а й у спричиненні проблем кібербезпеки через неправильне очищення пам’яті пристроїв. Комп'ютери зберігають багато особистих даних таких як конфіденційні документи або фінансова інформація. Якщо недотриматися правил повного видалення даних з ПК інформація може бути відновлена та використана в зловмисних цілях.

Комп’ютерне обладнання містить в собі багато елементів, що мають токсичні речовини, шкідливі для життя людини. Найбільш небезпечний – свинець, що застосовується при виготовленні електронно-променевих трубок та осцилографічних ламп. Проблема, що виникає при зберіганні небезпечних компонентів комп'ютерного обладнання, з'являється через те, що елементи дістаються неналежним чином, без дотримання основних заходів безпеки, а особи, що здійснюють це, можуть бути схильні до різних захворювань.

Ртуть використовується в деяких люмінесцентних лампах. Потрапляючи в мозок, вона може викликати порушення мови, зору і слуху, а також впливати на координацію рухів не найкращим чином. У старих пристроях може перебувати

фреон, який використовується в основному в системах кондиціювання повітря. Його використання вже заборонено через негативний вплив на озоновий шар Землі.

Сполуки брому, що застосовуються в комп'ютерній індустрії, є джерелом проблем з неврологією. Хронічне отруєння може викликати утруднення в мові, апатію і втрату пам'яті. Нікель, розташований в електронно-променевих трубках, батарейках або гальванічних покриттях, викликає зміни в кістковому мозку, пошкодження слизових оболонок, сприяє утворенню пухлин.

Це тільки деякі з небагатьох небезпечних речовин, які можна знайти в корпусі комп'ютерного обладнання. Дуже вагомим кроком для вирішення даної проблеми є усвідомлення масштабів загрози. Тільки одна батарея може забруднити до кубічного метра ґрунту і до чотирьохсот літрів води.

Хоча шкідливі речовини зустрічаються в приладах в невеликих кількостях загроза від них, як правило, не обмежується лише отруєнням при безпосередньому контакті. Неправильне зберігання або перероблені комп'ютери в першу чергу небезпечні для навколишнього середовища. Шкідливі речовини можуть потрапити в ґрунт, а потім - в ґрунтові води. Вони повернуться до людей у вигляді кислотних дощів або рослин, які отримують поживні речовини з ґрунту. У цілому, в межах України до атмосфери та ґрунтових вод від електронних відходів щороку потрапляє понад 40 кг ртуті, 160 кг кадмію, 400 т інших важких металів, 260 т сполук марганцю. Проблема зростає і починає безпосередньо загрожувати людині.

Найкращим вирішенням даної проблеми є утилізація комп’ютерної техніки, що здійснюється згідно з чинним законодавством України та дотриманням технологічних регламентів. Варто зауважити, що компанії, які займаються утилізацією електронних компонентів повинні мати відповідні ліцензії. До того ж звичайний комп’ютер містить в собі також і цінні метали, а сучасні технології дозволяють виділити і отримати з нього дорогоцінні метали такі як: золото, срібло, платина і паладій. Також компоненти комп’ютера можуть включати в себе речовини, що можуть використовуватися як вторинна сировина.

На сьогоднішній день в Україні існує велика проблема з утилізацією електронних відходів, оскільки в країні відсутня централізована система збору і

передачі на утилізацію відпрацьованої техніки. На даний час налічується всього лише півтора десятка підприємств, що займаються переробкою різного виду електронних відходів, та мають необхідний пакет ліцензій.

ВИСНОВКИ ДО РОЗДІЛУ 5

При дослідженні впливу електромагнітного випромінювання, яке надходить від комп'ютерного обладнання, з'ясовано, що ЕМП дуже негативно впливає на навколишнє середовище, зокрема і на людину. Кількість осіб, що мають контакт з надмірним випромінюванням ЕМП, невпинно збільшується. Проблема полягає не тільки в наявності радіохвиль, а й в підвищенні їх інтенсивності та зміні характеру випромінювання. Для захисту від негативного впливу електромагнітного випромінювання необхідно слідувати санітарним нормам і правилам, що базуються на основних положеннях гігієнічних вимог до розташування засобів застосування джерел випромінювання. Одним з найефективніших способів зменшення інтенсивності випромінювання людей на підприємстві є віддалення робочого місця від джерела випромінювання.

Ще однією не мало важливою проблемою та серйозною загрозою для навколишнього середовища є електронні відходи. Комп'ютерне обладнання містить в собі багато елементів, що мають токсичні речовини, шкідливі для життя людини, тому дуже важливим є утилізація відпрацьованої техніки. На сьогодні в Україні, на жаль, бракує організацій по прийому та переробці електронних відходів, які б мали всі необхідні ліцензії. Вирішення цієї проблеми може бути організація безкоштовних точок збору техніки, або щоб виробники техніки забезпечували утилізацію, коли техніка вийде з ладу. Це може бути забезпечено тільки на державному рівні.

РОЗДІЛ 6
ОХОРОНА ПРАЦІ

Стрімкий розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. На сьогодні, важко уявити підприємства, діяльність в яких здійснювалась би без використання комп'ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, а саме: правилами охорони праці під час експлуатації електронно-обчислювальних машин, затверджені, наказом Державного комітету України з промислової безпеки, охорони праці та гірничого нагляду 26.03.2010 N 65 та Державними санітарними правилами і нормами роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджені Постановою Головного державного санітарного лікаря України від 10 грудня 1998 р. №7.

З огляду на тему дипломного проєкту доцільним є обрати професію суб'єкта – фахівець з кібербезпеки, робочим місцем якого є персональний комп'ютер, розташований у офісному приміщенні.

6.1. Аналіз умов праці

Робота за ПК передбачає розумову працю, що зазвичай здійснюється ву відносно нерухомому стані. При цьому спостерігається висока рухливість кистей рук, та висока напруга зорових і нервово-емоційних функцій при дії різноманітних фізичних чинників.

Приміщення, в яких планується установка та подальша робота з комп'ютером, повинні відповідати проєктній документації будинку, погодженій з уповноваженими державними органами. Крім того, обов'язково повинно бути враховано існуючі санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура,

відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Конкретні показники зазначених санітарних норм вказані у Державних санітарних правилах і нормах.

До прикладу, існують заборони на встановлення комп'ютерної техніки в приміщеннях, розташованих у підвалах будинків та на нульовому поверсі. Приміщення, в яких наявні відеодисплейні термінали повинні бути укомплектовані системами центрального або індивідуального опалення, кондиціювання чи вентиляції повітря. Проте, при встановленні вище зазначених систем, необхідно переконатись, що вони перебувають під надійними захисними щитками, які зможуть попередити під падання робітника під напругу.

Досить непростим завданням є планування та розміщення комп'ютерної, яке включає в себе: правильне розміщення робочого місця у приміщенні, вибір виробничого положення, раціонального компонування комп'ютерного обладнання, урахування своєрідних властивостей трудової діяльності.

Площа, на якій розташовується одне робоче місце з відео дисплейним терміналом (ВДТ), має бути як мінімум 6,0 м^2, а приміщення з об'ємом , не менше 20 м^3. Робочі місця з ВДТ розташовується на відстані не менше 1 м від стіни зі світловими прорізами. Відстань між бічними поверхнями ВДТ має бути не менше 1,2 м; відстань між тильною поверхнею одного ВДТ та екраном іншого не повинна бути меншою за 2,5 м; прохід між рядами робочих місць має бути не менше метра. Важливим аспектом є врахування розмірів меблів для робочих місць обладнаних комп'ютерами, тобто висота 725 мм, ширина 600 – 1400 мм, глибина 800 – 1000 мм. Крім того, розміри столу для ВДТ складають: ширина – 1200 мм, глибина – 800 мм (рис. 6.1.). Слід зауважити, що розміщення відео терміналів є надзвичайно важливим. Для уникнення дзеркального відображення на екрані ВДТ джерел природного освітлення, їх варто розмістити впродовж стіни з вікнами.

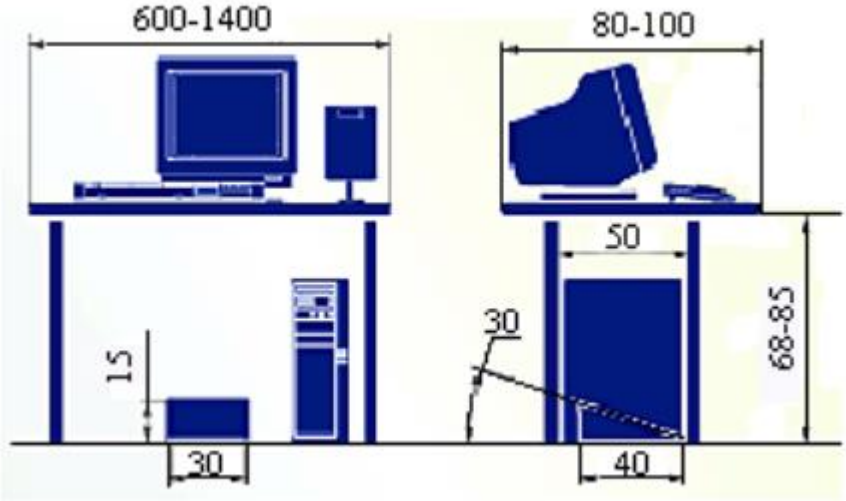


Рис. 6.1. Розміри для організації робочого місця при використанні комп'ютера

Розміщення комп’ютера, клавіатури та принтера на місці роботи є значущим аспектом у гарантуванні безпеки праці користувачів комп'ютерів. Розташування екрана (дисплея) має підтримувати комфорт зорового спостереження у вертикальній площині під кутом близько 30° від лінії зору оператора. Найбільш сприятливі зорові умови для розпізнавання цифр та символів, коли верхній край комп’ютера знаходиться на рівні очей, а погляд направлений вниз на центр екрану. Екран комп’ютера теж має бути нахилений назад на 20° від вертикалі. Екран комп’ютера та клавіатура слід розташовувати на найбільш сприятливій відстані від очей користувача комп'ютера, проте не ближче ніж 600 мм, враховуючи розмір букв та цифрових знаків та символів. Наприклад якщо розмір екрана по діагоналі 35 см, то відстань від монітора до очей повинна бути 60 – 70 см, при діагоналі 43 см – 70 см.

На поверхні робочого стола для клавіатури комп'ютера слід виокремити простір для переміщення та поворотів. Розміщення клавіатури та кут її нахилу вибираються індивідуально під кожного користувача комп'ютера. Кут нахилу клавіатури може коливатися у межах 5 – 10°. Також можна розміщувати клавіатуру на спеціальній робочій поверхні, окремо від столу.

Розміщення принтера або іншого пристрою введення-виведення інформації на місці роботи має забезпечувати гарну видимість екрану комп'ютера,

комфортабельність ручного управління пристроєм введення-виведення інформації в зоні досяжності моторного поля (висоті 900 - 1300 мм, глибина 400 – 500 мм).

6.2. Перелік та аналіз шкідливих та небезпечних виробничих чинників

При тривалому використанні комп'ютерної техніки можна виділити такі шкідливі чинники:

- Неіонізуюче випромінювання;
- Мікроклімат у приміщенні**;**
- Робоча поза.
- Напруженість праці.

Неіонізуюче випромінювання. Дуже часто, роботу працівників з ПК пов'язують зі негативним впливом електромагнітних полів. Це відноситься до моніторів з електронно-променевою трубкою. Сучасні комп'ютери мають рідкокристалічні монітори, тому вплив електромагнітного поля від монітора несуттєвий. Присутнім лишається електростатичне поле на поверхні монітора та поверхні клавіатури. Нормоване значення напруженості електростатичного поля дорівнює 150 В/см, зазвичай, не є вищим за нормоване значення. Рівень напруженості електростатичного поля залежить від таких параметрів як: вологість повітря, наявність регулярного прибирання робочого місця (усунення запиленості).

Мікроклімат у приміщенні. У теплу пору року температура повітря коливається у межах 22-25°С, швидкість руху повітря — до 0,1 м/с, відносна вологість повітря — 40-60%. У холодний пору року температура повітря може бути у межах 21-24 °С, швидкість руху повітря — до 0,1 м с, вологість повітря — 40-60%.

Для робочої зони працівників з ПК, які працюють в офісних центрах з централізованим забезпеченням повітря, як влітку, так і взимку типові значення відносної вологості повітря коливаються в межах 20-40%, та спостерігається зниження або підвищення швидкості руху повітря робочої зони.

Через постійне нагрівання деталей ПК та знижену вологість, температура повітря здебільшого є більшою за нормативні значення протягом року. Саме

температура та вологість повітря мають вплив на загальне самопочуття, стан слизових оболонок очей, верхніх дихальних шляхів та шкіри персоналу офісних приміщень. Низька вологість підвищує час «зависання » пилу в повітрі приміщення.

До параметрів повітря робочої зони користувачів ПК можна віднести такі, як вміст позитивних та негативних іонів у повітрі. В більшості випадків, у приміщеннях, що мають більш розвинену систему припливно-витяжної вентиляції та/або з кондиціонерами проявляється порушення норм аероіонного складу повітря, при тому що концентрація корисних для організму негативно заряджених аероіонів може бути в 10-50 разів менше норми, а концентрація шкідливих позитивних аероіонів значно перебільшувати норму. Через це дуже важливим є надходження свіжого повітря до робочого місця за комп'ютером.

У сучасних офісних приміщеннях з центральною вентиляцією і відсутності провітрювання приміщень, створення відповідної аероіонізації є доволі складним завданням.

Варто зауважити, що серед офісних працівників спостерігається високий рівень захворюваності з тимчасовою втратою працездатності, при чому захворювання органів дихання складають 45-60%. За даними медичних установ, серед офісних працівників значно поширені захворювання ЛОР-органів (до 25% працівників), при цьому мають перевагу ураження верхніх дихальних шляхів, а саме: хронічні катаральні фарингіти (15,7%). Варто додати високу частоту розвитку алергічних ринітів (1,3%), що у декілька разів є вищою за середню по Україні (0,28%).

Робоча поза. Даний чинник трудового процесу напряму залежить від правильної організації робочого місця для забезпечення зручної робочої пози, оскільки «закам'яніле» положення чинить негативний вплив на хребтово-м'язову систему. Стіл має бути широким та просторим, обов'язково маючи спеціальну підставку для ніг, а робочий стілець мати можливість відрегулювати висоту, певний кут нахилу сидіння і спинки. За час роботи за комп'ютером людина сидить по декілька годин поспіль у незручному положенні. Це в свою чергу викликає загальну втому, а також може призвести до розвитку остеохондрозу різних ділянок хребта —

шийного, грудного, попереково-крижового. Помилкове положення рук під час роботи за клавіатурою може призвести до хронічних захворювань кисті. Через це клавіатура має розміщуватися на відстані як мінімум 10-15 см від краю стола.

Для того щоб робота за комп'ютером не наносила шкоди здоров'ю, дуже важливо постійно стежити за своєю поставою. Правильна постава дозволяє максимально розвантажити м'язи тіла і працювати якомога довше, при цьому менше втомлюватися.

Напруженість праці. Напруженість праці осіб, що працюють з ПК, перш за все пов'язана з напруженістю очей, тривалістю зосередження уваги, що може сягати понад 75% всього часу роботи за комп'ютером. Важливе значення при роботі за комп'ютером мають: відстань до екрана, шрифт, розмір тексту на моніторі, наявність або відсутність мерехтіння, яскравість екрана, освітлення робочого місця, наявність перерви у роботі. Для збереження здоров'я працівників, запобігання професійним захворюванням і підтримки працездатності слід влаштовувати перерви для відпочинку: для розробників програм — 15 хв. через кожну годину роботи за комп'ютером; для операторів ЕОМ — 15 хв. через кожні 2 год.; для операторів комп'ютерного набору — 10 хв. після кожної години роботи. Саме ігнорування таких простих на перший погляд правил здебільшого призводить до погіршення зору та хвороб очей.

6.4. Розробка заходів з охорони праці

Електробезпека комп'ютерного обладнання. Під час проектування систем електропостачання, монтажу основного електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог Правил пожежної безпеки в Україні та інших нормативних документів, що стосуються штучного освітлення і електротехнічних пристроїв, а також вимог нормативно-технічної експлуатаційної документації заводу-виробника.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинна

виконуватися як окрема групова три провідна мережа, з використанням фазового, нульового робочого та нульового захисту провідників. Для заземлення (занулення) електроприймачів застосовується нульовий захисний провідник і прокладається від стійки групового розподільчого щита до розеток живлення.

У приміщенні, де використовується чи обслуговується більш ніж п'ять персональних ЕОМ одночасно, в доступному місці обов’язково встановлюється аварійний резервний вимикач, який у разі необхідності може повністю вимкнути електричне живлення приміщення, за винятком освітлення.

Не допускається підключення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ до звичайної двопровідної електромережі, зокрема не варто застосовувати перехідні пристрої.

При розташуванні в приміщенні за його периметром до 5 персональних ЕОМ, з використанням три провідникового захищеного проводу або кабелю в оболонці з негорючого або матеріалу, що важко горить допускається прокладання їх без металевих труб та гнучких металевих рукавів. Заземлені конструкції, що знаходяться у приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), повинні бути дуже добре захищені діелектричними щитками або сітками від ненавмисного торкання.

Нормалізація повітря робочої зони. Насамперед для створення оптимальних метеорологічних умов необхідно зменшити тепловиділення в джерелі, що певною мірою передбачено при конструюванні. ЕОМ повинні бути розташовані так, щоб теплові потоки від них не були спрямовані на оператора або його сусідів. За можливості слід обмежити кількість ЕОМ в одному приміщенні. Також не варто використовувати опалювальні системи, що знаходяться на підлозі.

Для забезпечення нормованих метеорологічних умов використовуються опалення, кондиціювання повітря і припливно-витяжну вентиляцію. Крім того застосовують установки або прилади зволоження та штучної іонізації. Також вологе прибирання має проводитися не менше одного разу на день. Оскільки позитивні іони здатні з’єднуватися з частинкам пилу, рекомендується протирати поверхню

столу серветкою з антистатиком. За можливості робити часті провітрювання приміщення.

Виробниче освітлення. Приміщення, в яких присутні ПК, система освітлення має бути з дотриманням таких умов:

- освітленість на місці роботи має бути у відповідності з характером зорової роботи, що можна визначити по трьом параметрам: об'єкт розрізнення – мінімальний розмір об'єкту, що можна побачити на моніторі ПК; фон, з головною характеристикою, якого є коефіцієнт відбиття; контраст об'єкту і фону;
- потрібно забезпечити наскільки це можливо рівномірне розподілення яскравості на робочій поверхні монітору, та в межах навколишнього простору;
- на робочій поверхні не має бути різких тіней;
- в зоні видимості не має бути прямих і відбитих відблисків (збільшеної яскравості поверхонь, що світяться та можуть викликати осліплення);
- величина освітленості повинна незмінною у часі;
- необхідно обирати найкращу спрямованість світлового потоку і відповідний склад світла.

При роботі з документами значення освітленості на робочій поверхні коливається в межах 300-500 лк. При штучному освітленні в якості джерела світла здебільшого використовуються люмінесцентні лампи типу ЛБ. Застосування метало галогенних ламп потужністю 250 Вт є допустимим у випадку влаштування відбитого освітлення у виробничих та адміністративно-громадських приміщеннях.

6.5. Пожежна безпека

Основним заходом для попередження пожеж і вибухів від електрообладнання є вибір правильного обладнання та його експлуатація у приміщеннях. Головними нормативними документами , які регулюють вимоги до пожежної безпеки є Закон України «Про пожежну безпеку», Правила пожежної безпеки в Україні.

Відповідно до правил улаштування електроустановок, в пожеже небезпечних зонах використовується електрообладнання закритого типу, внутрішній простір якого є відділеним від зовнішнього середовища оболонкою. Апаратуру управління і захисту, світильники слід використовувати пилонепроникні. Вся електропроводка повинна мати надійну ізоляцію. У вибухонебезпечних зонах та в зовнішніх установках все обладнання має бути вибухозахищене. Дроти у вибухонебезпечних приміщеннях повинні прокладатися у металевих трубах. Як варіант може застосовуватися броньований кабель. Світильники для класів В-I, В-II, В-IIа обов'язково мають бути захищені від вибухів.

При аналізі обставин пожеж можна зауважити, що однією з головних причин виникнення пожеж є людський фактор.

Найбільш розповсюджені і типові причин пожеж:

- наявність недосконалостей технологічних процесів;
- помилки при здійсненні монтажу електрообладнання;
- упущення при облаштуванні та обслуговуванні опалювальних систем;
- неприпустиме зростання температури речовин, що можуть сягнути до температури самозаймання;
- порушення режиму зберігання, транспортування та обробки самозаймистих речовин;
- розряди блискавки та занесення високих потенціалів у виробничі приміщення;
- поява горючого середовища в межах джерела займання;
- халатне ставлення до вимог нормативних документів, необережне поводження з вогнем, необізнаність з правилами пожежної безпеки, низький рівень кваліфікації та інші.

Офісне приміщення відноситься до класу В-Іа, в яких вибухонебезпечна концентрація газів і пари може бути лише внаслідок аварії або несправності.

До первинних засобів пожежогасіння відносять: вогнегасники; ящики з піском; бочки з водою; покривала з негорючого матеріалу. Найбільш ефективним способом на початку боротьби з пожежею вважається вогнегасник.

В якості засобу пожежної сигналізації можна використати ручний пожежний сповіщувач полум’я, що розташовується всередині будівлі на стіні або конструкціях на висоті (1,5 ± 0,05) м від рівня землі або підлоги до нижнього краю сповіщувача, в легкодоступних місцях.

У разі виявлення будь-яких ознак загоряння (диму, запаху, полум’я) необхідно негайно повідомити про це органи пожежної охорони, або керівника, а також задіяти систему оповіщення і вжити необхідних заходів щодо евакуації людей, в подальшому приступити до гасіння пожежі та за можливості збереження матеріальних цінностей.

6.6. Розрахункова частина

Перевірочний розрахунок штучного освітлення офісного приміщення.

Скористаємося методом використання світлового потоку. Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F = \frac{E \cdot S \cdot Z \cdot K}{N \cdot n \cdot \eta} \qquad (6.1)$$

F – світловий потік, що розраховується, Лм; (E·S·Z·К)/(N·n·η);

E – нормована мінімальна освітленість, Лк;

S – площа освітлюваного приміщення (у нашому випадку S=20 м^2);

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1... 1,2, в нашому випадку Z =1,1);

К – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку К = 1,6);

η – коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх

ламп, і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{ст.}$) і стелі ($\rho_{стелі}$) значення коефіцієнтів дорівнюють $\rho_{стін}$ = 50% і $\rho_{стелі}$ = 70%, $\rho_р$ = 0.)

Обчислимо індекс приміщення за формулою:

$$I = \frac{S}{h \cdot (A+B)} \quad (6.2)$$

S – площа приміщення, S = 20 м^2; h – розрахункова висота підвісу, h = 3,8 м; A – ширина приміщення, A = 5 м; B – довжина приміщення, B = 4 м.

Підставивши значення у формулу 6.2 отримаємо:

$$I = \frac{5 \cdot 4}{3.8 \cdot (5+4)} = 2 \text{ м}$$

Знаючи індекс приміщення I, знаходимо η = 56, світильник групи 1 та тип лампи ЛД 20-4, F=920 лм, знаходимо необхідну кількість світильників за формулою 6.1:

$$N = \frac{300 \cdot 20 \cdot 1{,}5 \cdot 1{,}1}{2 \cdot 920 \cdot 0{,}56} = 9{,}6$$

Отже, необхідно взяти 10 світильників, розмістивши їх в два ряди по 5 штук.

ВИСНОВКИ ДО РОЗДІЛУ 6

Стрімкий розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. На сьогодні, важко уявити підприємства, робота, яких здійснюється без використання комп’ютерної техніки. Саме тому дуже важливим є питання охорона праці користувачів комп’ютерного обладнання.

При тривалому використанні комп’ютерної техніки можна виділити такі шкідливі чинники як: неіонізуюче випромінювання; мікроклімат у приміщенні**;** робоча поза та напруженість праці. Тривала робота за комп'ютером – це дуже велике навантаження на очі. У користувача спостерігається погіршення зору, очі

починають сльозитися, з'являється головний біль, втома, зображення двоїться і спотворюється. Тривале сидяче положення може призводити до напруги м'язів шиї, голови, рук і плечей, і як наслідок до остеохондрозу.

З ціллю запобігання або зменшення впливу шкідливих і небезпечних чинників застосовують засоби колективного та індивідуального захисту. Засоби колективного захисту призначені для: нормалізації повітряного середовища приміщень і робочих місць (вентиляція, кондиціювання, опалення, автоматичний контроль і сигналізація); нормалізації освітлення виробничих приміщень і робочих місць (джерела світла, освітлювальні прилади, світлозахисне об ладнання, світлофільтри); захисту від іонізуючих, інфрачервоних, ультрафіолетових, електромагнітних, лазерних, магнітних та електричних полів (огородження, герметизація, автоматичний контроль і сигналізація, дистанційне керування, засоби індивідуального захисту тощо); дотримання правил пожежної безпеки.

Також було здійснено перевірочний розрахунок штучного освітлення офісного приміщення. Скорившись методом використання світлового потоку було визначено необхідну кількість світильників, які повинні забезпечити нормований рівень освітленості в офісному приміщенні.

ВИСНОВКИ

У першому розділі було розглянуто класифікацію бездротових мереж. Серед яких найбільш популярною та використовуваною є (WLAN - wireless local area network), іншою назвою яких є Wi-Fi. Головна функція таких систем – розгортання бездротових мереж усередині приміщень, проте є можливість їх застосування на відкритих майданчиках. Основна послуга – доступ в Internet або корпоративну мережу.

Також було розглянуто основні стандарти бездротового зв’язку серед яких стандарти сімейства IEEE 802.11. Для наглядності та розгляду потенціалу і функціональної спроможності стандартів бездротових мереж передачі інформації наведено таблицю, в якій наведені такі параметри як, швидкість передачі даних, дальність дії, частотний діапазон та технологія модуляції. Стандарт IEEE 802.11n має найкращі характеристики у порівнянні з іншими стандартами., саме тому він є найбільш застосованим для організації в житлових будинках та на відкритій місцевості.

В другому розділі було розглянуто основні загрози та вразливості для бездротових мереж. Загрози пов'язані з тим, що для злому дротової мережі, зловмиснику потрібен прямий доступ до кабелю, який набагато складніше отримати, ніж перехопити радіосигнал за допомогою спеціальних пристроїв. Крім того, часто бездротові мережі працюють навіть без базового захисту паролем.

Серед основних типів атак, які загрожують безпеці бездротової комп'ютерної мережі можна виділити: DDoS-атаки; помилкова точка доступу; «людина посередині»; атаки на мережеве обладнання.

В третьому розділі було розглянуто основні стандарти безпеки бездротових мереж такі як: WEP, WPA, WPA2, та WPA3. Проаналізувавши характеристики та особливості вищезазначених протоколів безпеки можна зробити висновки, що протокол WEP має низький рівень захисту та багато проблем із безпекою, через які ключі легко зламати, тому його використовувати не варто.

В четвертому розділі було розглянуто найбільш поширені способи генерування паролів та порядок покращення методу генерування паролів. Для зберігання паролів запропоновано мати ідентифікаційну картку з QR-кодом, яку можна зберігати у своєму гаманці. Для отримання доступу до своїх паролів (переглядати їх безпосередньо), знадобиться ідентифікаційна картка та сканування її за допомогою захищеного паролем смартфоном. Після можна побачити необхідні паролі. Після того як Ви зайдете в телефон і відкриєте налаштовану програму для зчитування пароля QR, ви зможете просто отримати прямий доступ до своїх паролів замість рівня QR-коду.

При дослідженні впливу електромагнітного випромінювання в п’ятому розділі, яке надходить від комп’ютерного обладнання, з’ясовано, що ЕМП дуже негативно впливає на навколишнє середовище, зокрема і на людину. Кількість осіб, що мають контакт з надмірним випромінюванням ЕМП, невпинно збільшується. Проблема полягає не тільки в наявності радіохвиль, а й в підвищенні їх інтенсивності та зміні характеру випромінювання. Для захисту від негативного впливу електромагнітного випромінювання необхідно слідувати санітарним нормам і правилам, що базуються на основних положеннях гігієнічних вимог до розташування засобів застосування джерел випромінювання. Одним з найефективніших способів зменшення інтенсивності випромінювання людей на підприємстві є віддалення робочого місця від джерела випромінювання.

В шостому розділі було розглянуто основні питання з охорони праці. При тривалому використанні комп’ютерної техніки можна виділити такі шкідливі чинники як: неіонізуюче випромінювання; мікроклімат у приміщенні**;** робоча поза та напруженість праці. Тривала робота за комп'ютером – це дуже велике навантаження на очі. У користувача спостерігається погіршення зору, очі починають сльозитися, з'являється головний біль, втома, зображення двоїться і спотворюється. Також було здійснено перевірочний розрахунок штучного освітлення офісного приміщення. Скориставшись методом використання світлового потоку було визначено необхідну кількість світильників, які повинні забезпечити нормований рівень освітленості в офісному приміщенні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Щербаков В. Б. БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ: СТАНДАРТ IEEE 802.11 / В. Б. Щербаков, С. А. Ермаков. – М: РадиоСофт, 2010. – 255 с.

2. What are the different types of network? [Електронний ресурс]. – Режим доступу до ресурсу: https://afteracademy.com/blog/What-are-the-different-types-of-network

3. The evolution of Wi-Fi standards: a look at 802.11a/b/g/n/ac/ax [Електронний ресурс]. – Режим доступу до ресурсу: https://www.actiontec.com/evolution-wi-fi-standards-look-802-11abgnac/

4. Matthew S. Gast. 802.11 Wireless Networks: The Definitive Guide, Second Edition 2nd Edition – O'Reilly Media, Inc., 2005. – 672 с.

5. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.

6. Examining 5 IEEE Protocols - ZigBee, WiFi, Bluetooth, BLE, and WiMax [Електронний ресурс]. – Режим доступу до ресурсу:https://www.iotforall.com/ieee-protocols-zigbee-wifi-bluetooth-ble-wimax

7. Wolfgang Osterhage. Wireless Network Security: Second Edition 2nd – CRC Press, 2018. – 184 с.

8. Wireless Security Vulnerabilities [Електронний ресурс]. – Режим доступу до ресурсу:https://www.streetdirectory.com/travel_guide/2497/computers_and_the_internet/wireless_security_vulnerabilities.html

9. Man in the middle (MITM) attack [Електронний ресурс]. – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

10. State of Password Use Report 2020 [Електронний ресурс]. – Режим доступу до ресурсу: https://www.balbix.com/resources/state-of-password-use-report-2020/

11. Top 200 most common passwords 2020 [Електронний ресурс]. – Режим доступу до ресурсу: https://nordpass.com/most-common-passwords-list/

12. The 9 Most Common Security Threats to Mobile Devices in 2021 [Електронний ресурс]. – Режим доступу до ресурсу: https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

13. Різниця між паролями WEP, WPA і WPA2 Wi-Fi [Електронний ресурс]. – Режим доступу до ресурсу: https://ua.phhsnews.com/articles/howto/the-difference-between-wep-wpa-and-wpa2-wi-fi-passwords.html

14. Security [Електронний ресурс]. – Режим доступу до ресурсу: https://www.wi-fi.org/discover-wi-fi/security

15. Wi-Fi Security: WEP vs WPA or WPA2 [Електронний ресурс]. – Режим доступу до ресурсу: https://www.avast.com/c-wep-vs-wpa-or-wpa2

16. 5 Common Password-Cracking Techniques [Електронний ресурс]. – Режим доступу до ресурсу: https://www.digitalprivatevault.com/blogs/password-cracking-techniques

17. How an 8-character password could be cracked in less than an hour [Електронний ресурс]. – Режим доступу до ресурсу: https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/

18. How to Create a Strong Password in 7 Easy Steps [Електронний ресурс]. – Режим доступу до ресурсу: https://terranovasecurity.com/how-to-create-a-strong-password-in-7-easy-steps/

19. Вплив електромагнітного випромінювання на живі організми [Електронний ресурс]. – Режим доступу до ресурсу: https://doza.net.ua/pages/ua_ref_emf.htm

20. Ефективні засоби захисту від електромагнітних полів. [Електронний ресурс]. – Режим доступу до ресурсу: https://simvolt.ua/efektivni-zasobi-zakhistu-vid-elektromagnitnikh-poliv.-zberezhit-zdorovya-svoyikh-ditey/