Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет прикладних інформаційних технологій та електроінженерії
(назва факультету)
Кафедра радіотехнічних систем
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

Магістр
(освітньо-кваліфікаційний рівень)

на тему: **Обґрунтування методів захисту Wi-Fi мережі від несанкціонованого доступу**

Виконав: студент (ка) 6 курсу, групи РРм-61
спеціальності (напряму підготовки) 172
“Телекомунікації та радіотехніка”
(шифр і назва спеціальності (напряму підготовки))

(підпис) Процик П.П (прізвище та ініціали)

Керівник (підпис) Умзар Ю.А. (прізвище та ініціали)

Нормоконтроль (підпис) Дедів І.Ю. (прізвище та ініціали)

Рецензент (підпис) Хвостівський М. О. (прізвище та ініціали)

Тернопіль – 2019

АНОТАЦІЯ

Процик Павло Петрович:. Обґрунтування методів захисту Wi-Fi мережі від несанкціонованого доступу. – Рукопис.

Дипломна робота магістра за спеціальністю 172 Телекомунікації та радіотехніка, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2019.

Дипломна роботі магістра присвячена вирішенню актуальної науково-практичної проблеми розробки методів забезпечення інформаційної і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів для підвищення рівня її захищеності від загроз безпеці різноманітного характеру, що полягають у розроблених теоретичних основах, методах, моделях та засобах забезпечення надійної роботи безпроводових систем та мереж.

Ключові слова: безпроводова інфраструктура, інтернет речей, надійність, доступність, цілісність, ефективність, пропускна здатність, інформаційна безпека.

ANNOTATION

Protsyk Pavlo Petrovych :. Rationale for methods to protect Wi-Fi network from unauthorized access. - Manuscript.

Master's diplom work on specialty 172 Telecommunications and Radio Engineering, Ternopil National Technical University Pulyy, Ternopil, 2019.

The master's thesis is devoted to solving the actual scientific and practical problem of developing methods of providing information and functional security of wireless infrastructure on the basis of hardware separation of subscribers to increase the level of its protection against security threats of various nature, which consist in the developed theoretical bases, methods, models and tools wireless systems and networks.

Keywords: wireless infrastructure, internet of things, reliability, availability, integrity, efficiency, bandwidth, information security.

ЗМІСТ

ВСТУП

Актуальність теми. Для передачі інформації між її користувачами все частіше застосовуються безпровідні мережі. Вони розгортаються, як правило, в аеропортах, університетах, готелях, ресторанах, на підприємствах та слугують для підключення користувачів до мереж провайдерів інтернет-послуг, а також об'єднання просторово рознесених підмереж в одну загальну мережу - тобто там, де кабельне з'єднання підмереж неможливе або небажане.

Такі зміни ведуть до того, що світ стає надто уразливим від появи нових деструктивних впливів - викликів, загроз та, фактично, неприхованих кібернетичних злочинів в IT сфері, які зумовлюють, як результат, збільшення частоти нападів та збитків від витоку інформації. Зважаючи, що основи такої діяльності на даний час формалізовано недостатньо, питання щодо забезпечення інформаційної та функціональної безпеки безпроводових мереж є надзвичайно актуальними.

Відомо, що вирішенню проблеми інформаційної та функціональної безпеки в цілому, та безпроводових мереж зокрема, присвячено праці відомих вітчизняних та закордонних вчених та їх наукових шкіл: Д. В. Агеєва, В. М. Астапені, В. М. Богуша, В. Л. Бурячка, В. В. Домарева, А. Карлсона, О. Г. Корченка, Г. Т. Маркова, М. В. Степашкина, С. В. Толюпи, В. О. Хорошка та Я. С. Шифрина та багатьох ін.

Наявність даних протиріч обумовлює актуальність теми магістерської роботи, а тому вирішення поставленої задачі забезпечення захисту Wi-Fi мережі (інформаційної безпеки безпроводових) має важливе наукове та практичне значення.

Мета і задачі дослідження. *Метою дослідження* є обґрунтування методів захисту Wi-Fi мережі (забезпечення інформаційної безпеки) від несанкціонованого доступу.

Досягнення цієї мети вимагає розв'язання таких задач:

1. Провести аналіз відомих методів (протоколів) захисту Wi-Fi мережі

для обґрунтування напрямку наукового дослідження.

2. Обґрунтувати метод та схему захисту Wi-Fi мережі (забезпечення інформаційної безпеки) від несанкціонованого доступу.

3. Розробити програмний комплекс захисту Wi-Fi мережі клієнтської й серверної частини для мобільних пристроїв з операційною систем Android.

4. Здійснити процес перевірки працездатності розробленого методу та схеми захисту Wi-Fi мережі від несанкціонованого доступу.

Об'єкт дослідження: процес організації захисту Wi-Fi мережі від несанкціонованого доступу.

Предмет дослідження: методи захисту Wi-Fi мережі (забезпечення інформаційної безпеки) від несанкціонованого доступу.

Наукова новизна отриманих результатів.

Вперше на основі взаємної ідентифікації між користувачами та точками доступу з використанням моделі протоколу Pretty Good Privacy розроблено схему захисту Wi-Fi мережі (забезпечення інформаційної безпеки) від несанкціонованого доступу.

РОЗДІЛ 1.
БЕЗДРОТОВІ ТОЧКИ ДОСТУПУ ТА МЕТОДИ ЇХ ЗАХИСТУ

Бездротові точки доступу стають найбільш популярним засобом підключення до ір-мереж таких, як Інтернет. Згідно із прогнозом компанії Cisco про глобальний мобільний трафік на 2015-2020 рр. [1], в 2016 році глобальний Ір-трафік подолає поріг в 1 зеттабайт (1000 ексабайт), а до 2019 року ця величина досягнеться двох зеттабайт. При цьому в 2014 році 54% і 46% трафіка виходило від провідних і бездротових підключень відповідно, а до 2019 прогнозується ескалація Wi-Fi і мобільного трафіку до 66% від його загальної кількості, з яких буде 13% чистого мобільного трафіка й 53% чистого Wi-Fi трафіка. На рисунку 1 наведена динаміка зміни кількості трафіка від різних технологій доступу.

Рисунок 1.1 Прогноз компанії Cisco на 2014-2019 рр. зміни ір-трафіку різних технологій доступу

Згідно тому ж прогнозу компанії Cisco [1], кількість бездротових точок доступу Wi-Fi виросте з 64,2 мільйонів в 2015 до 432,5 мільйонів в 2020 році. Ріст бездротового трафіка обумовлений насамперед простотою розгортання бездротових локальних мереж, ростом популярності, яка відноситься до електроніки (смартфонів, планшетів і т.д.), а також таких технологій, як Connected Car (Wi-Fi в автомобілі) та інших.

Незважаючи на очевидній ріст популярності бездротових точок доступу Wi-Fi, а також і клієнтів таких точок, існують недоліки в схемах аутентифікації між клієнтами й точками доступу. Наприклад, більшість адміністраторів бездротових точок доступу не міняють ключі аутентифікації, настроєні за замовчуванням. Інші ж точки доступу є відкритими через своє призначення. Крім цього, існують методи злому закритих точок доступу Wi-Fi за досить прийнятний час для одержання паролів аутентифікації. Подібні дії дозволяють проводити атаки такі, як «злий двійник» (англ. «Evil twin»), яка полягає в створенні підробленої точки доступу (англ. «Rogue AP»), що виступає в ролі справжньої [2], що дозволяє зловмисникові збирати персональні дані клієнтів.

З іншого боку, у малих мережах, захищених по протоколах WEP або WPA/WPA2 Personal контролювати доступ до бездротової точки можливо такими способами, як обмеження доступу по Mac-адресах і приховання даної точки. Однак, перший спосіб легко обійти підміною Mac-адреси. Виявлення схованих точок доступу не є проблемою, якщо до неї хто-небудь підключився під час прослуховування радіоканалу.

Таким чином, з'являється необхідність у взаємній аутентифікації клієнтів і точок доступу Wi-Fi.

1.1 Проблема аутентифікації клієнтів і точок доступу Wi-Fi мережі

Споконвічно мережна взаємодія відбувалася за допомогою провідних мереж, основу яких становлять комутатори, які у свою чергу перенаправляють пакети на порт одержувача, крім доступу до них інших хостів (див. Рисунок 2).

Щоб перехопити чужий трафік, зловмисник повинен фізично підключитися до комутатора, дістати права адміністратора на комутаторі, або ж здійснити процес атакування MITM з фізичним включенням між пристроями мережі (більш поглиблений розгляд безпеки провідних мереж виходить за рамки даної дипломної роботи).

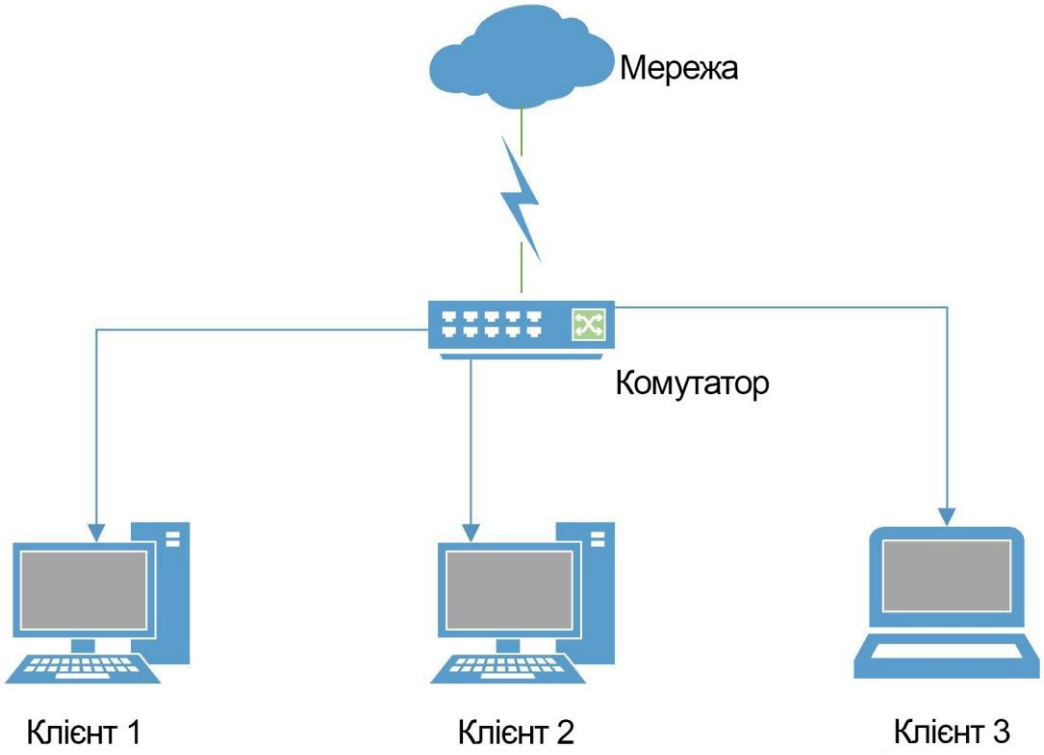


Рисунок 1.2 Принцип роботи комутаторів

Бездротові мережі передають дані в радіохвилях частот високих, зокрема дециметровий діапазон 2.4 ГГц та сантиметровий діапазон 5 ГГц. Тому, що це радіосигнал, то обмежити доступ до нього пристрою не можуть фізично, тому дані можуть бути отримані будь-яким пристроєм у зоні поширення даного сигналу (див. Рисунок 3). У нормальному режимі, також відомому як client або managed mode, мережне встаткування ухвалює пакети, призначені тільки йому. Однак існує цілий ряд програмного забезпечення (Commview for WIFI [2], aircrack-ng [1] та інші), яке дозволяє переводити бездротові мережні адаптери в режим моніторингу, дозволяючи пристрою одержувати й аналізувати весь мережний трафік.

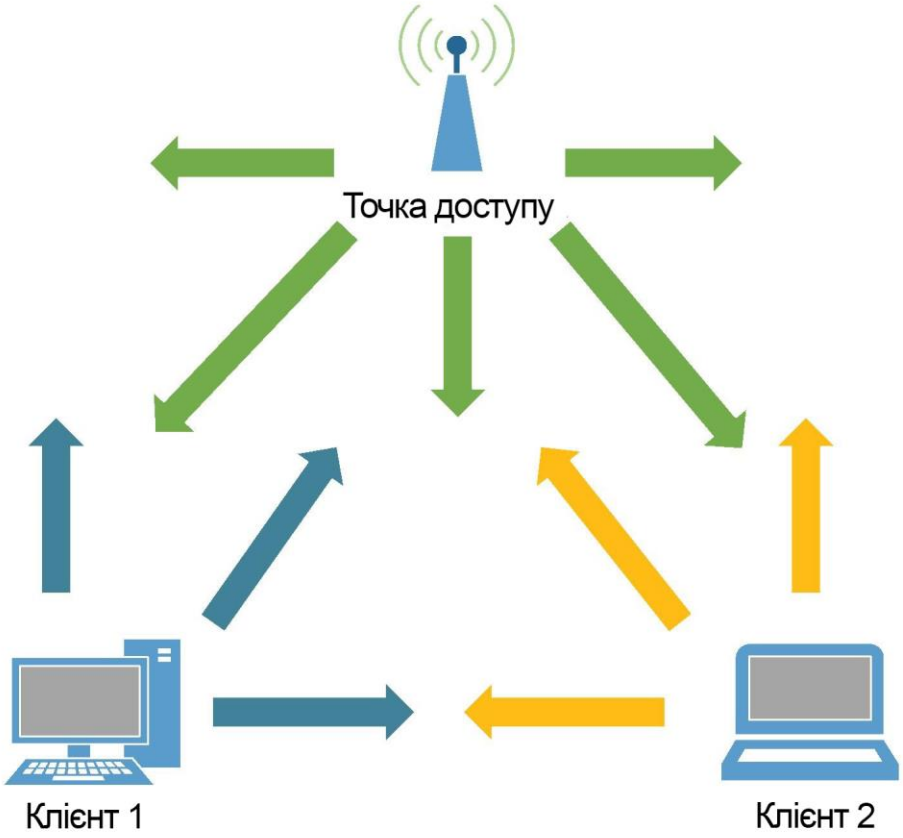


Рисунок 1.3 Принцип роботи бездротових точок доступу

Виходячи із цього, з'явилася необхідність аутентифікувати клієнтів для контролю радіодоступу до точки доступу й ЛВС, а також шифрувати трафік, трансльований між клієнтами й ТД. З даними цілями були спроектовано кілька протоколів безпеки, які відповідають за аутентифікацію й шифрування даних, а також кілька методів, що забезпечують додатковий контроль доступу до мережі. На рисунку 4 представлені різні методи забезпечення безпеки бездротових точок доступу залежно від рівня безпеки.

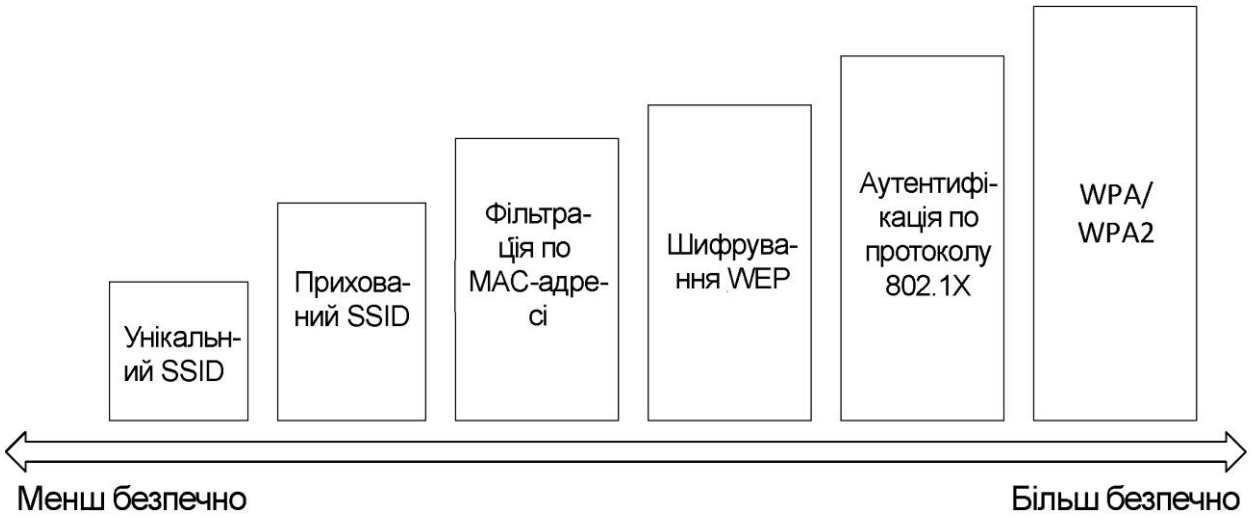


Рисунок 1.4 Заходу забезпечення безпеки бездротових мереж

1.2 Аутентифікація клієнтів і бездротових мереж

Основу будь-якої взаємодії бездротової мережі (і точок доступу) і її клієнтів становлять аутентифікація, тобто яким образом точка доступу дізнається про клієнта й підтверджує, що в нього є право працювати з нею, а також шифрування: який алгоритм застосовується, яким чином генеруються ключі й коли робити їхню зміну. Аутентифікація може відбуватися по одному з наступних варіантів [3]: відкрита аутентифікація, аутентифікація по відкритому ключу й аутентифікація по протоколу 802.1X. Перші два методи визначено в стандарті 802.11 і є небезпечними, а останній є описаним в стандарті IEEE 802.11i-2004. Власне стандарт IEEE 802.11i-2004 загалом визначає процедури керування ключами й взаємної аутентифікації 802.1X, які в сукупності називають RSNA, тобто сильним безпечним мережним спілкуванням [5].

1.2.1 Відкрита аутентифікація

Open – відкрита аутентифікація, найпростіший метод, у якому потрібно тільки те, щоб клієнт знав SSID (Service-Set Identifier) точки доступу. Клієнт надсилає запит на авторизацію точки доступу, яка у свою чергу автоматично підключить пристрій до мережі. Даний метод не є аутентифікацією як такою і

використовується або у відкритих мережах, або в мережах, захищених по протоколу WEP. На рисунку 1.5 представлений алгоритм відкритої аутентифікації клієнтів у мережі.

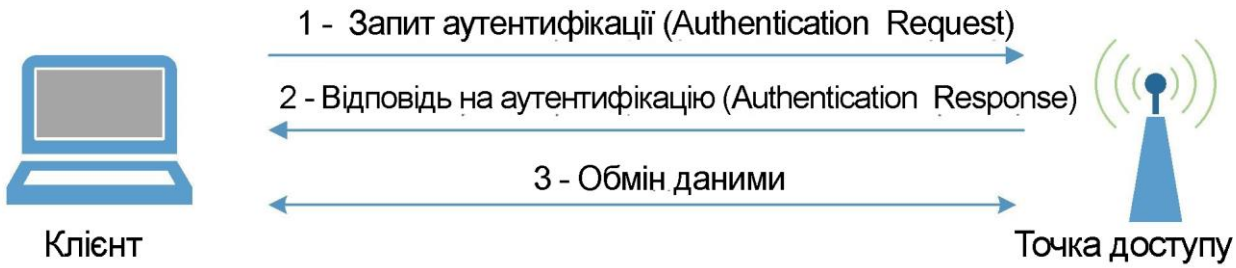


Рисунок 1.5 Алгоритм відкритої аутентифікації

На першому кроці клієнт відправляє запит на аутентифікацію, на другому кроці точка доступу аутентифікує клієнта, і далі клієнт підключається до мережі ТД.

1.2.2 Аутентифікація по загальному ключу

Shared Keys – аутентифікація по загальному ключу, дійсність клієнта, що підключається, перевіряється на основі ключа (пароля). Процедура аутентифікації містить у собі 4 повідомлення. Клієнт надсилає запит на аутентификацію точці доступу, яка відповідає на запит текстовим повідомленням. Клієнт, одержавши дане повідомлення, шифрує його (на ключі WEP) і відправляє зашифроване повідомлення назад на ТД. ТД розшифровує отримане повідомлення, і, якщо воно збігається з відправленим, то аутентифікація успішна. Алгоритм аутентифікації схематично представлено на рисунку 6.

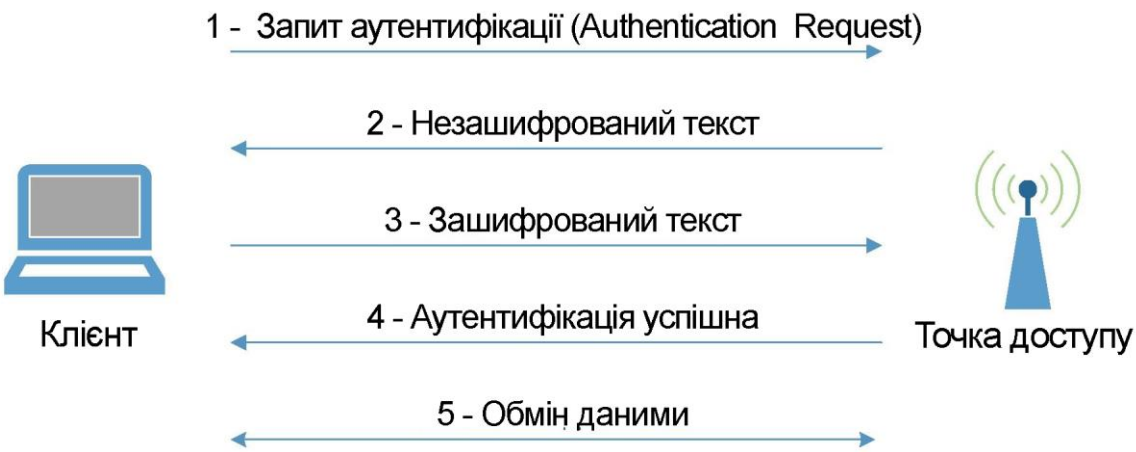


Рисунок 1.6 Алгоритм аутентифікації по загальному ключу

1.2.3 Аутентифікація по протоколу IEEE 802.1X

Мережевий протокол IEEE 802.1X є процедурою аутентифікації по протоколу PEA (Protocol Extensible Authentication), на якому ґрунтується стандарт IEEE 802.1X, що визначає його як Eapol (EAP over LAN) [5]. Eapol – це протокол канального рівня, що дозволяє доставляти Air-Пакети між користувачем і аутентифікатором прямо по Mac-адресах. Стандарт 802.1X визначає контроль доступу до мережі на основі портів для аутентифікації й авторизації пристроїв, а також визначає механізми керування ключами. Під портом у даному контексті мається на увазі єдина точка приєднання до ЛВС. 802.1x визначає трьох учасників взаємодії: аутентифікатор (англ. authenticator) – мережний пристрій, що вимагає провести аутентифікацію (комутатор або бездротова точка доступу); прохач або клієнт (англ. supplicant або peer) – пристрій, який запитує доступ до мережі і якому потрібно аутентифікація; сервер аутентифікації (англ. authentication server) – пристрій, який здатний за деяким даними аутентифицировать клієнта. У ролі такого сервера слугує AAA-сервер, який забезпечує аутентифікацію, авторизацію й збір відомостей про використовувані ресурси по однойменному протоколу [6] (див. Рисунок 7). Самою популярною реалізацією AAA є протокол RADIUS, який став стандартом де-факто. Для його використання на сервері аутентифікації настроюється однойменний Radius-Сервер (наприклад, Freeradius [7]). Прохач і

аутентифікатор взаємодіють за допомогою протоколу Eapol, аутентифікатор і сервер аутентифікації спілкуються по протоколу транспортного рівня RADIUS (див. Рисунок 1.7).

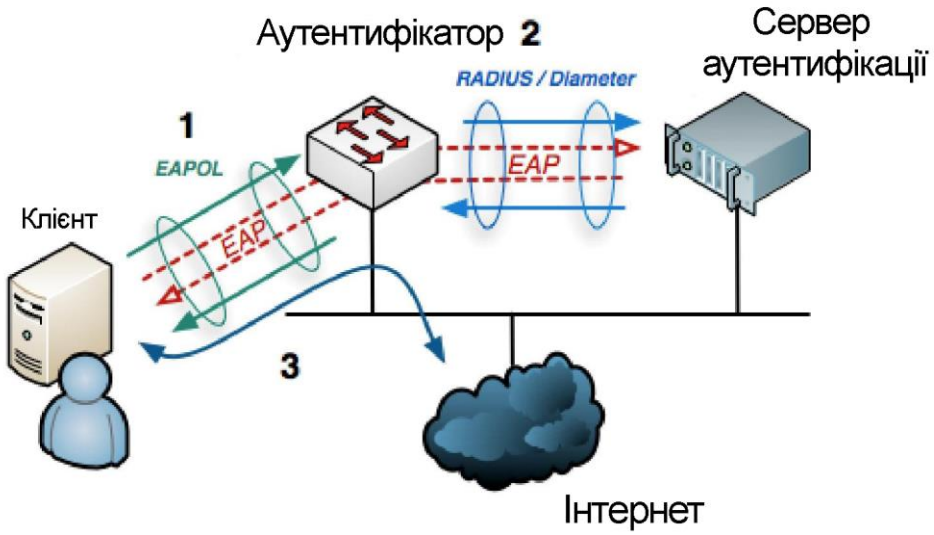


Рисунок 1.7 Архітектура мережі з настроєною аутентифікацією по стандарту 802.1X

Аутентифікатор взаємодіє з «контрольованим» і «неконтрольованими» портами, які є логічними (віртуальними) сутностями, але використовують одне фізичне підключення до ЛВС (див. Рисунок 1.8). До аутентифікації, відкритий тільки «неконтрольований» порт. Єдиний дозволений через нього трафік – це Eapol-пакети, а після аутентифікації відкривається «контрольований» порт.

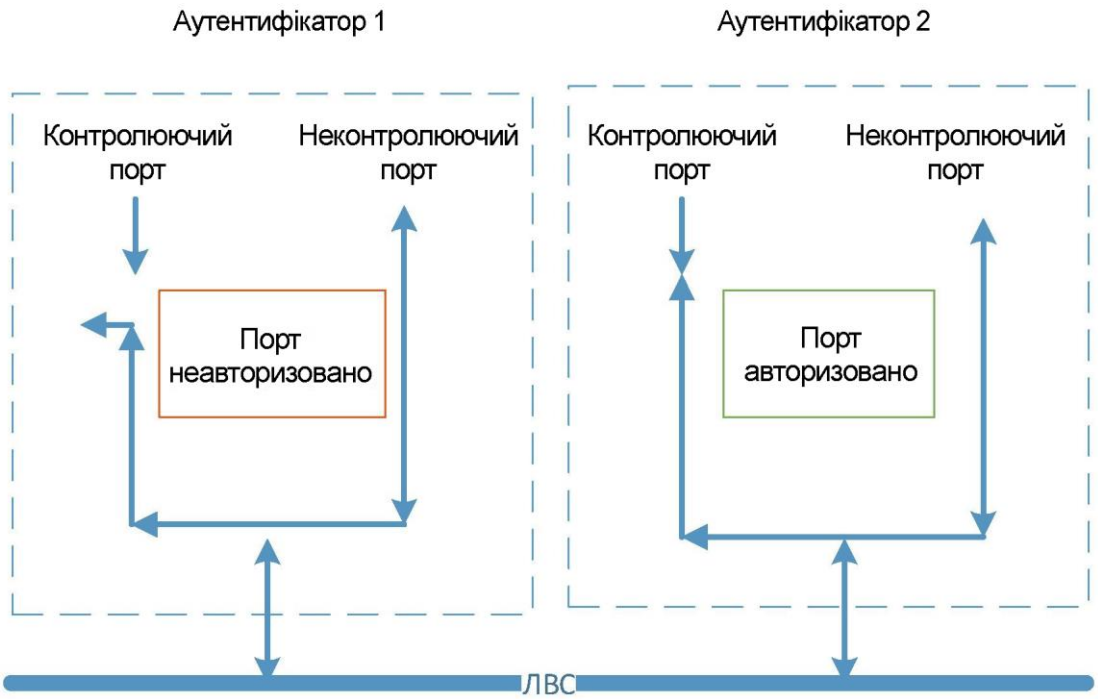


Рисунок 1.8 Контрольовані й неконтрольовані порти

Протокол EAP є транспортним протоколом, оптимізованим для аутентифікації, і не є конкретним методом. Протокол є фреймворком, що забезпечують безпечну доставку ключів, що визначають формати повідомлень, а також загальні методи, які дозволяють реалізувати протоколи. EAP працює поверх протоколів канального рівня, таких як PPP (Point-to-Point Protocol) або IEEE 802 (наприклад, Ethernet) без використання IP [8], і має кілька базових реалізацій, певних у стандартах IETF (у різних RFC), а також реалізовані фірмами такими, як Cisco, власні доповнення. Як було сказано вище, стандарт 802.1X адаптує протокол EAP для використання в провідних і бездротових мережах, завдяки чому для взаємної аутентифікації можна використовувати різні типи реалізації протоколу EAP. Які саме типи аутентифікації реалізовувати лягати на компанії, що роблять мережне встаткування й програмне забезпечення. Використання стандарту 802.1X забезпечує бездротовим ЛВС взаємну аутентифікацію клієнтів і серверів аутентифікації [6]. Процес аутентифікації по стандарту 802.1X у бездротових мережах представлено на малюнку 1.9.

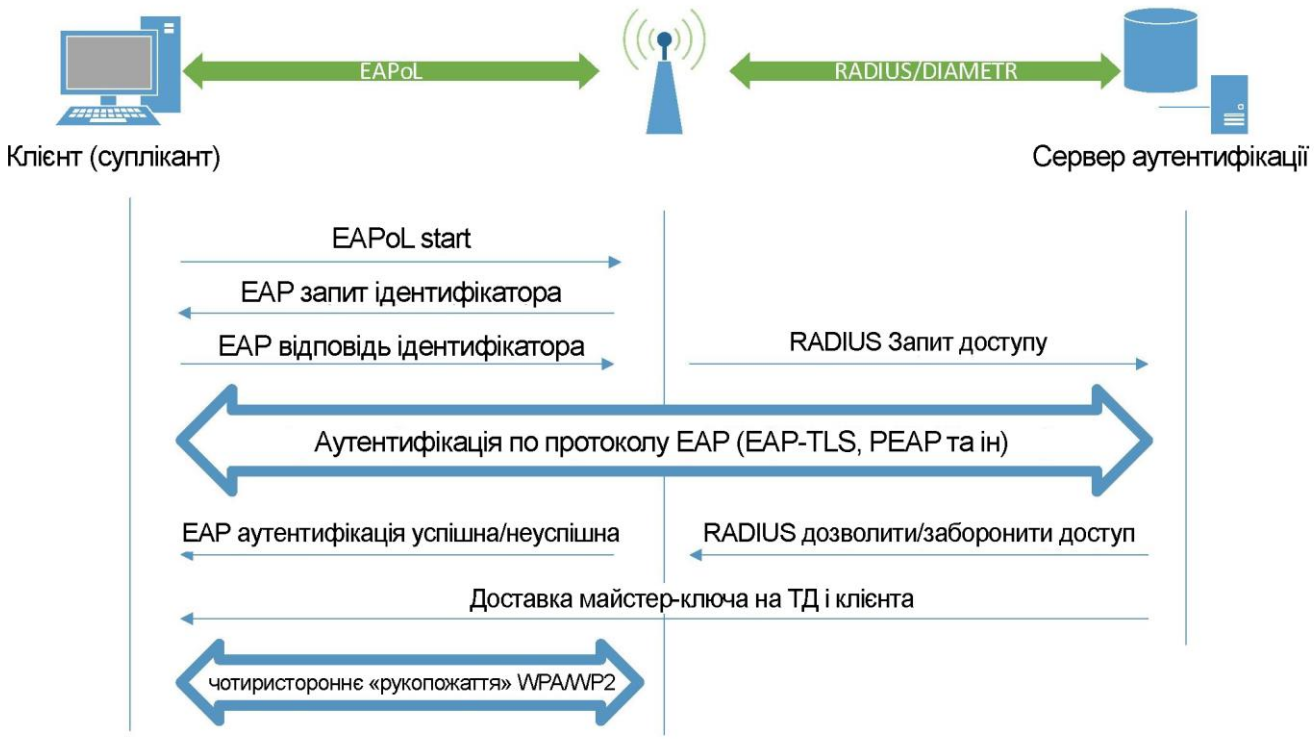


Рисунок 1.9 Аутентифікація по стандарту 802.1X у бездротових мережах

Існують також інші розв'язки. Наприклад, компанія Cisco у свої пристрої вбудовує такі методи аутентифікації, як аутентифікація по Mac-адресі, CCKM аутентифікація [3].

1.3 Протоколи безпеки Wi-Fi мереж

1.3.1 Протокол WEP

WEP є протоколом захисту/безпеки, прийнятий IEEE в 1997 році й представлений як частина протоколу 802.11 [10]. На даний момент оголошений застарілим і був замінений в 2004 році протоколом WPA2. Споконвічно протокол повинен був надати рівень безпеки, еквівалентний провідним з'єднанням і захистити трафік від прослуховування, однак з поставленим завданням упоратися не смог. Через помилки в проектування він підданий ряду атак і для одержання ключа й, отже, дешифрування трафіка необхідно перехопити достатню кількість пакетів, скористатися спеціальною утилітою

(наприклад, aircrack-ng [2]). Ключ підбирається за кілька хвилин. Основними недоліками є малі довжини ключа шифрування (40 або 104 біта) і шифрування всіх даних одним ключем (на практиці шифрування полягає в побітовій операції XOR із псевдовипадковим ключем).

Сам по собі протокол WEP є методом шифрування даних. Однак для аутентифікації клієнтів разом із протоколом можуть бути використано дві схеми: відкрита аутентифікація або аутентифікація по загальному ключу. При відкритої аутентифікації, як було описано в п. 1.2.1, клієнт не надає ніяких даних для аутентифікації в мережі. Однак далі, клієнт не зможе спілкуватися з мережею ТД, якщо ключі WEP не збіглися. На малюнку 1.10 схематично показаний процес відкритої аутентифікації при використанні протоколу WEP:

Рисунок 1.10 Відкрита аутентифікація при використанні протоколу WEP

У випадку аутентифікації по загальному ключу, ТД спочатку відправляє клієнтові у відповідь на запит аутентифікації деякий текстовий рядок. У відповідь клієнт надсилає зашифрований на WEP ключі текст. Точка розшифровує прийнятий текст за допомогою свого WEP ключа, порівнює розшифрований і споконвічний тексти. Якщо тексти збігаються, то точка аутентифікує клієнта й підключає його до мережі [3]. Дана схема була представлено на малюнку 6. Однак, аутентифікація по загальному WEP ключу менш безпечна, тому що зловмисник може прослухати радіоканал, одержати

вихідний текст від ТД і зашифрований текст від клієнта й зрівняти для одержання вихідного ключа [3].

1.3.2 Протоколи WPA і WPA2

Протокол WPA був випущений в 2003 році як швидка заміна протоколу WEP, тому що організація Wi-Fi Alliance прагла скоріше закрити існуючі уразливості. Робоча група IEEE 802.11 у той момент займалася адаптацією стандарту 802. IX під новий стандарт 802. Ш, у якому в 2004 році був описаний протокол WPA2. WPA2 реалізує методи аутентифікації, керування ключами й шифрування, певні як обов'язкові в стандарті 802.1 П. Основною відмінністю протоколу WPA2 від WPA став алгоритм, застосовуваний для шифрування трафіка між клієнтом і ТД. У випадку WPA - це алгоритм TKIP, у випадку WPA2 - це CCMP, заснований на стандарті AES (Advanced Encryption Standard). Тому що протокол WPA2 з 2006 року зобов'язаний підтримується тими ж пристроями, що й протокол WPA [11], далі буде розглядатися саме WPA2.

У відмінності від протоколу WEP, протокол WPA2 забезпечують і аутентифікацію, і шифрування. Аутентифікація може бути одного із двох типів:

- по попередньо розподіленому ключу захисту - WPA2 Personal, який можна зустріти як WPA2-PSK режим;
- по протоколу 802. IX - WPA2 Enterprise, який можна зустріти як режим WPA2-EAP.

Перед тем, як розглянути дані типи аутентифікації, необхідно описати типи ключів, які встановлюються в ході обох типів:

1. Сесійний майстер ключ MSK (англ. Master Session Key) – використовується для одержання ключа PMK.

2. Парний майстер-ключ PMK є головним 256-бітним ключем, використовуваний для забезпечення безпеки взаємодії ТД і клієнта. Виходить або прямо з попередньо розподіленого ключа MSK (WPA2 Personal), або за допомогою методів EAP (WPA2 Enterprise).

3. Тимчасовий парний ключ PTK є 512-бітним ключем, який використовується для аутентифікації й шифрування даних. Виходить за

допомогою перетворення ключа PMK і деяких інших даних за допомогою псевдовипадкової функції. Ключ PTK складається з 3 частин:

3.1. Ключ підтвердження ключа KCK застосовується для перевірки кадрової цілісності.

3.2. Ключ шифрування ключа KEK застосовується для шифрування групового тимчасового ключа GTK.

3.3. Тимчасовий ключ TK застосовується для шифрування трафіка.

На малюнку 11 зображено розподіл ключа PTK на такі частини:

Рисунок 1.11 — Складові частини ключа PTK

4. Груповий майстер-ключ GMK є ключем допоміжним 256-бітним, який застосовується для одержання GTK.

5. Груповий тимчасовий ключ GTK є ключем 256-бітним, який застосовується для шифрування широкомовного й багатоадресного трафіка від ТД до клієнтів. Виходить перетворенням ключа GMK.

Режими аутентифікації будуть відрізнятися тим, на основі чого робити взаємну аутентифікацію, а також хто саме і як управляє ключем PMK. Ціль же кожного типу аутентифікації полягає в тому, щоб ТД і бездротовий клієнт могли довести один одному, що вони знають однаковий парний майстер-ключ

PMK. Для установки майстер-ключа використовується протокол канального рівня Eapol в обох методах аутентифікації.

1.3.3 WPA2 Personal

Протокол захисту WPA2 Personal був розроблений для використання в малих і середніх мережах (наприклад, у домашніх мережах), коли кількість клієнтів не велика. При застосуванні WPA2 Personal задається один-єдиний пароль для всієї мережі, за яку відповідає ТД. Пароль являє собою відкритий текст довжиною від 8 до 63 Ascii-Символів. Обмеження в 63 символу було встановлено для того, щоб розрізняти пароль і попередньо розподілений ключ PSK з довжиною 256 біт, що й відображається як 64 hex-символу. Пароль у цьому випадку виступає в якості MSK. Для встановлення PMK на стороні клієнта й ТД пароль подається на вхід функції формування ключа на основі PBKDF2 пароля, який застосовує використовує алгоритм HMAC-SHA1 для одержання хеш-значення вхідної послідовності. Функція PBKDF2 повторює 4096 раз обчислення хеш-значення HMAC і, таким чином, одержує на виході 256-бітний ключ PSK.

Одержаний ключ PSK використовується в якості ключа PMK. Далі инициализируется процес 4-стороннього рукостискання (див. Рисунок 12).

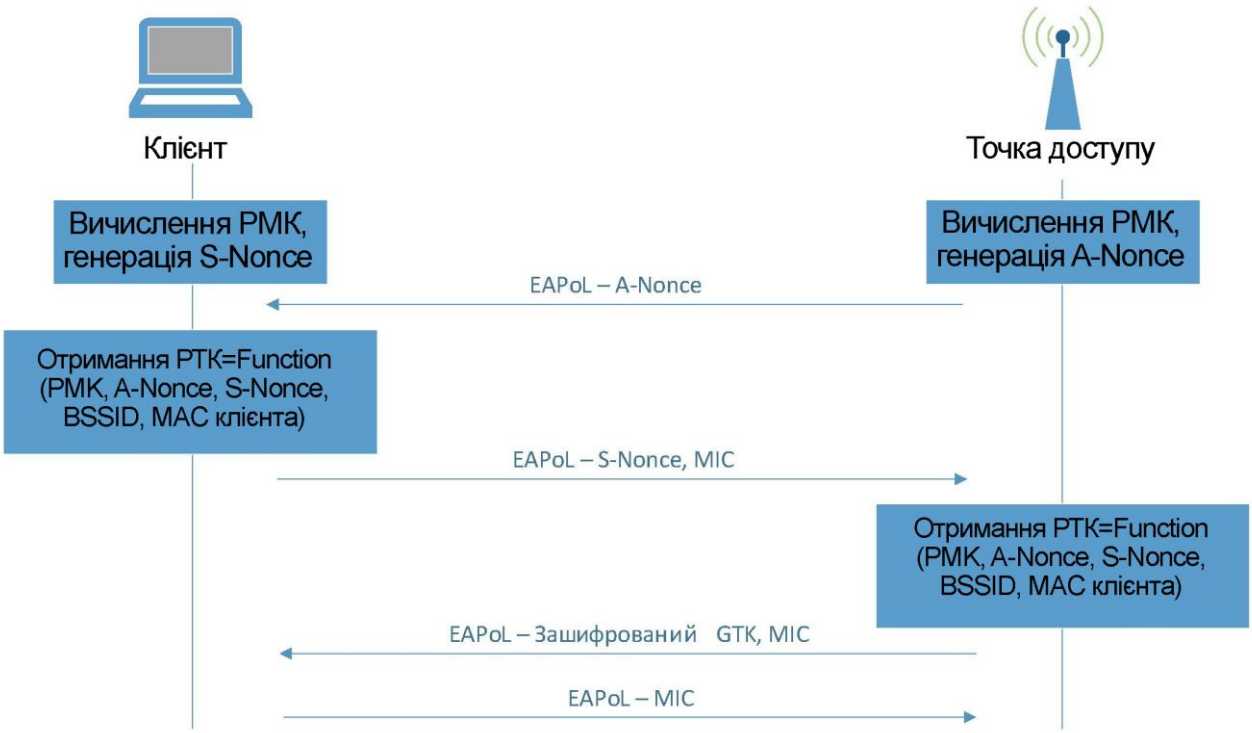


Рисунок 1.12 Схема чотирибічного рукостискання протоколу WPA2-PSK

У першому повідомленні ТД передає клієнтові деяку випадкову послідовність із 32 байт, називану A-Nonce, Mac-Адреса. У відповідь на неї клієнт передає на ТД свою випадкову послідовність також з 32 байт, так звану S-Nonce, а також MIC, код цілісності повідомлення, який додається до повідомлень для захисту від атак. Таким чином, клієнт і точка доступу мають наступну інформацію: A-Nonce, PMK, Basic SSID точки доступу (тобто її Mac-адреса) і Mac-адреса клієнта. Дані 5 параметрів контактуються в рядок, який подається на вхід функції PBKDF2, і обчислюється аналогічно обчисленню ключу PSK ключ PTK довжиною 512 біт [4]. Увесь процес генерації ключів PMK і PTK зображено на малюнку 1.13.

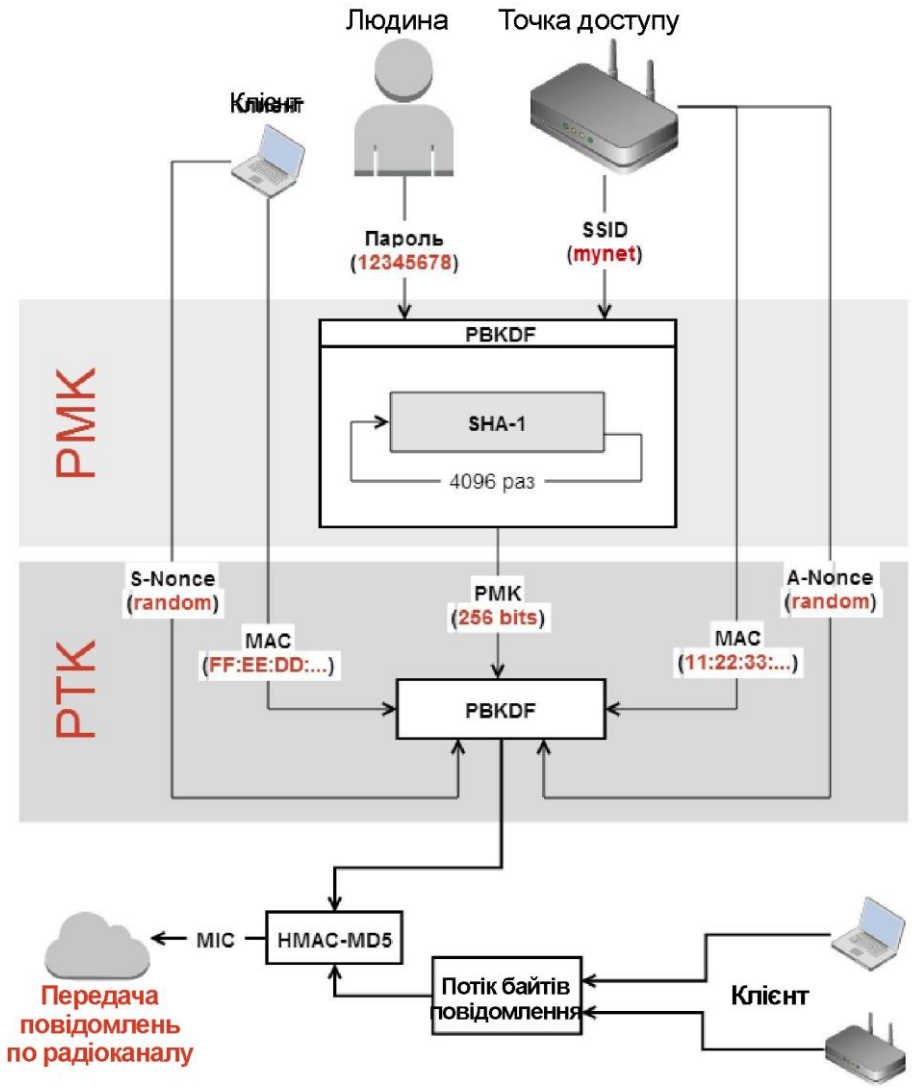


Рисунок 1.13 Схема генерації PMK і PTK ключів

Ключ GTK використовується для шифрування широкомовного й багатоадресного трафіка від ТД до клієнтів, тому генерується тільки на стороні точки доступу. Вона генерує його на основі двостороннього рукостискання й шифрує за допомогою KEK ключа. У першому повідомленні точка доступу відправляє клієнтові ключ GTK, зашифрований на ключі KEK, а також MIC, що використовує KCK. У відповідь клієнт надсилає повідомлення зі своїм MIC. При першій установці ключа GTK дане рукостискання відбувається під час 4-стороннього рукостискання, як показано на малюнку 1.12.

Ключ PTK використовується для аутентифікації й у якості симетричного ключа шифрування. Для аутентифікації перевіряється факт збігу паролів. Щоб

зрозуміти, що паролі збігаються, у процесі 4-стороннього рукостискання починаючи з 2 кроку (тобто кроку відправлення S-Nonce клієнтом) до повідомлень додається MIC. MIC обчислюється за допомогою HMAC-MD5, на вхід якому крім переданих потоків байт подається ще ключ PTK, використовуваний у якості солі. Таким чином, PTK використовується як для шифрування потоку даних, так і для формування контрольної суми. Якщо використовувалися однакові PTK, то при розшифруванні обчислений MIC збіжиться з отриманим, інакше MIC не збіжаться, отже, був використані різні PTK, отже, PMK були різними, отже, були різними PSK і вихідні паролі.

Після встановлення загального ключа PTK, точка доступу відправляє клієнтові ключ GTK і MIC, а клієнт відповідає повідомленням ACK. Взаємна аутентифікація вважається успішної, якщо в момент 4-стороннього рукостискання починаючи з 2 фрейму всі 3 наступних рукостискання виявилися успішними [12].

1.3.4 WPA2 Enterprise

У мережах, що використовує попередньо розподілений ключ, є один істотний недолік. Якщо даний ключ був скомпрометований або ж потрібно відкликати доступ одному із клієнтів, то необхідно перемінити ключ як на стороні аутентификатора, так і на стороні всіх клієнтів. Крім того, при перехопленні трафіка в зловмисника з'являється можливість провести оффлайн-атаку по добору пароля й, при його успішному одержанні й захвату 4-стороннього рукостискання між клієнтом і точкою доступу, дешифрувати трафік клієнта мережі [7]. Подібні недоліки роблять неприйнятним підхід WPA-PSK у корпоративних мережах, коли кількість клієнтів і точок доступу може бути велике.

При використанні WPA2 Enterprise схема аутентифікації ускладнюється й додається сторонній сервер аутентифікації (див. Рисунок 7). У відмінності від використання попередньо розподіленого ключа, аутентифікація проводиться по засобах стандарту 802.1X (див п. 1.1.3), а, отже, виконується на стороні сервера.

Протокол 802.1X, як було сказано в п. 1.1.3, визначає трьох учасників взаємодії: прохача, аутентифікатора й сервера аутентифікації.

Стосовно до бездротових мереж Wi-Fi, прохачем виступає клієнтський бездротовий пристрій (клієнт), а аутентифікатором є бездротова ТД. Сервером аутентифікації, як правило, виступає Radius-сервер. Під час аутентифікації ТД одержує Eapol-Пакети із запитами й відповідями від клієнта й перетворить їх у відповідний запит Radius-серверу.

В WPA2 Enterprise аутентифікація, як правило, не використовує розподілений ключ. Замість нього клієнт повинен надати персональні дані, формат яких залежить від використовуваної реалізації протоколу EAP (ім'я користувача й пароль, токен, сертифікат, одноразовий пароль і т.п.). В RFC 4017 визначені методи, рекомендовані до реалізації в Wi-Fi мережах: EAP-TLS, EAP-TTLS, PEAP, EAP-SIM [13].

Базовими методами є EAP-MD5 і EAP-TLS. EAP-MD5 використовує, як зрозуміло з назви, MD5 алгоритм для обчислення хеш-значення персональних даних (пароля), які відправляються на сервер і на його стороні звіряються зі збереженим хеш-значенням. У даного методу основним недоліком є те, що він не забезпечує взаємну аутентифікацію – тільки сервер аутентифікує клієнта. Метод EAP-MD5 звичайно не використовується, тому що забезпечує тільки однобічну аутентифікацію. Також метод характерний ще й тим, що починає аутентифікацію відразу після підключення, тобто всі дані передаються у відкритому виді, що піддає клієнтів і мережа атакам. Самим безпечним методом є EAP-TLS. Для взаємної аутентифікації в ньому використовуються x.509 сертифікати як на стороні клієнта, так і на стороні сервера. Повний процес аутентифікації методом EAP-TLS показано на малюнку 14. Незважаючи на те, що EAP-TLS є самим безпечним методом, використовується він нечасто через необхідність доставки сертифікатів кожному із клієнтів.

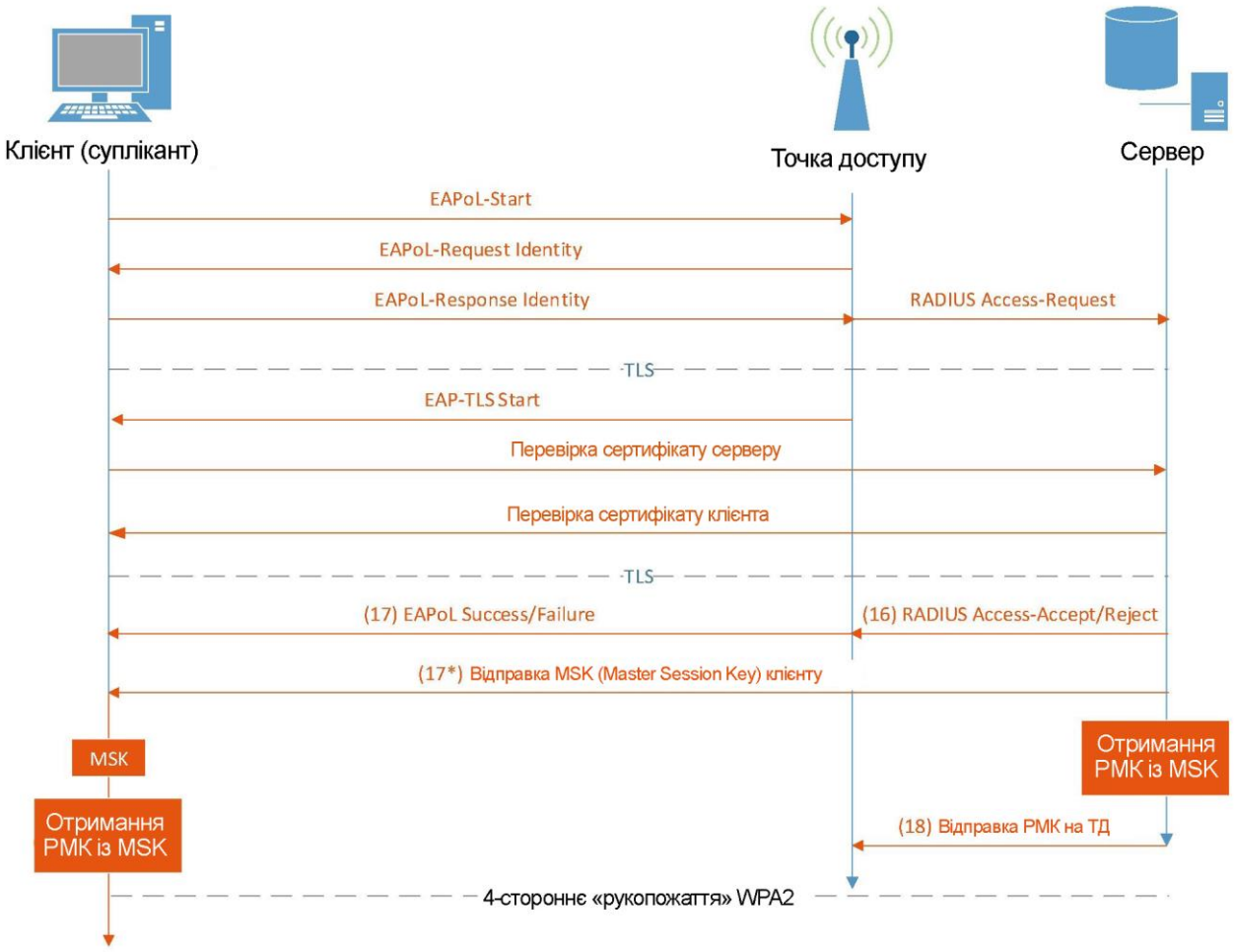


Рисунок 1.14 – Аутентифікація EAP-TLS

Для сполучення зручності аутентифікації клієнтів за персональним даними й безпеки методу EAP-TLS були спроектовані тунелірovані методи PEAP (Protected EAP, Захищений EAP) і EAP-TTLS (Tunneled TLS, Тунельований TLS). Обоє методів для передачі даних методу використовують EAP-TLS для аутентифікації тільки сервера й установлюють захищене TLS з'єднання між клієнтом і сервером, використовуючи x.509 сертифікат сервера подібно тому, як установлюються https-з'єднання. Клієнт спочатку переконується, що сервер має валідний сертифікат. Після цього використовуються «внутрішні методи» для аутентифікації клієнтів. Відмінність між методом EAP-TTLS та методом PEAP полягає саме у їх внутрішній структурі. В PEAP ними можуть бути Eap-mschapv2 (передається зашифрований пароль, підтримується тільки Microsoft), EAP-GTC (передається

одноразовий пароль, підтримується тільки Cisco), EAP-TLS (передається сертифікат клієнта, підтримується тільки Microsoft), у той час як в EAP-TTLS підтримуються ще й застарілі методи, типу PAP, CHAP і т.д, що пояснюється його більш раннім походженням. По суті своєї EAP-TTLS і PEAP є ідентичними, однак перший був розроблений компаніями Certicom та Software Funk, а PEAP – Cisco та Microsoft. Завдяки маркетингу останніх PEAP став найбільш популярним протоколом [14].

Показове порівняння тунельованих і базових методів аутентифікації зображено на рисунку 1.15.

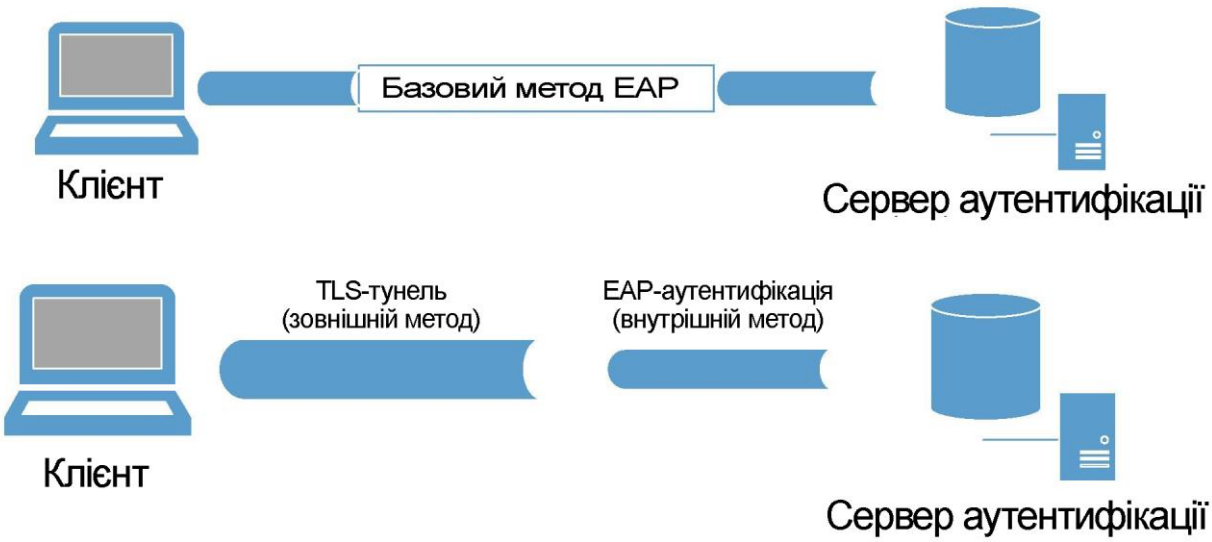


Рисунок 1.15 – Порівняння принципу роботи базових (а) і тунельованих (б) методів EAP

Після того, як клієнт і сервер аутентифікували один одного, необхідно встановити сеансові ключі. Ключі генеруються для кожного користувача й кожної сесії окремо, що збільшує безпеку. Залежно від використовуваного методу EAP, ключ PMK може бути обчислений окремо на стороні клієнта й на стороні сервера, або тільки на стороні сервера аутентифікації, після чого ключ доставляється на сторону клієнта по захищеному каналу. Сервер має так званий ключ 512-бітним AAA, який виступає в ролі ключа MSK. Ключ AAA обчислюється на основі даних, отриманої під час аутентифікації по протоколу EAP. Наприклад, при використанні EAP-TLS ключ установлюється в такий

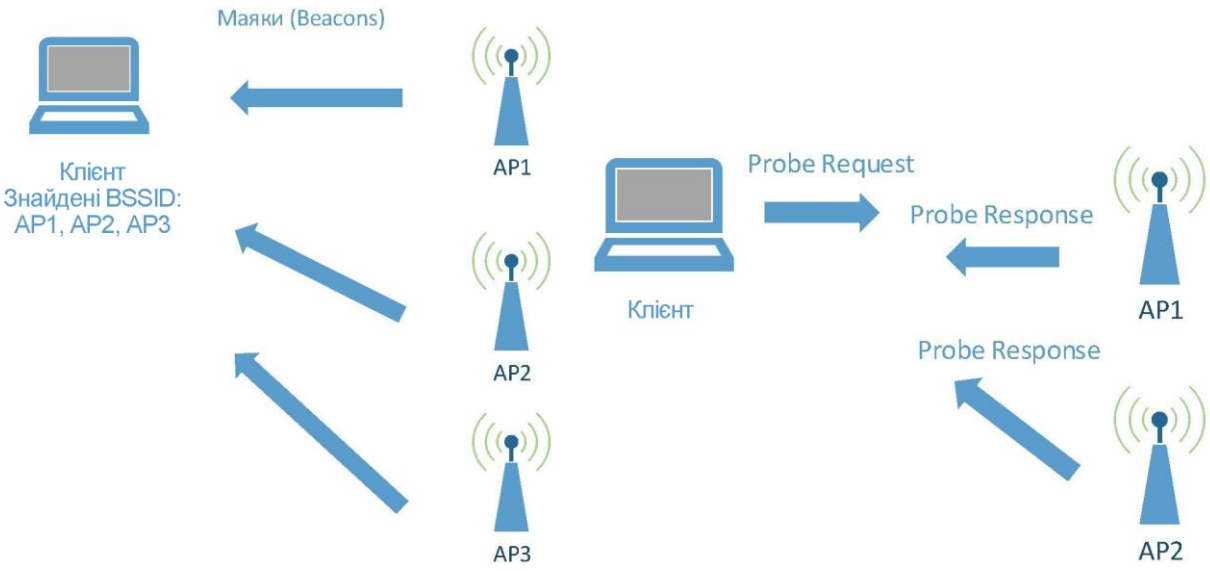
спосіб. Після проведення аутентифікації клієнт генерує деякий ключ, називаний Pre-master key, шифрує його на відкритому ключі сервера й відправляє йому. Pre-master key, деякий секретний рядок, випадковий рядок клієнта й випадковий рядок сервера за допомогою псевдовипадкової функції TLS-PRF перетворяться в ключ AAA. Ключ PMK виходить прямо із ключа AAA і є його першими 256 бітами [12]. Далі сервер по захищеному з'єднанню відправляє ключ PMK на ТД. Після цього ініціалізує 4-стороннє рукостискання, аналогічно тому, як це відбувалося в WPA2 Personal. Повна загальна схема роботи WPA2 Enterprise методу аутентифікації й установки ключів представлена в додатку А.

1.4 Процес підключення до ТД

Для того, щоб підключитися до мережі стандарту 802.11, що обслуговується ТД, клієнт спочатку повинен виявити її на одному з 14 каналів. Можливі два варіанти сканування каналів на наявність мережі [16]:

1. Пасивний режим. У ньому пристрій прослуховує всі канали на наявність пакетів-маяків (Beacon-Фреймів). Точка доступу періодично, залежно від настроювань (звичайно раз в 100 мілісекунд), розсилає beacon-фрейми, позначаючи свою присутність (див. Рисунок 16-а). У пакетах Beacon утримується інформація про підтримуваних швидкості, канали, алгоритми шифрування, керування ключами і т.д. Клієнт періодично опитує радіоефір по всіх каналах на наявність beacon-фреймів з інформацією про мережі, на основі якої ухвалює рішення щодо кращого варіанта підключення [15]. Даний підхід є неефективним і має недоліки. Наприклад, якщо клієнт очікує приймання beacon-пакета недостатньо часу на якому-небудь каналі, тобто шанс, що він пропустить його й не підключиться до мережі [16]. 2. Активний режим. Пристрій також сканує кожний канал, однак не очікує beacon-фреймів. Сканування відбувається за допомогою Probe-Запитів (Probe request) для одержання інформації про ТД, що розсилаються на широкомовний Mac-Адресу з нульовим SSID (рис. 1.16, б). У пакеті Probe Request може бути визначений SSID мережі (спрямований запит, Directed Probe Request). ТД одержує Probe

Request, перевіряє, зазначена чи в ньому хоча б одна сумісна з нею швидкість передачі й відповідає пакетом Probe-Відповідь (Probe response), яка в собі містить приблизно ту ж інформацію, що й beacon-фрейми (SSID, підтримувані швидкості передачі і т.д.). Після цього клієнт у випадку широкомовного Probe request вибирає із усіх Probe response, які він одержав, ті мережі, настроювання якої йому підходять найбільше.



а б

Рисунок 1.16. Активне (а) і пасивне (б) сканування мережі Wi-Fi

Після виявлення відбувається обмін пакетами аутентифікації й асоціації з обраної ТД (див. Рисунок 1.17). Пакети аутентифікації (Authentication Frames) забезпечують низькорівневу аутентифікацію на рівні протоколу 802.11, тобто на канальному рівні. Дана аутентифікація відрізняється від аутентифікації по стандарту 802.1X та протоколу WPA2, які розпочинають діяти тільки після того, як клієнт аутентифікувався й асоціювався по протоколу 802.11. Споконвічно аутентифікація 802.11 була спроектована для протоколу WEP, однак, як було сказано в п.1.2.1, протокол WEP був оголошений небезпечним і застарілим. Через це в пакеті аутентифікації майже завжди встановлюється тип 0, тобто відкрита аутентифікація, і вона проходить успішно. Якщо ТД одержує

від не аутентифікованого клієнта пакети, відмінні від Authentication або Probe request, то вона посилає клієнтові пакет де аутентифікації (Deauthentication Frame), переводячи клієнта в не аутентифікований й неасоційований стану. Аутентифікація 802.11 дозволяє клієнтові аутентифицироваться в безлічі ТД, що спрощує роумінг і наступну асоціацію з ними, тому що клієнт може бути асоційований тільки з однієї ТД. Запит на асоціацію (Association Frame) містить у собі обрані типи шифрування, якщо потрібні, і інші дані 802.11, необхідні для сумісності. Якщо ТД одержує від авторизованого клієнта, але не асоційованого, пакети, відмінні від Association, то вона посилає клієнтові пакет дисоціації (Disassociation Frame), переводячи клієнта в авторизоване, але неасоційований стану. Якщо процеси аутентифікації й асоціації 802.11 пройшли успішно, те ТД створює ID асоціації (Association ID) для даного клієнта [10].

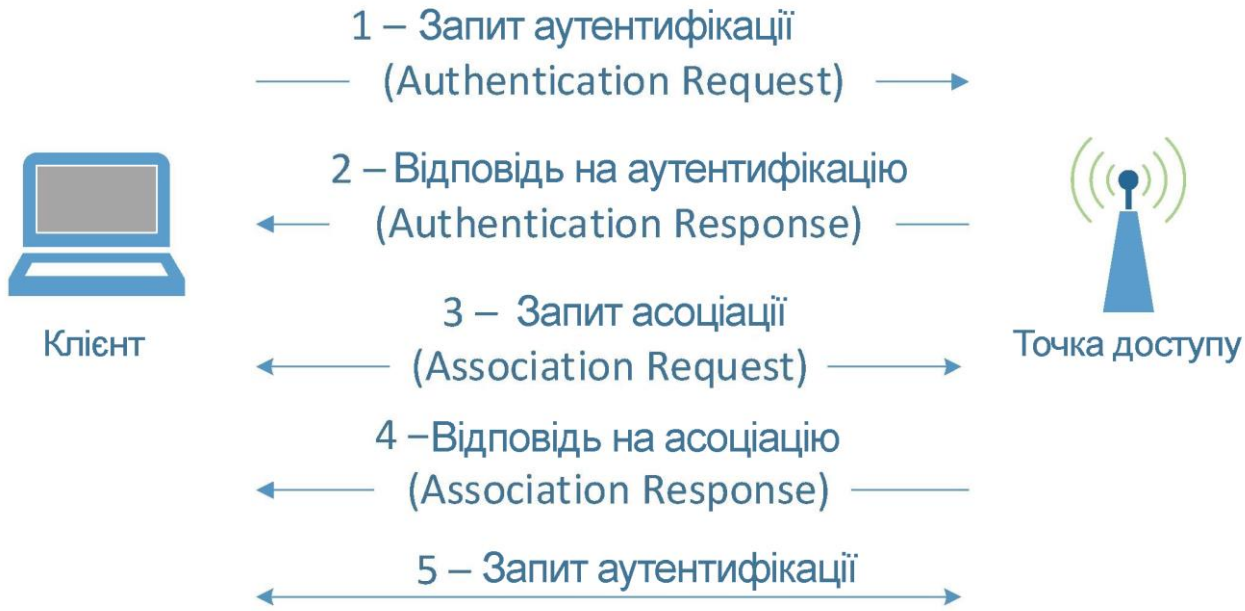


Рисунок 1.17 Аутентифікація й асоціація в мережах Wi-Fi

Тільки після цього починаються аутентифікація й генерація динамічних ключів WPA2/802.1X. На рисунку 1.18 показана послідовність обміну пакетами у випадку аутентифікації по протоколу WPA2.

D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	167	Probe Response, SN=156, FN=0, Flags=.....
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	802.11	41	Authentication, SN=841, FN=0, Flags=.....
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	30	Authentication, SN=157, FN=0, Flags=.....
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	802.11	107	Association Request, SN=842, FN=0, Flags=.
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	81	Association Response, SN=158, FN=0, Flags.
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	EAPOL	133	Key (Message 1 of 4)
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	EAPOL	155	Key (Message 2 of 4)
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	EAPOL	195	Key (Message 3 of 4)
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	EAPOL	133	Key (Message 4 of 4)

Рисунок 1.18 Послідовність обміну пакетами між клієнтом і ТД Wi-Fi у випадку подальшої аутентифікації й генерації ключів по протоколу WPA2

1.5 Висновок до розділу 1

У першому розділі описано проблеми аутентифікації клієнтів і точок доступу Wi-Fi та проаналізовані існуючі протоколи безпеки, застосовувані в Wi-Fi мережах, з погляду запобігання доступу підроблених клієнтів до ТД і проведення атак підроблених ТД.

РОЗДІЛ 2.
ОБҐРУНТУВАННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ

Усі існуючі заходи захисту від атаки підробленої ТД можна розділити по тому, на якій стороні взаємодії дані заходи застосовуються, а саме на стороні клієнта або мережі.

2.1 Атака підробленої ТД

В описані вище протоколах безпеки Wi-Fi мереж використовуються різні методи аутентифікації. Однак, жоден з методів не передбачає аутентифікацію точок доступу клієнтом, що дозволяє проводити атаки типу «підроблена точка доступу» (Rogue Access Point). Залежно від обраного протоколу й методу аутентифікації дана атака може бути критичної.

Атака підробленої ТД полягає в наступному: зловмисник довідується інформацію про ТД, до якої клієнт коли-небудь підключався, і створює ТД із аналогічними конфігураціями (див. Рисунок 2.1). Залежно від того, по якому протоколу безпеки ТД забезпечувала аутентифікацію в мережі, необхідно довідатися й створити різні параметри. Далі зловмисник проводить спроби відключити клієнта від точки доступу, до якої він підключений у цей момент (якщо підключений), або ж просто намагається підключити клієнта до своєї мережі.

Рисунок 2.1 Принцип дії атаки підробленої точки доступу

Можливі кілька сценаріїв:

1. Клієнт підключений у цей момент до якої-небудь Wi-Fi мережі й зловмисник намагається пері підключити його до ТД, що обслуговує ту ж мережу.

2. Клієнт підключений до Wi-Fi мережі, відмінної від тієї, яку обслуговує підроблена ТД.

3. Клієнт не підключений ні до якої Wi-Fi мережі.

4. Перебір публічних відомих стоків.

Залежно від конкретного сценарію зловмисникові необхідно провести деякі додаткові дії. У випадку ж, коли клієнт не підключений ні до однієї з мереж, зловмисникові досить настроїти з мереж, до якої клієнт коли-або підключався раніше, щоб процес підключення був прозорий для жертви. В інших двох випадках у зловмисника є два варіанти пері підключення клієнта до своєї підробленої ТД:

1. Посилка пакетів де аутентифікації клієнтові.

2. Атака Dos на точку доступу.

У кожному разі підроблена точка доступу повинна мати більш сильний сигнал стосовно жертви, ніж оригінальна, інакше при спробі асоціюватися

клієнт знову підключиться до валідної точки доступу. Після того, як зловмисникові вдалося підключити жертву до своєї підробленої точки доступу, йому необхідно показати клієнтові, що він є справжньою точкою.

У відкритих мережах це досить легко, тому що в них не проводиться ніякої аутентифікації, досить надати клієнтові легітимний SSID.

Підключившись до відкритої мережі, клієнт стає найбільш уразливий у порівнянні з іншими типами аутентифікації. У мережах, захищених по протоколу WEP, і з аутентифікацією, проведеної за допомогою пакетів 802.11 (див п.1.3.), зловмисникові повинен бути відомий загальний розділений ключ. Як було сказано в п. 1.1.2, протокол WEP був оголошений небезпечним, тому що загальний ключ можна підібрати пакетів з перехоплених мережних за досить малу кількість часу за допомогою утиліти (наприклад, тієї ж aircrack-ng) навіть без використання графічного процесора. Тому захист по протоколу WEP ненабагато краще захисту у відкритих мережах, і підмінити ТД такої мережі не важко.

У мережах же, захищених по протоколу WPA/WPA2, набагато складніше обійти захист й провести успішну аутентифікацію. У випадку WPA2 Personal зловмисникові повинні бути відомі Mac-адреса ТД (BSSID), SSID і PSK (попередньо розподілений ключ). З даного списку зловмисникові сутужніше всього довідатися ключ PSK, тобто пароль від мережі. Для того, щоб підібрати пароль, зловмисникові необхідно захопити процедуру 4-стороннього рукостискання. Однак, складність добору пароля залежить прямо від його довжини. Звичайно для добору використовуються словники або генератори паролів. Таким чином, набагато складніше підібрати пароль, який складається з 16 повторюваних декількох символів, ніж з 8 унікальних. Нижче в таблиці 1 наведена статистика перебору пароля WPA2-PSK на 8 відеокартах AMD 290X зі швидкістю перебору приблизно 1, 5 мільйони WPA-паролів у секунду (що порівнянне по швидкості перебору 94 мільярдів у секунду MD 5-хешів) і на чотирьох ядерному ЦП Intel Core-i7 3840QM із частотою 3.8 Ггц зі швидкістю перебору 4800 Wpa-Паролів у секунду [17].

Таблиця 2.1

Залежність швидкості перебору паролів WPA-PSK від довжини й використовуваних символів

Склад пароля	Затрачуваний час на перебір усіх значень	
	Intel Core-i7 3.8 ГГц	AMD 290X
8-значний з букв латинського алфавіту	268/ (4700 × 3600 × 24) = 514 днів	268/ (1500000 × 3600) = 38,7 годин
10-значний цифровий пароль	1010 / (4700 × 3600 × 24) = 24,6 дня	1010 / (1500000 × 3600) = 2 години
10-значний з букв латинського алфавіту	2610 / (4700 × 3600 × 24 × 365) = 952 року	2610 / (1500000 × 3600 × 24 × 365) = 3 року
12-значний цифровий	1012 / (4700 × 3600 × 24 × 365) = 6,7 років	1012 / (1500000 × 3600 × 24) = 7,7 днів
14-значний цифровий	1014 / (4700 × 3600 × 24 × 365) = 674,6 року	1014 / (1500000 × 3600 × 24 × 365) = 2,1 року

Звідси видно, що при певній довжині пароля не має змісту займатися добором, тому що шанс одержати вірний пароль дуже малий. Однак, адміністратори часто залишають паролі за замовчуванням, або роблять їхньої невеликої довжини для кращого запам'ятовування. У загальнодоступніх ж мережах паролі можуть бути видані обслуговуючим персоналом на прохання клієнта. Звідси випливає, що при певних обставинах загальний пароль WPA2-PSK може бути розкритий. Якщо подібна дія відбулася або було виявлено, що один з користувачів внутрішньої мережі є зловмисником і проводить атаки, то для обмеження доступу одного з користувачів можливі два варіанти: обмеження доступу по Mac-Адресі, або зміна ключа у всій мережі WPA2-PSK. Однак, Mac-адреса можна перемінити на кожній з ОС (особливо на ОС сімейства Linux, якими найчастіше користуються порушники), а зміна ключа всієї мережі WPA2-PSK доправить незручності через складність його поширення серед користувачів.

У випадку WPA2 Enterprise, де аутентифікація проводиться по протоколу EAP, безпека підключення залежить від обраного методу аутентифікації між клієнтом і Radius-Сервером, а також коректності настроювань аутентифікації як

на стороні сервера, так і на стороні клієнта. Як було сказано в п.1.2.2, метод EAP-TLS, PEAP, EAP-TTLS використовують сертифікати на стороні сервера (EAP-TLS ще й на стороні клієнта). Якщо не брати до уваги уразливості, пов'язані з інфраструктурою, що забезпечує роботу протоколу TLS (злом центру сертифікації, використання слабких алгоритмів генерації пара ключів, викрадення закритого ключа за допомогою шкідливого ПО на серверу і т.д.), то для того, щоб провести успішно атаку підробленої ТД, крім самої ТД необхідно настроїти підроблений сервер аутентифікації, у який необхідно буде помістити сертифікат TLS. Якщо не вдалося одержати сертифікат і закритий ключ справжнього сервера аутентифікації, то зловмисникові прийде використовувати або свій самозавірений сертифікат, верифікацію якого провести неможливо, або валідний сертифікат, що може вказати явно на того, хто є зловмисником. У випадку самозавіреного сертифіката при правильній конфігурації клієнт буде сповіщений про той (див. Рисунок 2.2), що дійсність сертифіката неможливо перевірити, і вже користувач повинен розв'язати, довіряти серверу аутентифікації чи ні. Таким чином, успішність атаки буде багато в чому залежати від людського фактора. У цьому випадку, зловмисник може тільки сподіватися, що користувач прийме підроблений сертифікат. Цьому сприяє той факт, що організації часто встановлюють саме завірені сертифікати. Крім практично невразливих методів EAP на основі TLS існує ряд інших методів, використання яких підвищує ймовірність проведення атаки.

Наприклад, була доведена уразливість методу LEAP до перебору паролів після проведення в автономному режимі (тобто офлайн).

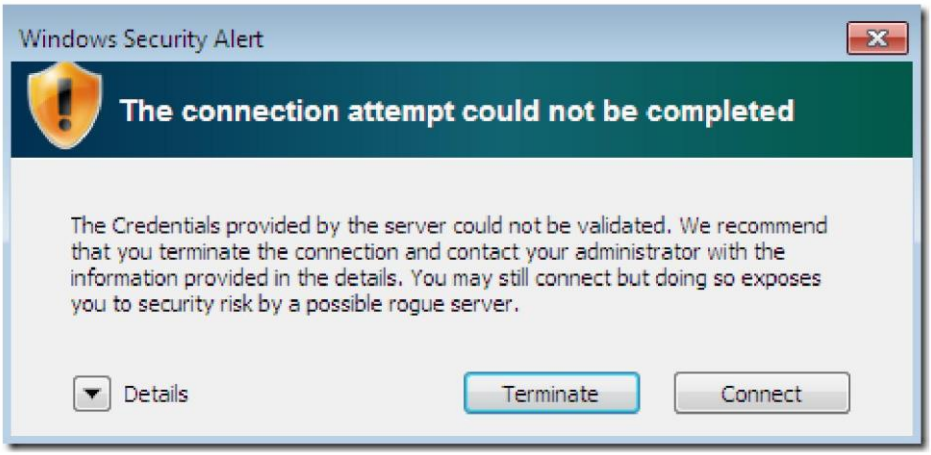


Рисунок 2.2 Приклад повідомлення користувача про неможливість перевірки дійсності сертифіката сервера в ОС Windows

При успішному підключенні клієнта до підробленої ТД у зловмисника з'являється можливість проводити будь-які атаки людини по середині (Man-in-the-middle). Приклади реалізації таких атак можуть бути наступними:

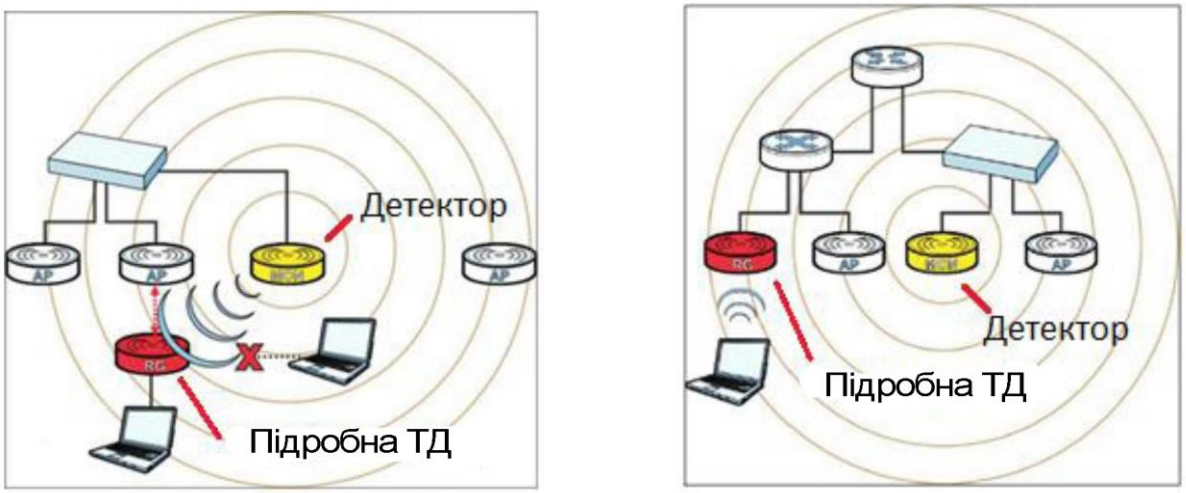
1. Перехоплення трафіка, у тому числі з використанням сторонніх утиліт, які запобігають захисту жертви. Наприклад, sslstrip-атака, що відбувається за допомогою однойменної утиліти. Зловмисник обходить HSTS (HTTP Strict Transport Security) і Ssl-Трафік.
2. Різні підміни (ARP, DNS і т.д.) і атаки (Dos, DHCP і т.д.).
3. Сканування конкретних хостів мережі для проведення подальших атак.
4. Таким чином, існує погроза успішного проведення атаки підробленої

ТД на клієнтські пристрої при відсутності й використанні більшості протоколів безпеки Wi-Fi і їх типів. Складність створення підробленої ТД певної мережі залежить від того, який саме протокол безпеки, що забезпечує аутентифікацію, використовується в даній мережі. Однак, якщо користувач коли-або підключався до мережі, захист якої була забезпечена не належним чином або не забезпечена зовсім, а також якщо зловмисникові відомі параметри безпеки однієї з мереж, до якої підключався клієнт, то підвищується успішність проведення атаки підробленої ТД.

2.2 Захист зі сторони мережі

У відкритих і персональних мережах даний вид захисту звичайно не проводиться, однак успішно застосовується в корпоративних мережах. Різні виробники, такі як Cisco, Tp-link, Zyxel, Aruba і інші, вбудовують у свої пристрої підтримку виявлення, запобігання й захист від підроблених ТД.

У корпоративних мережах можливі два сценарії установки підробленої ТД. У першому випадку підроблена ТД функціонує як незалежна від мережі точка (див. Рисунок 2.3.а), у другому – ТД підключається прямо до комутатора/контролеру локальної мережі (див. Рисунок 2.3.б). Іноді такі точки називають інтерферуючими ТД.

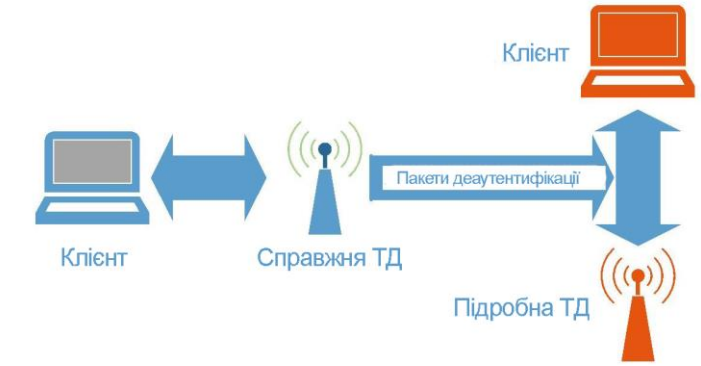


а б

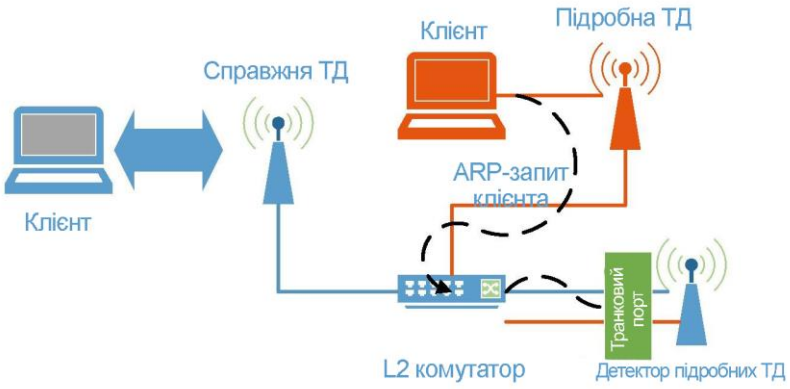
Рисунок 2.3 Можливі варіанти установки підроблених ТД у корпоративних мережах: а – випадок, коли підроблена ТД є незалежною; б – випадок, коли підроблена ТД підключена до внутрішньої мережі

У найпростішому випадку на контролері бездротової мережі настроюються списки довірених ТД на основі їх Мас-Адреси, а всі інші вважаються за замовчуванням не довіреними. Далі вже адміністратор ухвалює самостійно заходи безпеки на основі побачених не довірених ТД. Більш

ефективним розв'язком є настроювання однієї із ТД у режим моніторингу, тоді ТД сканує радіоефір і шукає підозрілі точки. Якщо підроблена ТД не підключена до локальної мережі, то детектор вносить перешкоди в їхня робота, наприклад, розсилаючи широкомовні пакети, щоб клієнти не могли підключитися до підробленої ТД (див. Рисунок 2.4.(а)). Якщо підключена провідним з'єднанням, то з'являється можливість заблокувати її роботу через порт комутатора (див. Рисунок 2.4.(б)).



а



б

Рисунок 2.4. Заходу захисту від підроблених ТД (а – підроблена ТД не підключена до провідної мережі, б – підроблена ТД підключена до провідної мережі).

Найдосконалішими технологіями в області безпеки бездротових з'єднань на сьогоднішній день володіє компанія Cisco, підтримуючи так звану технологію WIPS (Wireless Intrusion Prevention System), у завдання якої саме

також входить і виявлення підроблених ТД [18]. Розв'язок про те, що точка є підробленої, і критичність даної точки ухвалюється на основі SSID, який вона розсилає, інформації про те, чи підключена точка до провідної мережі, а також списків і деякої статистики, яка ведеться на спеціальній станції (Cisco Prime Infrastructure, CPI) для зменшення помилок першого роду. Керування підробленими ТД розбивається на 3 етапу:

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

2. Класифікація. Точки-детектори намагаються співвіднести дані про підроблену ТД, отримані по бездротовому каналу, з тими, що отримані по провідному каналу, завдяки тому, що їх розташовують на танковому порту й вони виходять можливість прослуховувати весь провідний трафік із усіх VLAN-ів. Якщо Mac-адреса підробленої точки або одного з її клієнтів був виявлений у провідній мережі, то така підроблена точка розглядається як критична. Крім цього, Cisco спроектувала спеціальний протокол RLDP, який допомагає визначити, чи підключена підроблена ТД до провідної мережі, підключаючись до неї прямо в якості клієнта й посилаючи її дані по протоколу RLDP на CPI.

3. Усунення. Визначається місце розташування ТД, створюються перешкоди, відключаються порти.

На рисунку 2.5 зображені всі застосовувані технології Cisco для виявлення підроблених ТД у локальній мережі.

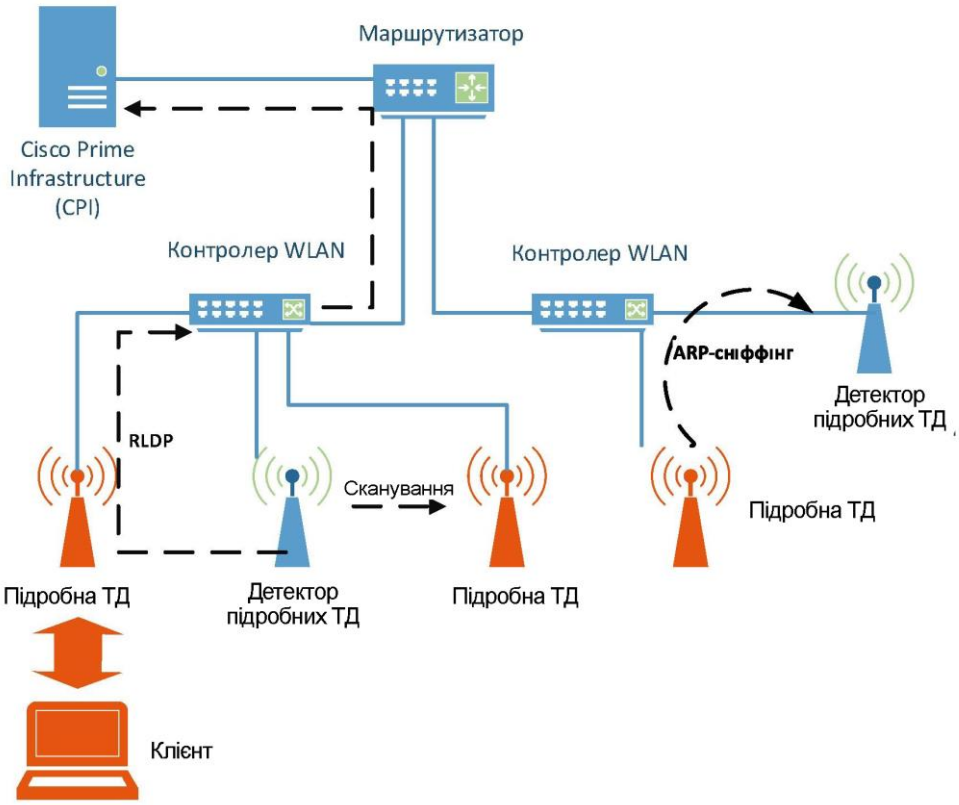


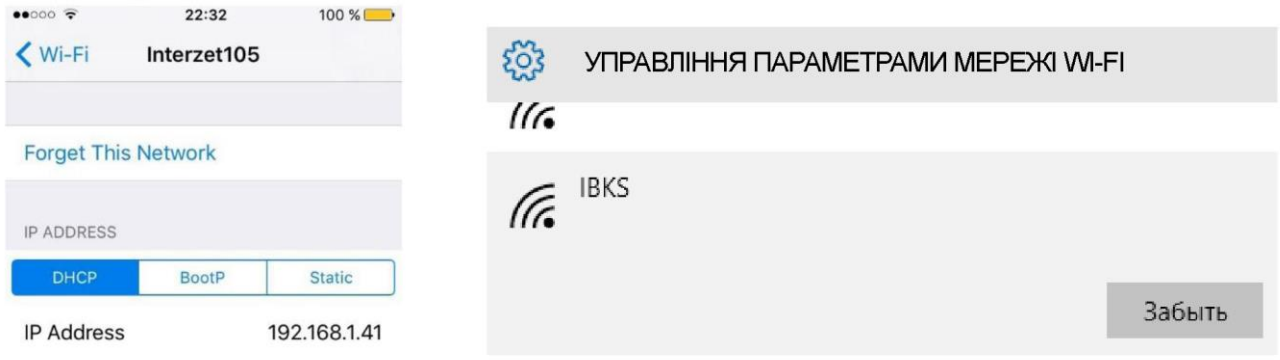
Рисунок 2.5. Використовувані компанією Cisco технології виявлення підроблених ТД

2.3 Захист зі сторони клієнта

Клієнтський пристрій може захиститися двома способами від атаки підробленої ТД, або запобігши підключення, або захистивши його. Для захисту від підключення до підроблених ТД користувач може скористатися наступними заходами захисту:

• відключати автоматичні підключення до мереж Wi-Fi. Залежно від ОС дана включається по-різному. Дана функція звичайно застосовується окремо до кожної з мереж, до якої підключається пристрій. Наприклад, при відключенні від мережі в пристроях під керуванням ios необхідно вручну нажати кнопку «Забути дану мережу», щоб пристрій не підключився до неї знову. Під керуванням ОС Windows дане настроювання необхідно виконати через панель керування (до ОС Windows 10), або через настроювання мережі в параметрах

(ОС Windows 10). Аналогічним образом відключається функція автоматичного підключення й в інших ОС. На малюнку 2.6 показана робота даної функції в ОС ios 9 (Рисунок 2.6.а) і ОС Windows 10 (Рисунок 2.6.б).



а б

Рисунок 2.6 Відключення автоматичного підключення в ОС ios 9 (а) і ОС Windows 10 (б)

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

```
netsh wlan add filter permission=block ssid=WLAN
networktype=infrastructure
```

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

```
iptables -A INPUT -m mac --mac-source <MAC> -j DROP
```

• використання сторонніх утиліт. Наприклад, утиліт, які дозволяють самостійно виявити підозрілих ТД. Одним з таких інструментів є утиліта Waidps [19], написана мовою програмування python і призначена для виявлення атак і аудита ТД. Вона підтримує виявлення й оповіщення користувача в декількох випадках:

1. Виявлена ТД із однаковим SSID (ESSID), що може вказувати на атаку підробленої ТД.

2. Виявлення потоку деаутентифікуючих пакетів (deauthentication flood), що може вказувати на те, що зловмисник прагне перепідключити клієнта до свого підконтрольного пристрою.

3. Пристрій клієнта перепідключився до іншої ТД, тобто відбулася переасоціація.

Іншим прикладом сторонніх утиліт, використовуваних для виявлення підроблених ТД, є Evilapdefender [20], яка може виявити підроблену ТД по декільком параметрам: ТД має той же SSID, але інша адреса BSSID, ТД має той же SSID, однак інші атрибути (канал, метод шифрування, протокол і аутентифікацію); ТД має той же SSID і ті ж атрибути, але інші параметри, що розсилаються в beacon-фреймах.

Крім утиліт, використовуваних для виявлення підроблених ТД, є можливість використовувати такі утиліти, як Smart Wi-Fi Toggler [21]. Дана програма дозволяє пристроям під керуванням ОС Android 2.3 і більш пізніх версій набудовувати включення й вимикання бездротового пристрою адаптера залежно від гео положення пристрою. Однак, даний розв'язок може врятувати від підроблених ТД тільки в тих місцях, які користувач не вказав як місця підключення до мереж Wi-Fi, тому в районі, наприклад, удома або робочого місця з'являється можливість провести атаку підробленої ТД.

- підключатися тільки до мереж, захищених по протоколах EAP, при цьому не підключатися до мереж, сертифікати яких не довірені.
- відключення бездротового адаптера. Метод є самим радикальним, однак найбільш діючим.

Дані методи є превентивними. Крім них користувач може захистити свої дані вже після підключення до ТД. Подібні заходи нічим не відрізняються від тих, що застосовуються для захисту конфіденційності й цілісності персональних даних. Основним і самим універсальним заходом захисту є використання Vpn-Підключень. Крім захисту на мережному й канальному рівнях, захист даних можна забезпечити на більш високому рівні за допомогою протоколу TLS, інакше кажучи, використовувати тільки Https-З'єднання. З

даною метою організація Electronic Frontier Foundation разом з організацією The Tor Project випустила розширення для більшості популярних браузерів (Chrome, Opera, Firefox) розширення «HTTPS Everywhere» [22], які зобов'язує кожний запит до веб-ресурсів робити тільки через захищене з'єднання.

Усі викладені вище методи захисту від підроблених точок доступу справляються з даним завданням, однак або є не універсальними, або мають інше призначення, що може утруднити їхнє використання, або викликати незручності користувача, як, наприклад, відключення автоматичного підключення до відомих мереж або використання VPN, послуги підключення до яких звичайно платні, або компанії обмежують швидкості й кількість дозволеного трафіка. Тому з'являється необхідність у створенні й реалізувати методу захисту від підроблених ТД, який буде спрямований саме на дане завдання й успішно справлятися з нею.

2.4 Висновок до розділу 2

У другому розділі проаналізовані існуючі методи й засобу захисту, які можуть захистити клієнтів Wi-Fi від підроблених ТД як з боку мережі, так і з боку клієнта. У ході дослідження було виявлено, що існуючі методи й засобу не дозволяють повною мірою захиститися від підроблених ТД.

РОЗДІЛ 3.
ІДЕНТИФІКАЦІЯ ВЗАЄМОДІЇ КЛІЄНТІВ ТА ДОСТУПУ ДО WI-FI МЕРЕЖІ

3.1 Схема ідентифікаційної взаємодії клієнтів та доступу до WI-FI мережі

На сьогодні більшість протоколів захисту, які забезпечують ідентифікацію, забезпечують проведення ідентифікації лише між клієнтом мережі та власне самою мережею SSID. В такому випадку, зловмисник намагається з'єднати клієнта до мережі підробленого центрального пристрою (точки доступу).

В такому випадку протоколи забезпечують процес не ідентифікації доступної точки мережі, в якій є ідентифікований клієнт/користувач і відповідно забезпечує обмін в цій мережі даними персонального виду.

Для розв'язування задачі проблеми доступних точок підробленого характеру необхідно:

- ввести процес ідентифікації кожної окремо взятої точки, до якої підключено пристрій клієнта;

- забезпечити підтримку взаємозалежної ідентифікації точок мережі з метою забезпечення кожній з них процес ідентифікації окремо взятого клієнта окремої мережі, зокрема у випадку малої та середньої мережі, які захищені протоколом WAP2 без сервера ідентифікації, доступ обмеженого характеру до мережі забезпечується за допомогою персонального клієнтського MAC-адреса.

Загальна схема ідентифікації в такому випадку розглядається тоді коли клієнт ідентифікує точку мережевого доступу, оскільки такий випадок є узагальненого характеру. Ідентифікація мережевою точкою клієнта здійснюється аналогічним способом.

Для здійснення процесу ідентифікації точкового доступу запропоновано застосувати криптосистему, а саме алгоритм шифрування повідомлень клієнта

ключом відкритого типу. Оскільки власне таке рішення забезпечує вирішення завдання проблеми довіри за допомогою цифрових підписів (ЦП). Як відомо, у криптографії з відкритим ключем (або асиметричної криптографії) використовується пара ключів: один ключ є відкритим (публічним), іншої – закритим (приватним) [23]. Закритий ключ (ЗК) ніколи не передається по каналу зв'язку, тому що його розголошення приведе до компрометації безглуздості використання всієї криптографії. Відритий же ключ (ОК), навпаки, передається вільно. Електронний підпис створюється за допомогою ЗК, а її перевірка виконується відповідним ОК. Стосовно до аутентифікації клієнтами точок доступу дана схема буде полягати в наступному (див. Рисунок 24):

1. Клієнт вибирає ТД, яку він уважає довіреної (наприклад, ТД домашню мережу, що забезпечує).
2. Клієнт одержує ОК даної ТД і запам'ятовує його.
3. При наступному підключенні до того, як клієнт почне передавати трафік до ТД, спочатку проводиться її аутентифікація:

a. Клієнт посилає деяку випадкову послідовність байт точці доступу.

b. Точка підписує дану послідовність байтів на своєму ЗК і відправляє результат підпису клієнтові.

c. Клієнт перевіряє отриманий підпис за допомогою ОК ТД і засвідчує, що ТД має вірний ЗК.

4. При успішної аутентифікації ТД клієнт починає передачу трафіка до неї, інакше підключення відміняється.

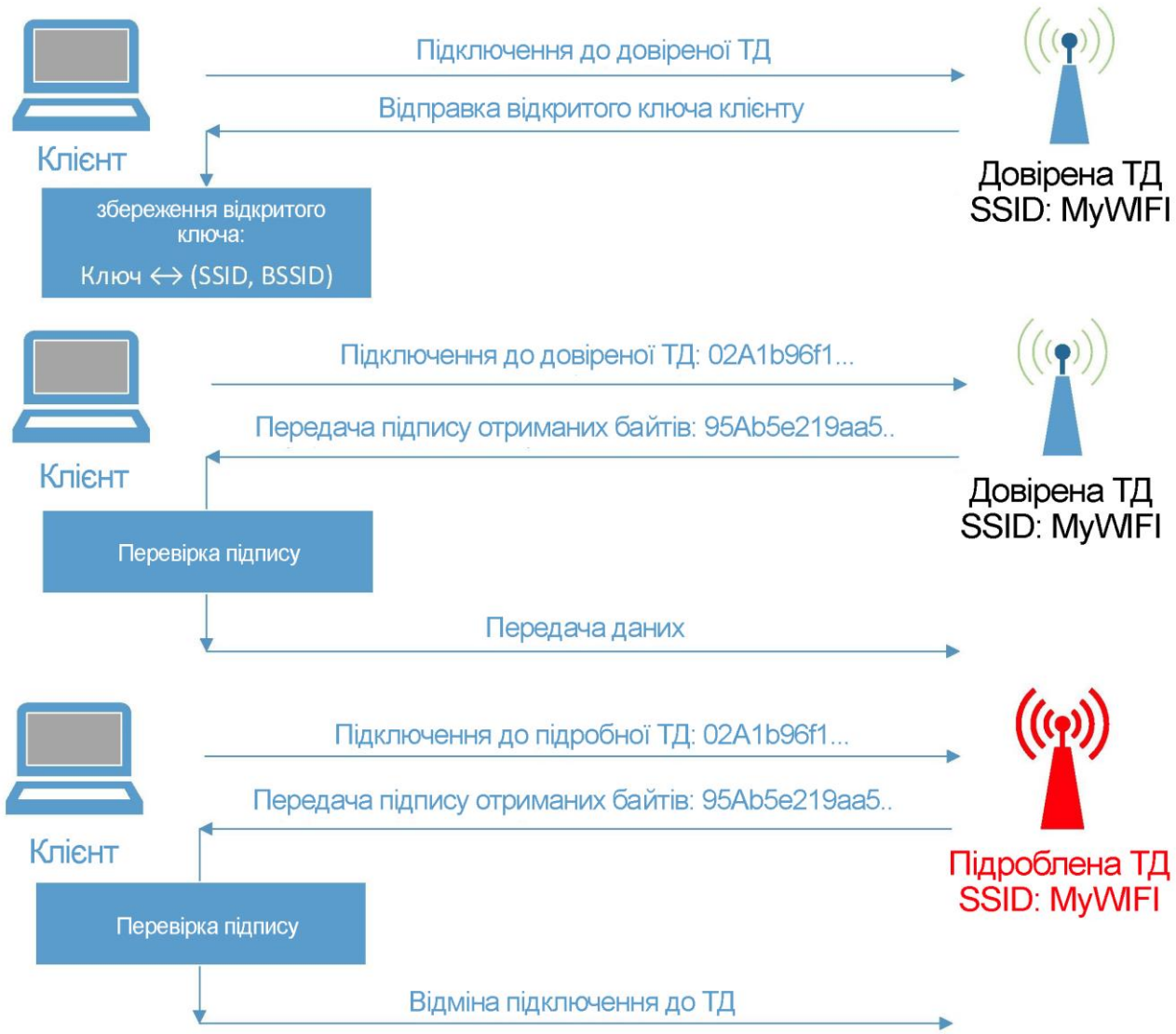


Рисунок 3.1 Схема аутентифікації точок доступу бездротовими клієнтами Wi-Fi

Існує безліч криптографічних алгоритмів з відкритим ключем, використовувані для створення й перевірки ЦП: схема RSA, ЦП Ель-Гамаля, DSA (схема така як у Ель-Гамаля), ДЕРЖСТАНДАРТ Р 34.10-2012 (схема така як у Ель-Гамаля), Eddsa, ECDSA та інші. Тому що передбачається, що й на клієнтові, і на ТД буде зберігатися в крайньому випадку (при взаємної аутентифікації) по парі відкритий-закритий ключ, а підключень може бути велика безліч, те першою вимогою при виборі алгоритму є довжина ключів, що зберігаються, повинна бути мінімальної з метою економії пам'яті. Крім цього, тому що цільовими є мобільні пристрої, то алгоритм повинен бути досить

швидким. Як відомо, алгоритми, засновані на еліптичних кривих, забезпечують більшу швидкість роботи й аналогічну крипто стійкість, що й алгоритми, що ґрунтуються на числах, однак при меншій довжині ключів [24]. Для прикладу розглянемо алгоритму DSA і його реалізацію на еліптичних кривих ECDSA. Крипто стійкість DSA ґрунтується на завданні дискретного логарифмування, крипто стійкість ECDSA ґрунтується на тій же завданні, однак розглянутої в теорії еліптичних кривих. Завдяки цьому, складність проведення атак на ECDSA зростає, і, як наслідок, довжина ключів і генеруючих підписів різко скорочується. Звичайно, довжина відкритого ключа в алгоритмах, заснованих на еліптичній криптографії, становить 32 байта (закритий становить 64 байта, але в стислому виді також 32 байта), а довжина підпису 64 байта. На малюнку 26 відображена залежність довжини ключів алгоритмів RSA/DSA і алгоритмів ECDSA/Eddsa.

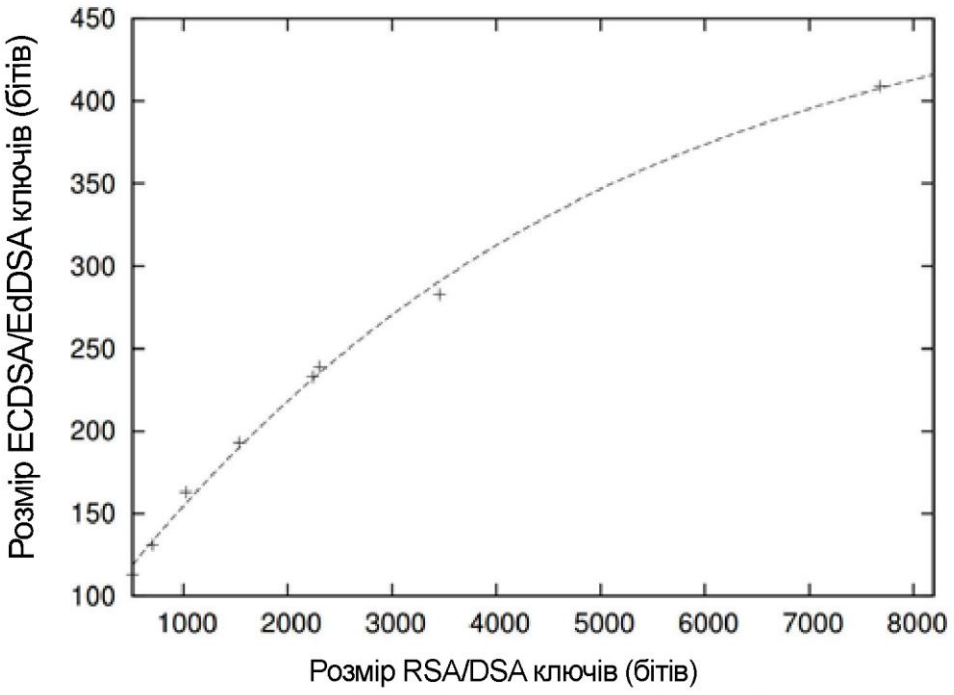


Рисунок 3.2 Залежність довжини ключів алгоритмів RSA/DSA і ECDSA (у бітах)

Тому для проведення аутентифікації слід використовувати саме протоколи ЦП, засновані на еліптичних кривих, наприклад, ECDSA або Eddsa. ECDSA є найбільш популярним алгоритмом і має реалізації на безлічі еліптичних кривих, найбільш оптимізованої з яких по швидкості й крипто стійкості є крива Curve25519. Алгоритм Eddsa був розроблений пізніше всіх і за заявою автора, Данила Бернштейна, його реалізація на еліптичній кривій Ed25519 (еквівалентна кривій Curve25519) є найбільш швидкою й безпечною криптографічною системою з відкритим ключем [25]. Однак, варто відзначити, що приріст продуктивності дуже малий, тому явних переваг у використанні того або іншого алгоритму в цьому випадку не спостерігається.

Викладену вище схему аутентифікації можна реалізувати на одному з рівнів стека протоколів TCP/IP такими способами:

- на канальному рівні в пакетах аутентифікації 802.11;
- на транспортному рівні по засобах Tcp-Сокетов;
- на прикладному рівні по засобах протоколу HTTP і веб-сокетів.

Як було сказано в п. 1.3, при підключенні після виявлення ТД відбувається обмін пакетами аутентифікації 802.11. Сам фрейм аутентифікації має такий вигляд (див. Рисунок 3.3):

Рисунок 3.3 – Структура фрейму аутентифікації

Тіло фрейму складається із чотирьох полів:

1. Номер алгоритму аутентифікації (Authentication Algorithm Number): 0 – відкрита аутентифікація, 1 – аутентифікація по розподіленому ключу (WEP).

2. Номер фрейму в послідовності (Authentication Transaction Sequence Number).

3. Код-код-статус-код (Status Code): 0 - успішно, 1 - невизначена помилка.

4. Текст аутентифікації (challenge text). Використовується при аутентифікації першого типу в 2 і 3 фреймах (див. Рисунок 6)

Як було сказано в п. 1.1.2, при використанні аутентифікації нульового типу відбувається обмін двома пакетами, а при використанні першого типу - чотирма пакетами аутентифікації, тому теоретично можливо додати нові типи аутентифікації 802.1. Пропонується ввести три додаткові типи аутентифікації:

- тип 2 - аутентифікація клієнтом точки доступу;
- тип 3 - аутентифікація точкою доступу клієнта;
- тип 4 - взаємна аутентифікація між ТД і клієнтом.

Тоді для другого типу обмін буде полягати в обміні пакетами запиту (Authentication request) і відповіді (Authentication response). У пакеті запиту клієнт буде вказувати тип 2 аутентифікації й вбудовувати поле тексту аутентифікації зі своєї випадково не сгенерованою послідовністю байтів. У відповідь на даний пакет клієнт буде одержувати підпис даного тексту також у поле тексту аутентифікації й перевіряти даний підпис. Після того, як клієнт перевірить підпис, то він ухвалює розв'язок або про проведення подальшої асоціації із ТД, або посилає пакет де аутентифікації точці, якщо підпис виявилося невірною. Викладена схема аутентифікації клієнтом ТД представлено на малюнку 3.4.

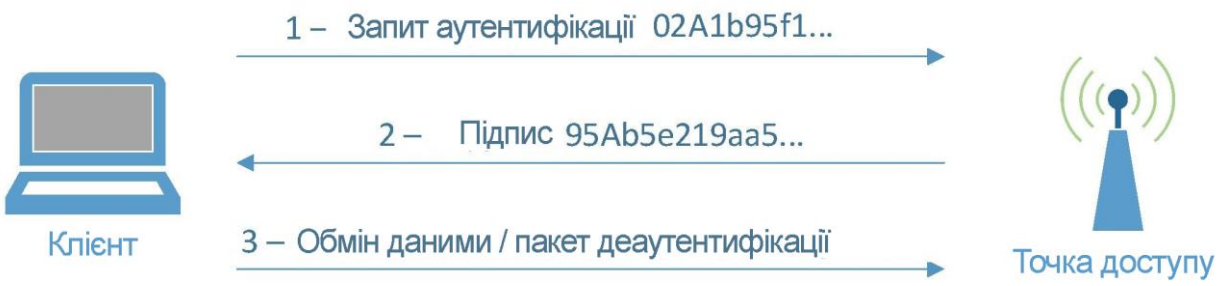


Рисунок 3.4 Схема аутентифікації клієнтом ТД

При аутентифікаціях типів 3 і 4 обмін уже буде відбуватися чотирма пакетами. Тип 3 не буде відрізнятися від уже існуючої схеми аутентифікації, викладеної в п. 1.1.2, тільки тим, що передаватися із клієнта на ТД буде не зашифрований на загальному ключі текст, а підписана клієнтом послідовність байтів. Тип 4 же буде відрізнятися, при цьому в кожному із чотирьох пакетів буде присутній поле «Challenge Text»:

1. Перший пакет із запитом на авторизацію від клієнта до ТД буде містити випадкову послідовність байтів клієнта.
2. Другий пакет, переданий від ТД клієнтові, буде містити випадкову послідовність байтів ТД.
3. Третій пакет, переданий від клієнта до ТД, буде містити підписані клієнтом байти ТД. Якщо підпис виявився вірної, то ТД переходить до кроку 4, інакше відправляє клієнтові пакет де аутентифікації.
4. Четвертий пакет, переданий від ТД до клієнта, містить підпис переданих випадкових байтів клієнта.

Схема взаємної аутентифікації на канальному рівні представлено на малюнку 3.5.

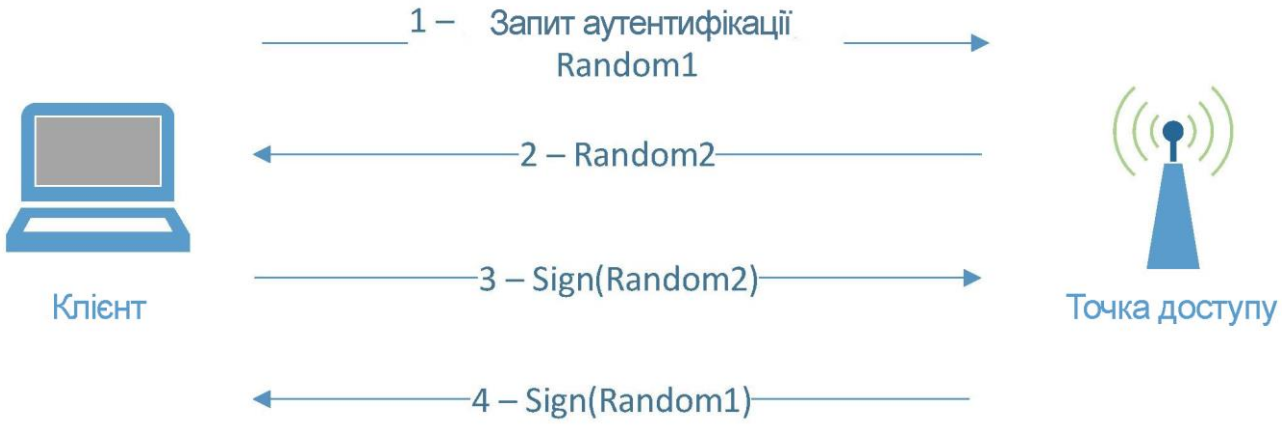


Рисунок 3.5 Схема взаємної аутентифікації між клієнтом і ТД по засобах пакетів аутентифікації 802.11

Гідність даного підходу полягає в тому, що інфраструктура пакетів аутентифікації 802.11 уже практично готова для використання даної схеми й

для реалізації через неї необхідно буде внести мінімальна кількість змін. Крім того, якщо внести зміни в сам стандарт 802.11, то схема аутентифікації стане універсальною для всіх пристроїв. Однак, внесення змін у сам стандарт є й недоліком даної схеми, тому що для цього необхідно змінити конфігурації в безлічі вже існуючих пристроїв.

Два інших способу реалізації (через Tcp-Сокети й веб-сокети) схожі між собою й пророблюють усі ті ж послідовності обміну даними, що й при реалізації на канальному рівні, однак з урахуванням особливостей реалізації технологій (див. рис.3.6). Обоє способу для свого функціонування повинні бути реалізовані в якості прикладного програмного забезпечення (ПО) і працюють прямо з API операційних систем. Обоє підходу мають явну перевагу простоти реалізації як на стороні клієнта, так і на стороні сервера. Переважніше виглядає реалізація через веб-сокети, тому що настроїти роботу через них простіше, тому що більшість ТД підтримують графічні режими керування (інтерфейс^-інтерфейси-веб-інтерфейси), що дозволить досить просто внести зміни в прошивання роутеров. Однак, незважаючи на простоту розгортання існує кілька недоліків даних підходів:

- перевага даних підходів у реалізації без зміни існуючих протоколів канального рівня є і їх недоліком, тому що губиться універсальність реалізації, тому що можливість реалізації додатка під ту або іншу платформу буде залежати від доступних функцій API;
- обоє підходу можуть виконувати свої функції тільки після того, як клієнт підключився до самої ТД уже стандартними засобами й одержав Ip-Адресу, що обслуговується їй мережі, тому що протокол Tcp-Сокети реалізовані через однойменний протокол, що працює поверх IP протоколу, а веб-сокети реалізовані над HTTP (точніше, є його розширенням), отже, працюють поверх TCP. Як наслідок, розроблювальне ПО повинне контролювати обмін даними й блокувати передачу даних на стороні клієнта, якщо ТД не була аутентифікована, у той час як на ТД забороняти доступ клієнта до мережі, якщо він не був аутентифікований.

Це утрудняє реалізацію взаємної аутентифікації й аутентифікацію клієнта точкою доступу.

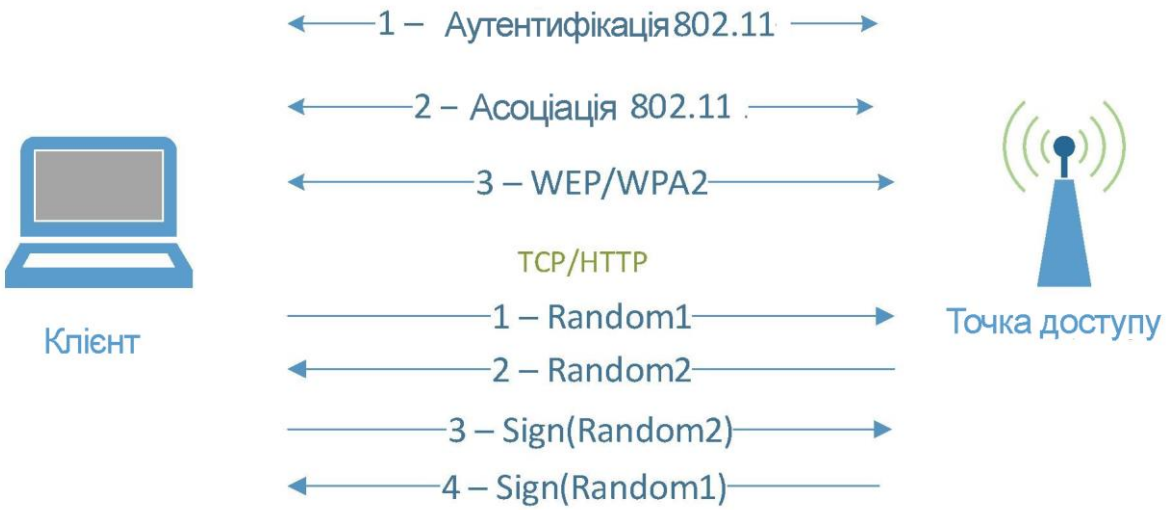


Рисунок 3.6 Схема взаємної аутентифікації між клієнтом і ТД по засобах TCP-сокетів або WEB-сокетів

3.2 Висновок до розділу 3

У третьому розділі була розроблена схема, що дозволяє аутентифікувати клієнтам точки доступу. Дана схема може застосовуватися й для додаткової аутентифікації клієнтів точками доступу й виступати в якості взаємної аутентифікації.

РОЗДІЛ 4.
ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ СХЕМИ АУТЕНТИФІКАЦІЇ

З метою демонстрації роботи запропонованої в п. 3 схеми аутентифікації між бездротовими клієнтами й ТД Wi-Fi була розроблений програмний комплекс, що реалізує аутентифікацію точок доступу клієнтами за допомогою ЦП, створюваних, що й перевіряються алгоритмом з відкритим ключем Eddsa. Комплекс складається із серверної й клієнтської частини. У якості алгоритму створення й перевірки ЦП був використаний алгоритм Eddsa у своїй реалізації на еліптичній кривій Ed25519. Довжина відкритих ключів становить 256 біт, довжина підпису становить удвічі більше – 512 біт.

4.1 Серверна частина програмного комплексу

Серверна частина є консольною програмою, емулюючу роботу ТД: включає, виключає ТД Wi-Fi на пристрої, а також підтримує роботу сервера аутентифікації. Розроблена в середовищі Node.JS мовою Javascript і є повністю стерпною на всі ОС, де підтримується середовище виконання Node.js (ОС Windows, Linux, Mac OS і ін.), за винятком тієї частини, яка відповідає за настроювання ТД Wi-Fi, тому що є особливою для кожної ОС. Керування ТД в ОС Windows проводиться викликом вбудованих команд консольної утиліти netsh. В ОС Linux конфігурування ТД проводиться за допомогою сторонньої бібліотеки wireless-tools [26], яка так само викликає стандартні команди Linux. Варто відзначити, що для демонстрації конфігурування, включення й відключення ТД можна робити без використання розробленого ПО, скориставшись стандартними засобами ОС. Інтерфейс розробленої серверної частини представлено на рисунку 4.1.

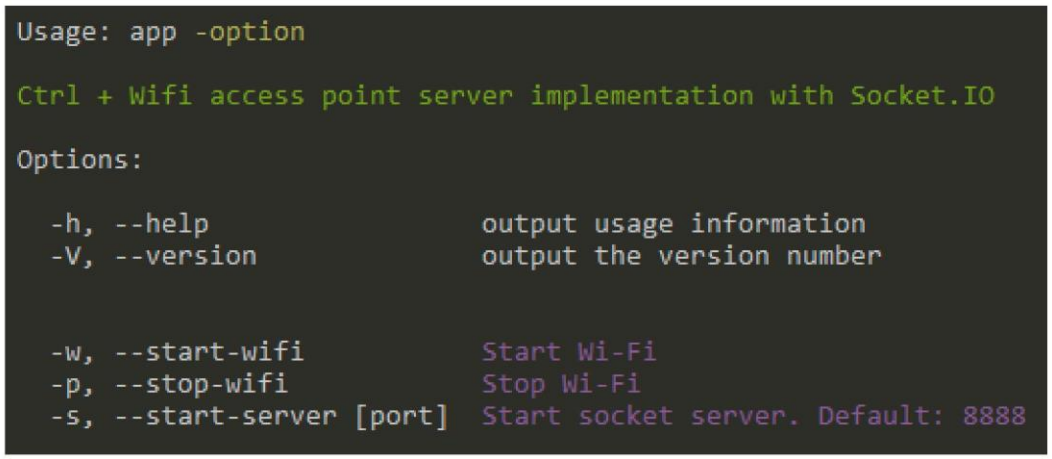


Рисунок 4.1 Інтерфейс серверної частини розробленого програмного комплексу

Аутентифікована складова розроблена за допомогою бібліотеки socket.io [27], яка реалізує роботу веб-сокетів. Для роботи сервера досить включити його на певному порту й підключити оброблювачі вхідних повідомлень, як показано у вирізці з коду нижче:

```
const server = io.listen(
     require('http').createServer(app).listen(PORT),
     options);
server.sockets.on('connection', function (socket) {
     socket.on('deriveKey', function () {
          socket.emit('deriveKeyResponse', {
               key: key.getPublic('hex')
          });
     });
     socket.on('checkKey', function (data) {
          const signature = key.sign(data).toHex();
          socket.emit('checkKeyResponse', {
               encodedString:  signature
          });
     });
});
```

Сервер аутентифікації обробляє два види подій:

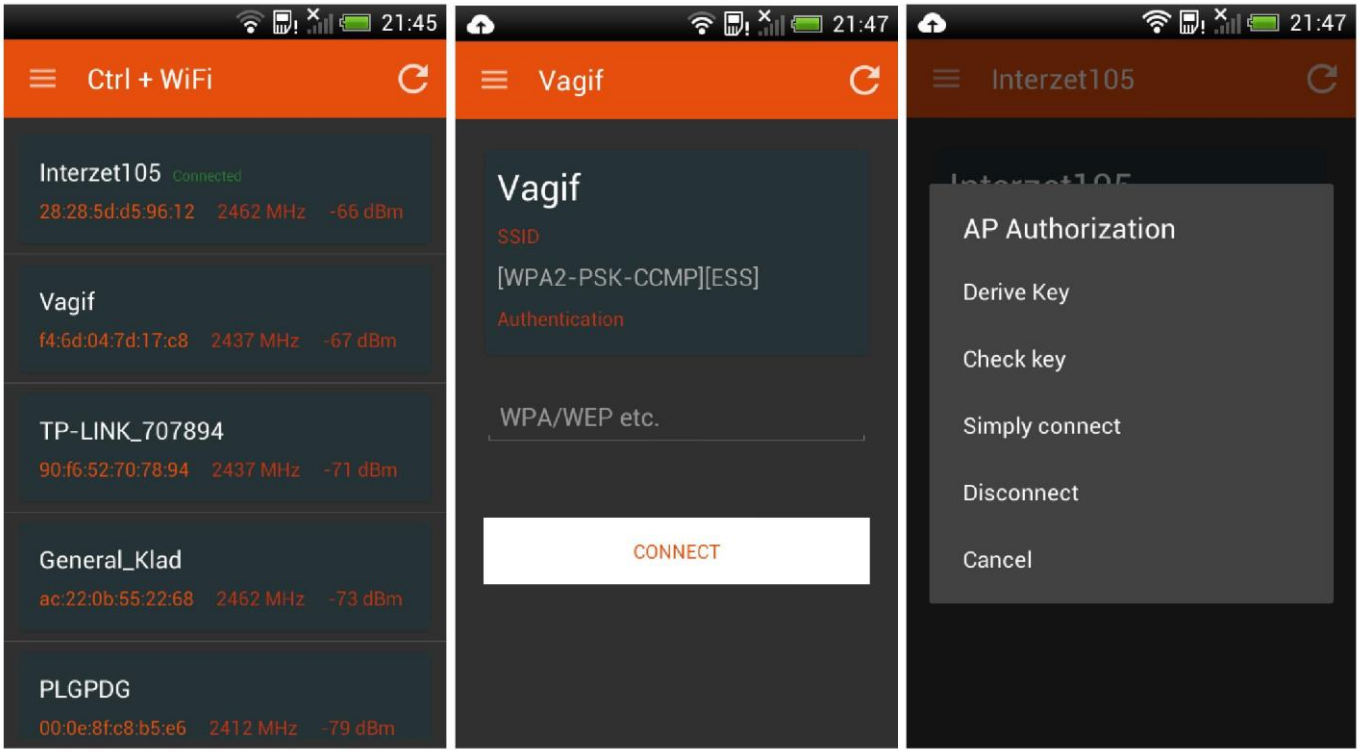
1. Одержати відкритий ключ ТД (подія «derivekey»). По настанню

даного події сервер аутентифікації генерує відкритий і закритий ключі й відправляє ОК ТД клієнтові.

2. Перевірка відкритого ключа ТД (подія «checkkey»). По вступу даного події ТД ухвалює від клієнта деяку послідовно байт, підписує її за допомогою алгоритму Eddsa на своєму закритому ключі, і відправляє підпис клієнтові.

4.2 Клієнтська частина програмного комплексу

Клієнтська частина написана мовою Kotlin і реалізована у вигляді додатка із графічним інтерфейсом під пристрої з ОС Android версії 4.0.3 і вище (використовувалося API Level 15). При запуску додатка запускається локальний сервіс VPN, який продовжує роботу у фоновому режимі. Даний сервіс працює як спрощений міжмережевий екран і забороняє передачу даних на ТД за винятком тих, що передаються на Ip-Адресу й порт ТД, на якому працює сервер аутентифікації, доти, поки ТД не була авторизована через додаток. Після авторизації в локальну базу даних заноситься інформація про те, що дана ТД аутентифікована й передачу трафіка до неї можна дозволити. Основний інтерфейс додатка відображає список доступних Wi-Fi-мереж і деяку інформацію про них: Mac-Адреса видимої точки доступу, частоту каналу в Мгц і рівень сигналу в dbm (див. Рисунок 4.2-а). При виборі конкретної мережі зі списку відкривається інтерфейс, за допомогою якого можна підключитися до мережі (див. Рисунок 4.2-б), а після авторизувати точку, одержати її ключ, підключитися без перевірки або скасувати підключення (див. Рисунок 4.2-в). Якщо клієнт уперше підключається до ТД, то він може на підставі особистої довіри до неї одержати відкритий ключ.



а б в

Рисунок 4.2 – Інтерфейс головного екрана, що відображає список доступних мереж Wi-Fi (а); інтерфейс обраної точки доступу (б); інтерфейс вибору дій для подальшої взаємодії із ТД послу підключення до неї (в)

Ключ зберігається в локальну базу даних і зіставляється з SSID мережі й Mac-адресою точки, відображуваних в інтерфейсі «Key database» (див. Рисунок 4.3), звідки їх можна вилучити на вибір відповідного елемента зі списку. При наступних підключеннях клієнт може здійснити перевірку наявності на ТД валідного закритого ключа.

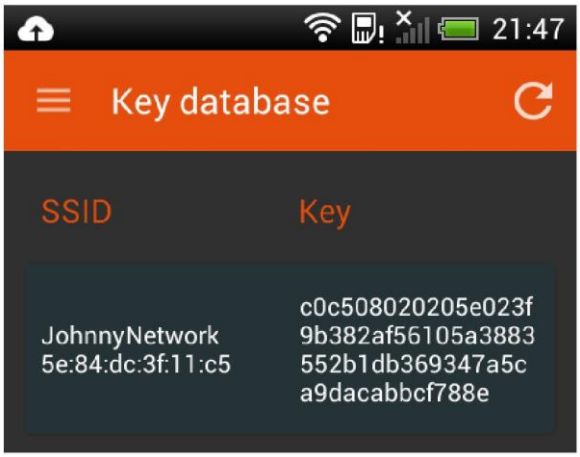
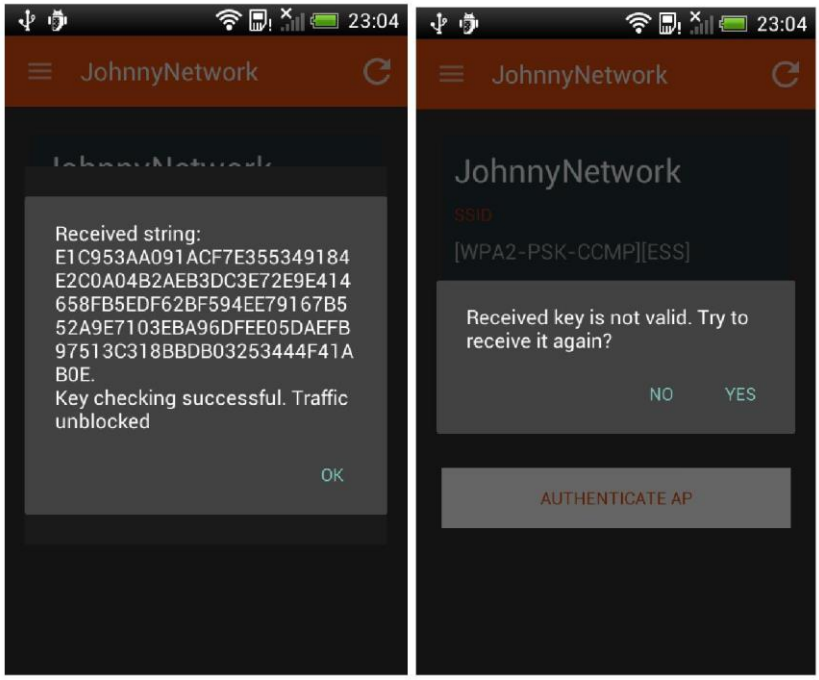


Рисунок 4.3 Інтерфейс локального сховища зіставлених мереж і ТД із їхніми відкритими ключами

Для авторизації ТД і відправлення довільної послідовності байтів клієнт підключається до веб-сервера ТД і обмінюється даними з нею по засобах веб-сокетів, реалізованих за допомогою тієї ж бібліотеки Socket.IO [28]. При успішної аутентифікації дозволяється обмін даними із ТД (див. Рисунок 4.4-а), інакше з'являється запит на повторну перевірку ключа, або скасування підключення (див. Рисунок 4.4-б).



а б

Рисунок 4.4 Спливаючі вікна при успішній (а) і невдалій (б) аутентифікації ТД

Якщо змінити послідовність байтів, на основі яких генерується закритий і відкритий ключі ТД алгоритмом Eddsa, то ОК, що зберігається на стороні клієнта, не буде парним для ЗК, що зберігаються на стороні ТД. Тому перевірка підпису переданого на ТД повідомлення не пройде, про що буде сповіщений користувач. Допустимо, споконвічно ЗК, на основі якого генерувалися ОК ТД був наступним: 693e3cab5f693e3cab5f693e3cab5f. Тоді ОК будуть мати такий вигляд:

$ОК_{ТД}$=*c0c508020205e023f9b382af56105a3883552b1db369347a5ca9dacabbcf788e*

Тепер змінимо ЗК на наступну: 693e3cab5f693e3cab5f693e3cab5**d**. У такому випадку пари ОК буде наступним:

$ОК_{ТД}$=*6da1d9401a981766d913ed939c3ae9319e5b86c9783a615a7bc95fc6b2756f12*

На стороні клієнта ж у базі збережених ключів утримується первісний ОК ТД (див. Рисунок 4.4). Тоді при перевірці користувач одержить повідомлення, що ЗК на ТД не пройшов перевірку (див. Рисунок 4.4, б).

4.3 Висновок до розділу 4

У четвертому розділі було реалізовано програмний комплекс із клієнтської й серверної частинами. Клієнтська частина розроблена під ОС Android і дозволяє аутентифікувати ТД по публічному ключу. У якості подальшої роботи може бути розглянуте питання первісної довіри клієнта до точки доступу, що може бути реалізоване, через сертифікати X.509, або через модель, використовувану в протоколі PGP (Pretty Good Privacy).

РОЗДІЛ 5.
СПЕЦІАЛЬНА ЧАСТИНА

5.1. Область застосування програмного забезпечення Microsoft Office Visio.

Програмні продукти Visio Corporation, об'єднані під загальною назвою Visio, останнім часом активно завойовують світ, виступаючи вже не в якості одного із зразків, а як еталон ділової графіки.

Коли необхідно що-небудь пояснити співрозмовникові, простіше за все взяти олівець і намалювати. Це може бути схема з декількох прямокутників, розташування якихось предметів, зв'язки між об'єктами. Практично в будь–якому звіті, нотатках, поясненнях, статтях є місце для графічного матеріалу. Десь він допомагає розібратися у суті понять і зв'язків, а десь просто робить документ більш привабливим. Усі ці застосування відносяться до ділової графіки.

Власне, для малювання на комп'ютері існують десятки різних засобів. Це і прості графічні редактори типу Paint, і системи растрової графіки типу PhotoFinish, і векторні системи типу Corel Draw. У конструюванні використовуються так звані CAD–системи (системи комп'ютерного проектування – computer – aided design).

Visio не замінює усіх існуючих, особливо сильно розвинутих професійних систем, але усе більш тіснить їх. Особливо це помітно у середовищі професіоналів. Відомо, що професіонала, що звик до одного продукту, практично неможливо схилити до переходу на інший. Але з'являється багато прикладів, коли інженер, що використовує, наприклад, AutoCAD, починає все частіше і частіше застосовувати ще й Visio. Адже існують області, для яких немає спеціалізованих продуктів окрім Visio. Не існує іншого спеціального графічного редактора для малювання хімічних структурних

діаграм, ніхто швидше Visio не впорається з малюванням блок– схем алгоритмів, структурних схем, презентаційною графікою і багатьох інших типів малюнків.

Таким чином Visio відноситься до тих продуктів, які повинні бути на кожному комп'ютері, так само як практично на кожному комп'ютері є текстовий редактор. І незалежно від того, хто за ним працює – студент або академік, початківець або професіонал – Visio надасть йому неоціниму допомогу.

5.2. Загальні принципи програми Microsoft Office Visio.

В основі механізму малювання Microsoft Office Visio лежить векторний редактор. Тобто в простому випадку, не використовуючи жодних досконаліших засобів, ви маєте декілька графічних примітивів (лінія, крива, прямокутник, еліпс тощо), за допомогою яких можна намалювати потрібне зображення, зафарбувати його фрагменти.

Для двовимірних фігур можна використовувати не лише колір, але і зразки зафарбовування. Існують команди для роботи з текстовими блоками, що використовують шрифти, встановлені у Windows, що дозволяють форматувати слова, абзаци та інші фрагменти тексту.

Одиницею малюнка у Visio є шейп (shape – форма, графічний образ). Малюнок набирається з шейпів, як з елементів конструктора, причому при роботі потрібні набори шейпів розташовуються під рукою поряд з вікном малюнка, як палітра у художника. Процес створення малюнка зводиться до перетаскування шейпів з палітри (трафарету) у вікно малюнка і додаванні з’єднувальних елементів.

Набори шейпів адаптують Visio до тієї або іншої області використання і багато в чому визначають ту або іншу версію продукту. Наприклад, версія Visio Professional містить близько 1000 мережевих і телекомунікаційних шейпів, а версія Visio Enterprise – містить велику кількість шейпів для побудови мереж LAN і WAN. Шейпів розроблена велика кількість, вони продовжують

розроблятись і можуть розроблятися самим користувачем для певної специфічної області використання.

Але це не є найголовнішою відмінністю Visio. Виявляється шейпи мають інтелект. Тобто вони знають, як поводитися при тих або інших змінах малюнка. Наприклад, може існувати шейп стіни з віконним отвором, в якому при зміні розмірів стіни збільшуються, а розміри віконного отвору залишаються незмінними, причому ці розміри автоматично відслідковуються.

І, мабуть, останній штрих – існування коннекторів – шейпів, подібних до звичайної лінії, але за рахунок своєї інтелектуальності мають здатність приклеюватися до певних точок інших шейпів, зв'язуючи їх і зберігаючи цей зв'язок при переміщенні шейпів. Тобто, ви можете пересунути декілька мікросхем на схемі двома рухами миші, і при цьому усі електричні зв'язки залишаться незмінними. Найрозумніші коннектори ще й відшукують оптимальний шлях на малюнку, щоб по можливості не перекривати інші шейпи.

5.2.1. Шаблони і трафарети.

Найважливіші елементи Visio – шаблони і трафарети – служать для адаптації програми до потрібної прикладної області і надання процессу малювання властивій Visio легкості і зручності.

Шаблон (Template) – термін, що міцно увійшов останнім часом до практики офісних додатків Windows. У загальному випадку – це спеціальний файл, в якому зберігається інтерфейс додатку, а часто і прообраз малюнка або документу. До складу основних елементів, що зберігаються, входять властивості сторінки малюнка (такі як розмір сторінки, масштаб зображення, одиниця виміру тощо), набір і параметри стилів ліній, тексту і зафарбовування, набір трафаретів, що використовуються.

Подальший розвиток шаблону – візарди (Wizards – помічники, чарівники) – програмні елементи, як при створенні нового файлу малюнка окрім відкриття шаблону і потрібних трафаретів ведуть діалог з користувачем, щоб прийняти

значення деяких змінних, і налагоджують малюнок у відповідності до їх значення.

Трафарет (Stencil) – файл з набором майстер–шейпів, зазвичай об'єднаних якою–небудь загальною ідеєю або орієнтованих на певну прикладну область.

5.2.2. Організація робочого простору Visio. Типи файлів.

Робочий простір Visio містить вікна, меню та інструменти, що використовують для малювання. Його можна налагоджувати, пристосовуючи до області діяльності або просто до своїх звичок.

Користувач може змінювати наступні елементи:

- розмір і положення вікон Visio;
- розмір і розміщення трафаретів Visio;
- спосіб відображення майстер–шейпів в новому в трафареті;
- зображення сторінки;
- лінійки, лінії сітки, точки зв'язку, направляючі лінії;
- зовнішній вигляд панелі інструментів і рядка стану.

Частіше програму Visio запускають або для того, щоб намалювати новий малюнок, або для того, щоб відредагувати існуючий.

Створення нового малюнка зазвичай починають, відкриваючи файл шаблону, який у свою чергу завантажує Visio, відкриває трафарет і сторінку малюнка.

Вже наявний файл відкривається по–різному в залежності від майбутньої роботи. Користувач може відкрити:

- початковий файл, щоб редагувати його;
- копію файла, щоб змінити файл, не впливаючи на оригінал;
- версію тільки для читання, щоб проглянути файл, не змінюючи його.

Visio використовує чотири типи файлів: шаблони, трафарети, малюнки, і робочі простори. Ви можете ідентифікувати тип файлу по em розширенню. Шаблон має розширення .VST, трафарет – .VSS, малюнок – .VSD, робочий простір – .VSW.

Після внесення істотних змін до малюнка, необхідно зберегти файл малюнка. При зміні трафарету або шаблону може виникнути потреба знадобитися зберегти їх.

За замовчуванням Visio зберігає існуючі файли в тому форматі, в якому вони були створені. Користувач може зберігати файли Visio у додаткових форматах, враховуючи більш ранні версії Visio, використовуючи команду Save As.

Для побудови діаграми, архітектура серед інших фігур у цій роботі виконувалось різних процедур такі як:

Відкрилось програму та вибралось тип фігури або архітектури, які ми хочемо зробити (рис.6.1.1.1);

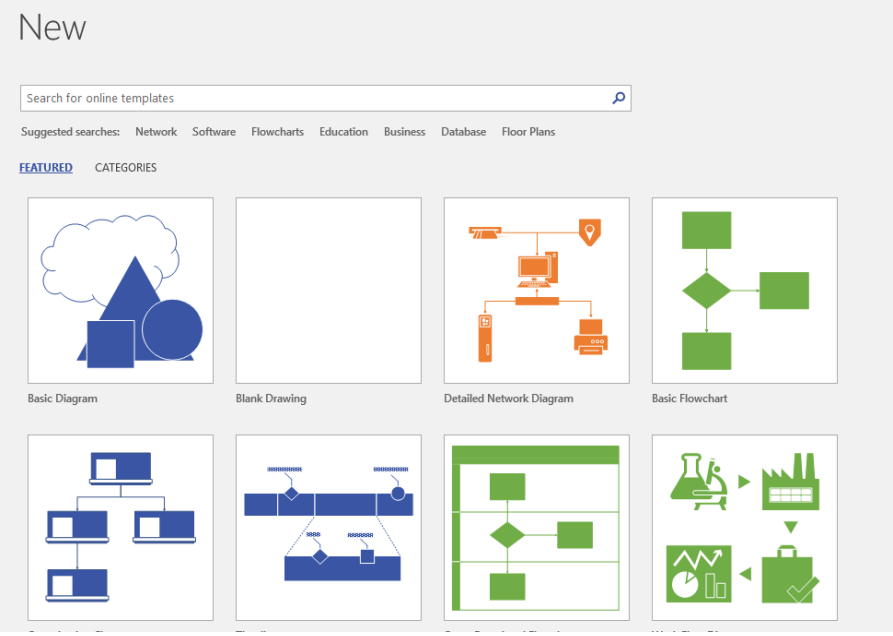


Рисунок 5.1 - Панель діаграм у програмного забезпечення VISIO

Для дипломної роботи, мова йде про супутникові системи та телекомунікації, тоді було обрано два варіанти: *Детальний сегментний діаграми* та *бланкова діаграма* (рис.5.1);

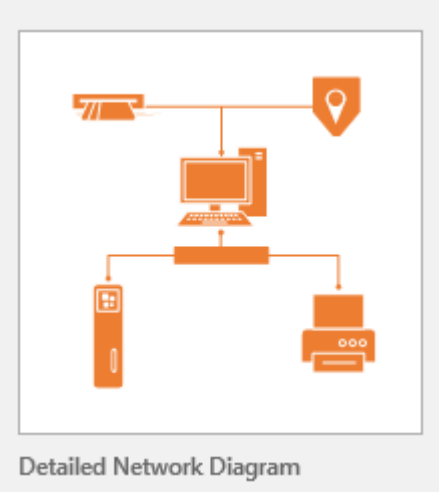


Рисунок 5.2 Детальна модель побудови мережевого діаграм

Детальна модель бо вона приносить з собою деякі мережеві пристрої. Моє завдання було тільки додати до неї кілька елементів для побудови бажаної архітектуру в цьому випадку принципову архітектуру.

Для додавання потрібних цифр та надписів потрібно як показано на (рис.5.3) вибирати TEXT BOX як показано у жовтому кольорі. Можна змінювати кольори, збільшити розмір фігури серед інших варіантів.

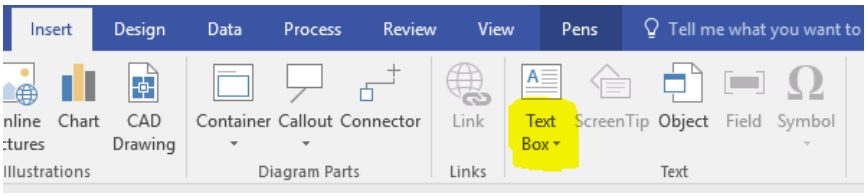


Рисунок 5.3 Вікно для додавання цифр або текст

5.3 Висновок до розділу 5

У цьому розділі описано кроки, які використовувались для побудови структурних схем та архітектури цієї магістерської роботи. За допомогою програмного забезпечення Microsoft Office Visio можна проектувати та використовувати в різних областях навчання від бухгалтерського обліку до механіки. У нього типові та унікальні функції, які багато допомагають і дуже прості у використанні.

РОЗДІЛ 6
ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

6.1 Розрахунок витрат на проведення науково-дослідної роботи

Розрахунок усіх витрат організації-виконавця НДР, пов'язаних з виконанням теми, дає можливість встановити її собівартість або кошторисну вартість.

Встановлення величини витрат на проведення робіт по темі в розрізі типових статей кошторисної вартості (калькуляції собівартості) НДР наводяться нижче.

6.1.1 Витрати на оплату праці. Витрати за цією статтею включають заробітну плату безпосередніх виконавців теми, а заробітна плата адміністративно-управлінського персоналу, працівників дослідних виробництв включаються в кошторисну вартість теми через статтю «Накладні витрати». Крім цього, слід враховувати, що для тем, які фінансуються за рахунок держбюджету прибуток не планується і тому в дану статтю витрат включається тільки основна заробітна плата (без премій та інших виплат, що здійснюються із прибутку). Витрати на оплату праці розраховують на основі даних про трудомісткість окремих робіт по темі (табл. 6.1) та посадових окладів безпосередніх їх виконавців.

Загальна трудомісткість робіт, що виконуються безпосередньо студентом (інженером - дослідником), визначається навчальним планом спеціальності магістра 163 «Біомедична інженерія».

Таблиця 6.1

Трудомісткість робіт по темі НДР

Найменування робіт по темі дослідження	Трудомісткість за виконавцями, людино-днів					
	Науковий керівник	Старший науковий співробітник	Молодший науковий співробітник	Інженер	Лаборант	Студент
1	2	3	4	5	7	8
1. Уточнення та конкретизація завдань по темі дослідження	1	–	–	–	–	1
2. Аналіз науково-технічних публікацій з теми	1	–	–	–	–	1
3. Розроблення математичної добового електроенеце-фалосигналу	1	–	–	–	–	1
4. Розроблення методу аналізу добового електроенеце-фалосигналу	1	–	–	–	–	1
5.Аналіз добового електроенеце-фалосигналу	1	–	–	–	–	1
6. Формування звіту по НДР	1	–	–	–	–	1
Разом за виконавцями теми	6	–	–	–	–	6

Подальші розрахунки витрат на оплату праці проводиться за алгоритмом, зрозумілим із табл. 6.2.

Середньоденна заробітна плата за категоріями виконавців розраховується шляхом ділення їх посадового місячного окладу на 21,2 (де 21,2 – усереднене число робочих днів за місяць).

Таблиця 6.2

Розрахунок витрат на оплату праці

Посада виконавців теми	Планова трудомісткість, люд-днів	Заробітна плата, грн		
		Посадовий місячний оклад	Середньоденна зарплата	Усього за виконавцями
1.Науковий керівник	1	4289,70	202,34	3237,44
2. Студент	1	1302	61,42	1289,82
Разом оплата праці з теми				4527,26

6.1.2 Відрахування на соціальні заходи. До цієї статті витрат належать виплати у вигляді єдиного соціального внеску, які здійснює організація – виконавець теми в пенсійний фонд в розмірі 37,26%, що становить 1686,86 грн. від загальних витрат на оплату праці.

Базою вказаного нарахування слугують загальні витрати на оплату праці по темі (табл.6.2).

6.1.3 Обладнання, необхідне для проведення досліджень. В даній статті враховують вартість усіх видів матеріалів, необхідних для проведення НДР, з вирахуванням вартості зворотних відходів.

Тематика дослідницьких робіт, які виконуються на факультеті прикладних інформаційних систем та електроінженерії, передбачає використання, перш за все, електроенцефалографа, комп’ютерів для для аналізу добового електроенцефалосигналу та формування матеріалів звітності, оргтехніки та ін.

Розрахунки зведено за формою у табл.6.3

Таблиця 6.3

Розрахунки витрат на обладнання

Найменування обладнання	Одиниця виміру	Кількість	Ринкова ціна за одиницю, грн	Сума, грн.
1. Електроенцефалограф та електроди	шт	1	25520	25520
1. ПК (системний блок, монітор, клавіатура, мишка, кабель живлення)	шт	1	4000	4000
4 Принтер лазерний	шт	1	850	850
5 Кабелі для підключення електроенцефалографа до ПК	шт	1	100	100
Загальні витрати на матеріали				30470

6.1.4 Енергоносії для проведення досліджень. На підприємстві електроенергія використовується для електроенцефалографа, освітлення, живлення медобладнання, комп'ютерної техніки та оргтехніки [ ]:

$$З_{см} = \sum_{i=1}^{n} P_i \cdot Ц_i, \qquad (6.1)$$

де P_i – витрата і-го виду матеріального ресурсу, натуральні одиниці;

$Ц_i$ - ціна за одиницю і-го виду матеріального ресурсу, грн.

i - вид матеріального ресурсу;

n - кількість видів матеріальних ресурсів.

Якщо для проведення НДР використовується електрообладнання, то необхідно розрахувати витрати на електроенергію за формою (6.1), наведеною в таблиці 6.4.

Таблиця 6.4

Витрати на електроенергію

Найменування обладнання	Паспортна потужність, Вт	Коефіцієнт використання потужності	Час роботи обладнання для розробку АІС, год	Ціна електро-енергії, Грн/ (кВт/год)	Сума, грн.
Електроенце-фалограф	100	0,25	3	2,68	201
ПК (системний блок, монітор, клавіатура, мишка, кабель живлення)	150	0,25	90	2,68	3618
Принтер лазерний	700	0,15	5	2,68	804
Лампи розжарювання (освітлення)	80	0,45	10	2,68	134
РАЗОМ витрати на електроенергію					4757

6.1.5 Витрати на службові відрядження. Дані витрати складаються із фактичних витратна службові відрядження штатних працівників, зайнятих виконанням НДР: витрат на проїзд до місця відрядження і назад; витрат на проживання у готелі; добових витрат, які розраховуються на кожний день перебування у відрядженні, враховуючи час перебування в дорозі, та деякі інші.

Під час виконання НДР здійснюються ряд відряджень, які пов’язанні із доповідями на конференціях, які наведено у таблиці 6.5.

Таблиця 6.5

Приблизні витрати на службові відрядження

Тип відрядження	Кількість	Приблизна вартість відрядження
Конференція	5	2000
Здача звітів НДР	1	200
Впровадження результатів НДР	3	900
Всього	–	4600

6.1.6. Розроблення планової калькуляції кошторисної вартості теми. Планова калькуляція вартості проведення досліджень по темі складається на підставі виконаних розрахунків та нормативних даних (табл.6.6).

Таблиця 6.6

Планова калькуляція кошторисної вартості НДР (умовні дані)

Найменування статей витрат	Сума, грн	Обґрунтування
1	**2**	**3**
1.Витрати на оплату праці	4527,26	Відповідно до розрахунків
2.Відрахування на соціальні заходи	1686,86	Відповідно до діючих загальнодержавних нормативів
3.Обладнання для проведення досліджень	30470	Відповідно до розрахунків
4.Енергоносії для проведення досліджень	4757	Відповідно до розрахунків
5.Витрати на службові відрядження	4600	Відповідно до розрахунків
6.Інші невраховані прямі витрати по темі	4604,10	10% від суми прямих розрахованих витрат по темі
7.Кошторисна вартість теми	50645,20	Сума попередніх статей

Кінцевим результатом науково-дослідницьких робіт є досягнення наукового, науково-технічного, економічного, соціального, екологічного та інших видів ефектів.

Науковий ефект від виконання теми передбачає приріст наукових знань у певній сфері науки, а науково-технічний ефект характеризує можливість використання цих наукових знань в інших наукових напрямах та при розробці принципово нових технічних рішень. Економічний ефект відображає потенціал НДР в досягненні кращого співвідношення результатів виробництва до витрат і має прогнозний характер. Соціальний ефект заводиться до збільшення числа робочих місць, поліпшення умов праці та побуту, скорочення тривалості робочого тижня, розвитку охорони здоров’я, науки, культури, освіти.

Екологічний ефект полягає в поліпшенні стану навколишнього середовища, зменшенні електромагнітного та іонізуючого випромінювання тощо.

6.2 Науково-технічна ефективність науково-дослідної роботи

Економічна оцінка фундаментальних і пошукових НДР у вартісному вимірі, як правило, неможливо, бо ймовірність доведення результатів таких досліджень до конкретного практичного застосування невелике. Для таких досліджень рекомендується [25] визначати науковий та науково-технічний ефект, який враховує результати наукових досліджень та їх значущість для прискорення науково-технічного прогресу та розвитку національної економіки.

Науковий та науково-технічний ефект рекомендується оцінювати коефіцієнтом науково-технічної ефективності ($E_{нт}$) за допомогою формули [25]:

$$E_{нт} = \frac{\sum B_i \cdot Б_{ij}}{\sum B_i \cdot Б_{ij}^{\max}}, \qquad (6.2)$$

де B_i – нормативні значення коефіцієнтів вагомості факторів науково-технічної ефективності (табл. 6.7);

$Б_{ij}$ – середнє значення балу, який виставляється експертами і-му фактору;

$Б_{ij}^{\max}$ – максимально можливе значення балу (табл. 6.8);

i – порядковий номер фактору;

j – відповідна характеристика і-го фактора.

Нормативні значення коефіцієнтів вагомості факторів науково-технічної ефективності наведені в табл. 6.7.

Таблиця 6.7

Нормативні значення коефіцієнтів вагомості факторів науково-технічної ефективності

Фактори (i)	Коефіцієнти вагомості (B_i)
1.Новизна очікуваних або одержаних результатів	0,25
2.Глибина наукового опрацювання	0,16
3.Ступінь ймовірності успіху	0,09
4.Перспективність використання результатів	0,25
5.Масштаб можливої реалізації результатів	0,15
6.Завершеність одержаних результатів	0,10
Разом	1,00

Характеристика факторів науково-технічної ефективності НДР наведена в табл. 6.8.

Таблиця 6.8

Характеристика факторів науково-технічної ефективності НДР

Фактор наукової та науково-технічної ефективності	Характеристика фактора	Оцінка фактора	
		Якісна	Бальна A_{ij}^{max}
1	**2**	**3**	**4**
1.Новизна одержаних або передбачуваних результатів	Одержані принципово нові результати, раніше невідомі в науці, розроблена нова теорія, відкрита нова закономірність	Висока	10
	Встановлені деякі часткові закономірності, методи, способи, які дозволяють створити принципово нові види техніки	Середня	7
	Позитивне вирішення поставлених задач на підставі простих узагальнень, аналіз зв'язків між факторами, розповсюдження відомих наукових принципів на об'єкти	Недостатня	3
	Опис окремих елементарних фактів, передача та поширення отриманих раніше результатів, реферативні огляди	Тривіальна	1

1	2	3	4
2.Глибина наукового опрацювання	Проведена значна кількість експериментів по нетрадиційним методикам, виконані складні теоретичні розрахунки, підтверджені експериментальними даними	Істотна	10
	Проведена обмежена кількість розрахунків по відомим методикам, виконані теоретичні розрахунки невисокої складності, частково перевірені експериментальними даними	Середня	6
	Проведена недостатня кількість експериментів, виконані прості теоретичні розрахунки без експериментальної перевірки	Несуттєва	1
3.Ступінь ймовірності успіху	Висока ймовірність повного вирішення поставлених задач НДР	Значна	10
	Середня ймовірність вирішення більшості експериментальних або теоретичних задач	Помірна	6
	Низька ймовірність вирішення поставлених задач, отримання позитивних результатів сумнівне	Незначна	1
4.Масштаб використання результатів	Результати можуть бути використані в багатьох наукових напрямках, мають значення для розвитку суміжних наук	Широкий	10
	Результати можуть бути використані в конкретному науковому напрямку при розробці нових технічних рішень, спрямованих на суттєве підвищення продуктивності суспільної праці	Достатньо широкий	8
	Результати будуть використані при проведені наступних НДР, при розробці нових технічних рішень в конкретній галузі	Достатній	5
5.Ступінь реалізації результатів	Строк впровадження,роки: До 2	Висока	10
	До 4	Середня	7
	До 6	Достатня	4
	Більше 6	Недостатня	2
6.Завершення одержаних результатів	Авторське свідоцтво, стаття в фаховому виданні, методика, інструкція, класифікатор, стандарти, нормативи.	Висока	10
	Технічне завдання на прикладну НДР	Середня	8
	Рекомендації, розгорнутий аналіз, пропозиції	Достатня	6
	Огляд, інформаційне повідомлення	Недостатня	3

Кількісна оцінка факторів науково-технічної ефективності НДР здійснюються експертним шляхом за десятибальною шкалою і визначається як середньоарифметичне. Отримані результати зводять за формою табл. 6.9.

Таблиця 6.9

Результати розрахунків науково-технічної ефективності НДР

Фактори науково-технічної ефективності	Характеристика фактора	Розрахунок $Б_{ij}$			$Б_{ij}^{max}$
		Експертні оцінки		$Б_{ij}$	
		1	2		
1	2	3	4	5	6
1.Новизна очікуваних або одержаних результатів	Встановлені деякі часткові закономірності, методи, способи, які дозволяють створити принципово нові види техніки	5	5	5	10
2.Глибина наукового опрацювання	Проведена обмежена кількість розрахунків по відомим методикам, виконані теоретичні розрахунки невисокої складності, частково перевірені експериментальними даними	8	8	8	10
3.Ступінь ймовірності успіху	Середня ймовірність вирішення більшості експериментальних або теоретичних задач	6	6	6	10
4.Перспективність використання результатів	Результати можуть бути використані в конкретному науковому напрямку при розробці нових технічних рішень, спрямованих на суттєве підвищення продуктивності суспільної праці	8	8	8	10
5.Масштаб можливої реалізації результатів	До 2 років	10	10	10	10
6.Завершеність одержаних результатів	Рекомендації, розгорнутий аналіз, пропозиції	6	6	6	10

Розраховане за формулою 6.2 значення $E_{нт}$ буде відображати рівень наукової та науково-технічної ефективності конкретної теми фундаментального чи пошукового дослідження:

$$E_{нт} = \frac{0.25 \cdot 5 + 0.16 \cdot 8 + 0.09 \cdot 6 + 8 \cdot 0.25 + 10 \cdot 0.15 + 6 \cdot 0.1}{1 \cdot 10} = 0{,}717 .$$

Загальну оцінку бакалаврської НДР можна здійснити, користуючись даними табл. 6.10.

Таблиця 6.10

Загальна оцінка наукової та науково-технічної ефективності фундаментальних та пошукових НДР

Загальна оцінка наукової та науково-технічної ефективності		Можливі рекомендації по результатам виконання НДР
Розраховане значення $E_{нт}$	Загальна якісна оцінка ефективності	
0,91-1,00	Відмінно	Оформлення авторського свідоцтва, публікація у фаховому виданні, продовження досліджень по даній тематиці
0,76-0,90	Дуже добре	
0,61-0,75	Добре	Рекомендації можуть бути сформульовані після ретельного аналізу отриманих результатів
0,36-0,60	Достатня	Переглянути технічне завдання у разі продовження досліджень по даній темі
Менш 0,35	Незадовільна	Здійснити всебічний аналіз отриманих результатів по темі

6.3 Висновки до розділу 6

У розділі на підставі виконаних розрахунків та нормативних даних встановлено, що планова калькуляція вартості проведення досліджень по темі становить 50645,20 грн., а кількісна оцінка науково-технічна ефективність науково-дослідної роботи, яка здійснюються експертним шляхом за десятибальною шкалою і визначається як середньоарифметичне, що складає 0,717 від максимального числа 1, а рекомендації по результатам виконання НДР можуть бути сформульовані після ретельного аналізу отриманих результатів.

РОЗДІЛ 7
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Охорона праці

Під час роботи з радіотехнічними системами враховано всі небезпечні фактори ризику (перевищений рівень шуму та вібрацій, електротравматизм, негативний вплив освітлення освітлення та інші), які би негативно впливали на рівень безпеки обслуговуючого персоналу в процесі експлуатації системи.

Оскільки система, живиться безпосередньо від електромережі, тому необхідно максимізувати рівень електробезпеки обслуговуючого персоналу шляхом адекватного дотримання правил роботи з електроприладами, зокрема системою, які прописані в стандарті ГОСТ 12.1.030-81 «ССБТ. Електробезпека. Захисне заземлення. Занулення» [38].

Із врахуванням вище сформульованого припущення, встановлена необхідність розроблення рекомендації по питанням охорони праці при роботі з радіотехнічною системою шляхом аналізу негативного впливу електричного струму на обслуговуючий персонал при роботі із системою, способів нормування та захисту від його дії.

Внаслідок дії електричного струму на організм обслуговуючого персоналу під час експлуатації блоку може виникнути загальна (електричний удар) або місцева електротравма (опіки, електричні знаки, електрометалізація шкіри, механічні пошкодження). Розрізняють три ступені впливу струму при проходженні через організм людини (змінний струм) [38]:

- відчутний струм – початок болісних відчуттів (до 0-1,5 мА);
- невідпускний струм – судоми і біль, важке дихання (10-15 мА);
- фібриляційний струм – фібриляція серця при тривалості дії струму 2-3с, параліч дихання (90-100 мА).

На рисунку 7.1 зображено основні фактори, які впливають на організм

людини при ураженні електричним струмом.

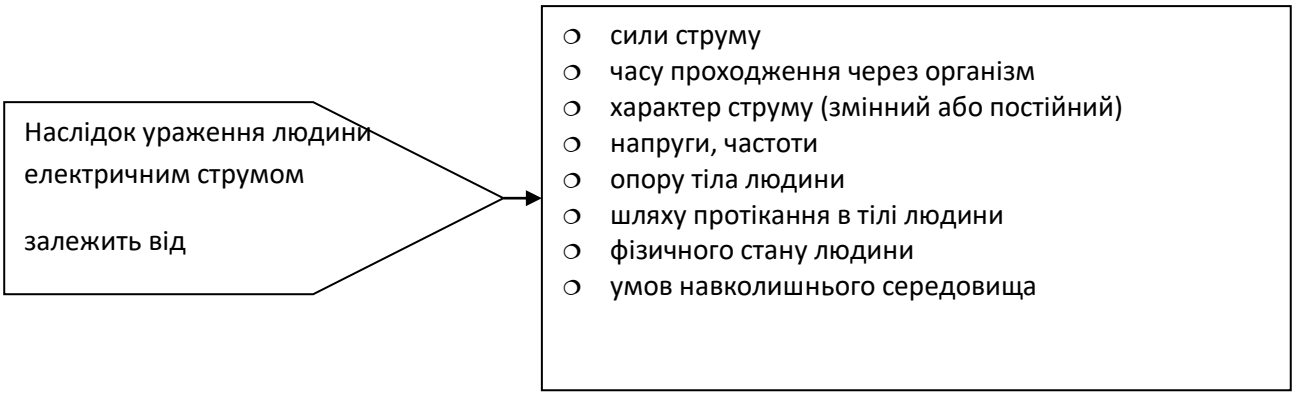


Рисунок 7.1. Фактори впливу електричного струму на людину

Правильне визначення необхідних засобів та заходів обслуговуючого персоналу від ураження електричним струмом необхідно враховувати гранично допустимі значення напруг дотику та струмів, що проходять через тіло людини по шляху "рука - рука" чи "рука - ноги" (таблиця 7.1) (регламентується ГОСТом 12.1.038-82).

Таблиця 7.1

Гранично допустимі значення напруги дотику та сили струму, що проходить через тіло людини

Вид струму	Нормоване значення	Тривалість струму, сек					
		0,1	0,2	0,5	0,7	1	Більше1
Змінний, 50 Гц	Напруги дотику, В (не більше)	500	250	100	70	50	36
	Сила струму, мА (не більше)	500	250	100	70	50	6

Основне завдання електробезпеки - мінімізувати можливість негативного впливу електричного струму на людину. Досягти цієї мети можна за допомогою таких заходів і засобів: 1) безпечною і надійною конструкцією елементів системи; 2) організаційними та технічними заходами щодо безпечної

експлуатації системи та використання електричної енергії; 3) технічними засобами захисту.

У даному випадку це досягнуто шляхом конструктивного виконання складових системи класу I, який відповідає вимогам технічних умов і стандарту ГОСТ 12.1.030-81. Згідно класу I складові системи мають робочу ізоляцію і виконаний таким чином, що підключити його до електричної мережі можна лише після під'єднання корпусу до заземлювача (нульового захисного провідника), а при від'єднанні від мережі - корпус відключається від заземлювача (нульового захисного провідника) в останню чергу.

Стан ізоляції струмопровідних частин відповідає правилам використання системи. Цими правилами передбачене періодичне випробування ізоляції 2 рази на рік у приміщеннях зі складними умовами, підвищеною вологістю і 1 раз на рік у приміщеннях з нормальним середовищем. Ізоляція створює великій опір, який перешкоджає протіканню через неї струму. Опір ізоляції складових системи становить не меншим 0,5 МОм (згідно вимог ГОСТ 12.1.030-81). Якщо опір ізоляції знижується на 50% від початкового, мережу або ізоляцію необхідно замінити.

При роботі в приміщеннях без підвищеної небезпеки напруга складових системи повинна бути не більше 220 В. При роботі в приміщеннях з підвищеною небезпекою і за межами приміщень напруга складових системи повинна бути не більше 36 В. В особливих умовах дозволяється використовувати блок з напругою до 220 В, але при наявності захисного відключення або надійного заземлення корпусу з використанням захисних засобів (діелектричні рукавички, килимки, калоші).

Захисне заземлення - навмисне електричне з'єднання із землею металевих струмопровідних неструмоведучих частин, на яких може з'явитися напруга. Заземлення - це сукупність заземлювача і заземлювальних провідників. Заземлювачі можуть бути штучні (створені спеціально для заземлення блоку) і природні. Для штучних заземлювачів застосовують вертикальні і горизонтальні електроди. Вертикальні - зі стальних прутів діаметром 10-12мм, кутової сталі

розміром 40х40 мм або стальних труб діаметром 30-50мм, довжиною 2,5-3 м. Вертикальні електроди з'єднують стальною штабою розміром 4х12 мм або круглим дротом діаметром не менше6 мм. Опір заземлюючого пристрою не повинен перевищувати 4-10 Ом (перевіряється щорічно).

Таким чином врахувавши вище сформульовані рекомендації по питанням охорони праці при експлуатації радіотехнічної системи буде забезпечено небезпечні умови праці обслуговуючого персоналу.

7.2 Безпека в надзвичайних ситуаціях

7.2.1. Структура та завдання Єдиної державної системи запобігання і реагування на надзвичайні ситуації техногенного і природного характеру (ЄДСЗР).

Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного і природного характеру (ЄДСЗР) включає в себе центральні та місцеві органи виконавчої влади, виконавчі органи рад, державні підприємства, установи та організації з відповідними силами і засобами, які здійснюють нагляд за забезпеченням техногенної та природної безпеки, організовують проведення роботи із запобігання НС техногенного та природного походження і реагування у разі їх виникнення з метою захисту населення і довкілля, зменшення матеріальних втрат.

Основною метою створення ЄДСЗР є забезпечення реалізації державної політики у сфері запобігання і реагування на НС, забезпечення цивільного захисту населення.

Завданнями ЄДСЗР є:

– розробка нормативно-правових актів, а також норм, правил та стандартів із питань запобігання надзвичайним ситуаціям та забезпечення захисту населення і територій від їх наслідків;

– забезпечення готовності центральних та місцевих органів виконавчої влади, виконавчих органів рад, підпорядкованих їм сил і засобів до дій, спрямованих на запобігання і реагування на НС;

– забезпечення реалізації заходів щодо запобігання виникненню НС;

– навчання населення щодо поведінки та дій у разі виникнення НС;

– виконання цільових і науково-технічних програм, спрямованих на запобігання НС, забезпечення сталого функціонування підприємств, установ та організацій, зменшення можливих матеріальних втрат;

– збирання й аналітичне опрацювання інформації про НС, видання інформаційних матеріалів з питань захисту населення і територій від наслідків НС;

– прогнозування й оцінка соціально-економічних наслідків НС, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах;

– створення, раціональне збереження і використання резерву матеріальних та фінансо вих ресурсів, необхідних для запобігання і реагування на НС;

– та інше.

ЄДСЗР складається з постійно діючих функціональних і територіальних підсистем і має 4 рівні: загальнодержавний, регіональний, місцевий та об’єктовий.

Функціональні підсистеми створюються міністерствами та іншими центральними органами виконавчої влади для організації роботи, пов’язаної з запобіганням НС та захистом населення і територій від їх наслідків.

Кожний рівень ЄДСЗР має координуючі та постійні органи управління щодо розв’язання завдань у сфері запобігання НС, захисту населення і території від їх наслідків, систему повсякденного управління, сили і засоби, резерви матеріальних та фінансових ресурсів, системи зв’язку та інформаційного забезпечення.

До системи повсякденного управління ЄДСЗР входять оснащені необхідними засобами зв’язку оповіщення, збирання, аналізу і передачі інформації:

– центри управління в НС, оперативно-чергові служби уповноважених органів з питань НС та цивільного захисту населення усіх рівнів;

– диспетчерські служби центральних і місцевих органів виконавчої влади, державних підприємств, установ та організацій.

До складу сил і засобів ЄДСЗР входять відповідні сили і засоби функціональних і територіальних підсистем, а також недержавні (добровільні) рятувальні формування, які залучаються до виконання відповідних робіт.

7.2.2. Техногенні небезпеки та їх вплив на життєдіяльність людини. У результаті активної діяльності людини в середовищі існування воно поволі змінювало свій вигляд, що призвело до порушення біосфери і появи штучного середовища, яке називають техногенним (техносферою). За науковими даними, на сьогоднішній день майже все середовище, в якому перебуває людина, є техногенним. Штучно створена людиною техносфера охоплює практично всю планету і навіть вийшла за її межі у космос.

Техногенне середовище (техносфера) як складова навколишнього середовища є похідною діяльності людини, яка виникла як наслідок впливу антропогенних чинників.

Діючи у техногенному середовищі, людина безперервно виконує, як мінімум, два основних завдання:

— забезпечує своє комфортне перебування у середовищі проживання;

— створює та використовує системи захисту від його негативних чинників впливу.

Вплив негативних чинників техносфери на людину. До середини XX століття людина ще була неспроможною ініціювати великомасштабні аварії та катастрофи, які б викликали зміни у біосфері. Поява об'єктів ядерної енергетики, потужних хімічних підприємств та висока концентрація їх у певних регіонах зумовили руйнування екосистеми. Класичними прикладами є трагедія

у Чорнобилі (Україна), Бхопалі (Індія). Створена руками і розумом людини техніка ніби й була покликана максимально задовольнити її потреби у комфорті та безпеці, але загалом не виправдала сподівань. Біосфера у багатьох регіонах планети активно змінювалася техносферою. Це, у свою чергу, призвело до зниження якості компонентів системи "Л — НС" і, перш за все, природного середовища. За прогнозами вчених, цей вплив буде і в подальшому збільшуватися із поглибленням глобалізації світової економіки.

Розрізняють прямий і непрямий вплив на навколишнє середовище та організм людини негативних чинників техносфери.

Прямий вплив — це виробничий і побутовий травматизм, професійні захворювання.

Непрямий вплив — це погіршення складу повітря, якості води, їжі тощо.

При певних умовах цей негативний вплив може призвести до зростання концентрації домішок у біосфері і погіршення екологічної рівноваги, збільшення кількості захворювань населення та тварин, посилення епідеміологічного неблагополуччя.

Середовище техносфери сучасного існування людини поділяють на побутове та виробниче.

Виробниче середовище — це простір, де людина провадить свою трудову діяльність. До нього належать підприємства, організації, установи, заклади освіти, транспорт, комунікації тощо. Виробниче середовище характеризується певними параметрами його життєздатності і життєдіяльності, специфічними для кожного виробництва. В умовах виробничого середовища на здоров'я людини можуть впливати небезпечні та шкідливі виробничі фактори (НіШВФ).

Деякими з таких факторів є:

— електричний струм;

— рівень шуму;

— рівень вібрації;

— рівень теплового, електромагнітного випромінювань;

— ступінь загазованості, запиленості.

Перелічені небезпечні і шкідливі виробничі фактори повинні відповідати певним параметрам, які людина визначає сама, проектуючи і будуючи ті чи інші об'єкти. Межа зміни параметрів повинна гарантувати безпеку, а у деяких випадках — і комфорт трудової діяльності. При цьому функціонування об'єкта загалом повинно бути безпечним.

Дія небезпечних і шкідливих виробничих факторів може призвести до травматизму і професійного захворювання людини.

Кожні 3 хвилини у світі внаслідок к виробничого травматизму чи професійного захворювання помирає людина.

Щороку в Україні на виробництві травмується понад 60 тисяч осіб. З них приблизно до 2 тисяч осіб зі смертельним наслідком. 10 тисяч осіб набувають професійних захворювань і 6 тисяч стають інвалідами. Щорічно в результаті нещасних випадків на виробництві економіка України зазнає збитків у розмірі 4 млрд. грн.

7.2.3. Призначення першої долі карської допомоги та загальні принципи її надання. У результаті виникнення й розвитку будь-якої надзвичайної ситуації можуть з'явитися постраждалі або навіть жертви. Характер надзвичайної ситуації не дає змоги заздалегідь підготувати ресурси, необхідні для надання медичної допомоги (медичний персонал, медикаменти, лікувальні установи, спеціалізований транспорт). У зв'язку з цим постає питання про надання першої долікарської допомоги потерпілим.

Перша долікарська допомога — це комплекс простих термінових дій, спрямованих на збереження здоров'я і життя потерпілого.

Якщо людина постраждала в результаті надзвичайної ситуації, треба передусім звільнити її, винести з небезпечної зони, вжити потрібних заходів щодо відновлення життєво важливих функцій організму і запобігти ускладненням, що становлять загрозу для життя людини. Вчасно й правильно здійснена перша долікарська допомога рятує життя потерпілому і попереджає

розвиток несприятливих результатів. У разі відсутності поблизу людей потерпілий має сам подбати про себе.

При організації надання першої медичної допомоги особливу увагу необхідно звернути на її своєчасність, зокрема при травмах, що супроводжуються кровотечею, шоком, асфіксією, втратою свідомості, отруєнням. В обсязі першої долікарської допомоги особливого значення набуває виконання таких заходів, як зупинення зовнішньої кровотечі за допомогою тампонів, перев'язувальних пакетів, накладення джгута (закручення за допомогою підручних засобів), введення знеболювальних засобів, усунення асфіксії, проведення штучного дихання, непрямий масаж серця з метою відновлення серцевої діяльності, закриття поверхні рани пов'язкою тощо.

Не менш важливим етапом надання першої допомоги постраждалому є раціональне його транспортування до лікарської установи, де йому буде надано кваліфіковану медичну допомогу.

При наданні першої долікарської допомоги необхідно:

1) керуватися принципами правильності, доцільності, швидкості, продуманості, рішучості, спокою;

2) дотримуватись послідовності таких дій:

• усунути вплив на організм факторів, що загрожують здоров'ю та життю потерпілого (звільнити від дії електричного струму, винести із зараженої зони чи з приміщення, що горить, погасити палаючий одяг, дістати з води);

• оцінити стан потерпілого, визначити характер і тяжкість травми, що становить найбільшу загрозу життю потерпілого, і послідовність заходів щодо його рятування;

• виконати необхідні дії щодо рятування потерпілого в порядку терміновості (забезпечити прохідність дихальних шляхів, провести штучне дихання, зовнішній масаж серця, зупинити кровотечу, іммобілізувати місце перелому, накласти пов'язку тощо);

• викликати швидку медичну допомогу чи лікаря або вжити заходів для транспортування потерпілого в найближчу медичну установу;

• підтримувати основні життєві функції потерпілого до прибуття медичного працівника, пам'ятаючи, що зробити висновок про смерть потерпілого має право лише лікар.

Засвоєння знань прийомів надання першої долікарської допомоги постраждалим у надзвичайних ситуаціях є однією з найважливіших складових підготовки працівників служби цивільного захисту України.

7.3 Висновки до розділу 7

У підрозділі з охорони праці розроблено рекомендації по питанням охорони праці при роботі з радіотехнічною системою шляхом аналізу негативного впливу електричного струму на обслуговуючий персонал при роботі із системою, способів нормування та захисту від його дії.

У підрозділі з безпеки в надзвичайних ситуаціях проаналізовано заходи організаційно-технічного характеру протипожежного захисту на виробництві радіотехнічної системи.

РОЗДІЛ 8
ЕКОЛОГІЯ

8.1 Вплив Wi-Fi частот на здоров’я людини

Сучасний світ неможливо уявити без Інтернету. Глобальна мережа міцно увійшла в наше життя. Середньостатистична людина проводить в Інтернеті від двох до десяти годин в день, тому проблема стабільного з'єднання висувається на перший план. Вирішити її допомагає мережа Wi-Fi. Однак чи безпечна вона так, як здається на перший погляд?

Існує безліч думок щодо того, шкідливий для нашого здоров'я Wi-Fi чи ні. Бездротове підключення до мережі, яке може використовувати велика кількість людей одночасно, є сьогодні практично у всіх громадських місцях. Багато хто з нас встановили роутер будинку, і тепер користується інтернетом легко та комфортно. Але чим популярнішою стає ця технологія, тим більше виникає суперечок щодо її безпеки для людини [1].

Wi-Fi - це абревіатура відомої торгової марки, яка використовується для організації бездротового з'єднання до Інтернету. Щоб якесь обладнання отримало право називатися Wi-Fi, потрібно, щоб воно пройшло спеціальні випробування, встановлені світовими стандартами Wi-Fi Alliance [2].

Wi-Fi було винайдено в 1996 році, його творцем вважається інженер Джон О'Салліван. Інновацію швидко та гідно оцінили: Wi-Fi не тільки забезпечував надійне і, що вкрай важливо, бездротове з'єднання, але і швидко окупався. Wi-Fi стали встановлювати в готелях, кафе, вокзалах і інших громадських місцях.

Щоб встановити Wi-Fi, потрібно мати хоча б одну точку доступу і одного Користувача. Зрозуміло, між ними повинен бути безперервний контакт [2].

Роутер з Wi-Fi-технологією «ділиться» з іншим обладнанням високошвидкісним доступом до інтернету за допомогою електромагнітних хвиль — саме через них виникли суперечки про шкоду цієї технології.

Електромагнітні хвилі присутні в нашому житті вже багато років, адже ще колись їх використовували в радіоприймачах для передачі сигналу. Сьогодні завдяки їм стала можливою робота великої кількості техніки — від ноутбуків і мобільних телефонів до мікрохвильової печі [3].

В епоху розвитку всіляких технологій немає нічого дивного в тому, що люди починають турбуватися за своє здоров'я, на яке можуть вплинути різні електромагнітні випромінювання. На багатьох форумах гаряче обговорюється дана проблема. Деякі люди свідомо відмовляються від використання Wi-Fi. Вони переконують громадські організації наслідувати їхній приклад.

Зупинимося на наступних параметрах Wi-Fi-роутера:

- Потужність випромінювання.
- Радіус впливу.
- Тривалість використання пристрою і його розташування.

Частота роутера, становить 2,4 ГГц — як і в мікрохвильовій печі, але остання набагато шкідливіша для здоров‘я. Чому? Вся справа в потужності — у мікрохвильовці вона в десятки разів вища, саме цей показник визначає вплив випромінювання на людину. Таким же чином порівнюємо роутер з мобільним телефоном — у першого пристрою потужність вимірюється у показнику мВт, а ось у стільникового вона становить мінімум 1 Вт, що в рази вище. Таким чином, потужність випромінювання Wi-Fi-роутера незначна порівняно з іншою технікою.

Зверніть увагу на те, як розташовується мережеве обладнання в будинку. Оскільки ми користуємося доступом до мережі без прив‘язки до роутера, потужність випромінювання ділиться пропорційно відстані до вас. Той же смартфон ми прикладаємо безпосередньо до вуха при розмові, тому він сильніше впливає на наше здоров‘я і шкідливий в більшій мірі, так як багато хто з нас протягом дня здійснюють досить багато дзвінків.

Має значення те, скільки часу ми зазвичай користуємось пристроєм — якщо просидіти цілий день за ноутбуком, це вплине на нас гірше, ніж двохвилинна розмова по телефону. Тому все залежить не від наявності або відсутності випромінювання в будь-якій техніці, а від того, наскільки доцільно й помірковано ми її використовуємо. Щоб Wi-Fi роутер зміг завдати дійсно суттєвої шкоди людському організму, потрібно, щоб він діяв на вас цілеспрямовано і з великою силою [3].

Бездротові пристрої: мобільні телефони, ноутбуки, планшети створюють електромагнітні поля, що нагрівають тканини живого організму [4].

Про це застерігає La Vanguardia [5].

Такі висновки роблять не лише вчені, але й влада ЄС, де діє стандарт, що обмежує потужність випромінювання пристроїв мобільного зв‘язку.

«Чимало фахівців і деякі громадські організації вимагають посилити заходи безпеки при використанні wi-fi та нових технологій, особливо в громадських місцях, особливо у школах та лікарнях», – йдеться у статті.

Фонд Vivo Sano підрахував: дитина, що ходить у дитячий садок і школу з 3 до 16 років, буде більше 10 тис. годин зазнавати впливу випромінювання бездротових пристроїв.

ВООЗ зазначає, що головний ефект від радіовипромінювання – нагрівання тканин організму. Щоправда, випромінювання мобільного телефону великою мірою абсорбується шкірою, а в мозку чи інших внутрішніх органах температура підвищується незначно. Що ж стосується мереж wi-fi, то вони впливають на мозок ще слабке, ніж телефони, запевняє Елізабет Кардіс із Центру досліджень епідеміології навколишнього середовища.

8.2 Джерела іонізуючих випромінювань і методи їх знешкодження

Іонізуючим випромінюванням називається випромінювання, взаємодія якого з речовиною призводить до утворення у цій речовині іонів різного знаку. Іонізуюче випромінювання складається із заряджених та незаряджених

частинок, до яких відносяться також фотони. Енергію частинок іонізуючого випромінювання вимірюють у позасистемних одиницях – електрон-вольтах, еВ. 1 еВ = 1,6·10-19 Дж.

Джерело іонізуючого випромінювання (джерело випромінювання) – об'єкт, що містить радіоактивну речовину, або технічний пристрій, який створює або в певних умовах здатний створювати іонізуюче випромінювання. Пристрій для генерування іонізуючого випромінювання (нерадіонуклідне джерело) - технічний пристрій (рентгенівська трубка, прискорювач, генератор і т. п.), в якому іонізуюче випромінювання виникає за рахунок зміни швидкості заряджених часток, їх анігіляції або ядерних реакцій.

Всі джерела іонізуючих випромінювань поділяються на закриті та відкриті.

Відкриті джерела іонізуючого випромінювання – це рідкі, газоподібні або у вигляді порошків чи суспензій радіоактивні речовини при використанні яких можливе забруднення оточуючого середовища, потрапляння на одежу персоналу, на шкіру та в організм людини.

Закриті джерела випромінювання влаштовані так, що це виключає забруднення оточуючого середовища. До них слід відносити: рентгенівські установки; радіоактивні препарати у вигляді бус, трубок, голок; гамма-терапевтичні апарати; лінійні та циклічні прискорювачі, де радіоактивний препарат знаходиться у металічній герметичній трубці.

Види іонізуючих випромінювань:

1) α-(Альфа)-випромінювання- - корпускулярне випромінювання, що складається з ядер гелію (He). 2) Нейтрони.

3) β-Бета-випромінювання - корпускулярне електронне або позитронне (протонне).

4) γ-(Гама)-випромінювання - короткохвильове електромагнітне (фотонне) випромінювання, довжина хвилі λ.

Радіаційна безпека являє собою комплекс заходів, що спрямовані на обмеження опромінення населення та запобігання виникнення як ранніх, так і віддалених наслідків опромінення.

Головними принципами протирадіаційного захисту є:

-захист кількістю – розрахунок допустимої активності джерела випромінювання;

-захист відстанню – розрахунок допустимої відстані до джерела випромінювання; -захист часом – розрахунок допустимого часу роботи із джерелом іонізуючого випромінювання;

-захист за допомогою екранування – розрахунок необхідної товщини захисного екрану;

-хімічні методи захисту – використання спеціальних фармацевтичних препаратів і сполук: радіопротекторів та радіоінгібіторів;

-захист культурою праці – дотримування правил техніки безпеки та особистої гігієни.

Правила роботи з закритими радіонуклідними джерелами і пристроями, що генерують іонізуюче випромінювання, відображені в Основних санітарних правилах (ОСП-72/87, ОСПУ-2001, ОСПУ-2005).

8.3 Висновки до розділу 8

ВИСНОВОК

У даній дипломній роботі були проаналізовані існуючі протоколи безпеки, застосовувані в Wi-Fi мережах, з погляду запобігання доступу підроблених клієнтів до ТД і проведення атак підроблених ТД. Результати показують, що в більшості випадків протоколи забезпечують аутентифікацію клієнтів у мережі, однак не забезпечують аутентифікацію ТД. Внаслідок цього проаналізовано існуючі методи й засобу захисту, які можуть захистити клієнтів Wi-Fi від підроблених ТД як з боку мережі, так і з боку клієнта. У ході дослідження було виявлено, що існуючі методи й засобу не дозволяють повною мірою захиститися від підроблених ТД. Тому була розроблена схема, що дозволяє аутентифікувати клієнтами точки доступу. Дана схема може застосовуватися й для додаткової аутентифікації клієнтів точками доступу й виступати в якості взаємної аутентифікації. Для демонстрації працездатності розробленої схеми було реалізовано програмний комплекс із клієнтської й серверної частинами. Клієнтська частина розроблена на ОС Android і дозволяє аутентифікувати ТД по публічному ключу. У якості подальшої роботи може бути розглянуте питання первісної довіри клієнта точки доступу, що може бути реалізоване, наприклад, через сертифікати X.509, або через модель, використовувану в протоколі PGP (Pretty Good Privacy), за назвою Web Of Trust, коли безліч учасників взаємодії, відомих клієнтові, дозволяють припустити, що даної ТД можна довіряти з певною часткою ймовірності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Программное обеспечение CommView for Wi-Fi. 2015. URL: http://www.tamos.ru/products/commview/.

2. Программное обеспечение Aircrack-ng. 2015. URL: http://www.aircrack-ng.org/.

3. Authentication Types for Wireless Devices. 2008. URL: http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuth enticationTypes.html#wp1034623.

4. Changhua He, John C Mitchell. Security Analysis and Improvements for IEEE 802.11i. 2004. URL: http://seclab.stanford.edu/pcl/mc/papers/NDSS05.pdf.

5. 802.1X: Port-based network access control. 2010. URL: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf.

6. AAA protocols. 2013 URL: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/acsuserguide/rad_tac_phase.html.

7. FreeRadius. Enterprise Wi-Fi / IEEE 802.1X. 2015. URL: http://freeradius.org/enterprise-wifi.html.

8. Extensible Authentication Protocol (EAP). 2004. URL: https://tools.ietf.org/html/rfc3748.

9. Cisco Wireless LAN Security Overview. 2006. URL: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html.

10. The Working Group for WLAN Standards. 2016. URL: http://www.ieee802.org/11/.

11. WPA2™ Security Now Mandatory for Wi-Fi CERTIFIED™ Products. 2006. URL: http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products.

12. IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements. 2004. URL:

http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

13. IETF RFC 4017. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. 2005. URL: https://www.ietf.org/rfc/rfc4017.txt.

14. Understanding the updated WPA and WPA2 standards. 2005. URL: http://www.zdnet.com/article/understanding-the-updated-wpa-and-wpa2-standards/.

16. Типы фреймов сети стандарта IEEE 802.11. 2011. URL: http://wi-life.ru/texnologii/wi-fi/wi-fi-frames-management-control-data -

17. What are passive and active scanning. 2016. URL: http://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning.

18. Wi-Fi сети: проникновение и защита. 3) WPA. OpenCL/CUDA. Статистика подбора. 2014. URL: https://m.habrahabr.ru/post/226431/.

19. Cisco Rogue Management. 2013. URL: http://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_ Detection.html.

20. Программное обеспечение. Waidps. URL: https://github.com/SYWorks/waidps.git.

21. Программное обеспечение EvilAP_Defender. URL :https://github.com/moha99sa/EvilAP_Defender/wiki.

22. Программное обеспечение Smart Wi-Fi Toggler. URL: https://play.google.com/store/apps/details?id=com.sebouh00.smartwifitoggler.

23. Программное обеспечение HTTPS Everywhere. URL: https://www.eff.org/https-everywhere.

24. Криптография с открытым ключом 2011 URL: http://www.intuit.ru/studies/courses/28/28/lecture/20422.

25. Ed25519: high-speed high-security signatures. URL: https://ed25519.cr.yp.to/.

ДОДАТКИ

ДОДАТОК А

УДК 004.056
П.П. Процик, к.т.н В.Л. Дунець
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ МЕТОДІВ ЗАХИСТУ МЕРЕЖ Wi-Fi

P.P. Protsyk, Ph. D. V.L. Dunets

ANALYSIS OF PROTECTION METHODS OF THE Wi-Fi NETWORKS

Функціонування більшості сучасних підприємств базується на використанні комп'ютерних мереж. Для ефективного вирішення задач, пов'язаних із мобільністю та масштабністю мережі, доцільно використовувати бездротові комп'ютерні мережі стандарту IEEE 802.11. В той же час використання бездротових мереж створює нові виклики, пов'язані з розробкою систем захисту від кіберзагроз. Якщо захисту мережі не приділити належної уваги може трапитись втрата конфіденційної інформації користувачів, втрата доступу до ресурсів і дисків користувачів Wi-Fi-мереж і ресурсів LAN, спотворення інформації, що проходить в мережі, впровадження підроблених точок доступу і т.п. [1]

Класифікувати методи захисту бездротової мережі можна за різними ознаками, в першу чергу існують методи фізичного, технічного та програмного захисту. В даному дослідженні акцент робиться на останньому, як такому, що є найбільш прогресивним. Методи програмного захисту у свою чергу поділяються на методи обмеження доступу, методи автентифікації і шифрування [2].

Одним із методів обмеження доступу є фільтрування MAC-адрес. Даний метод дозволяє визначити список пристроїв і дозволити лише цим пристроям доступ до вашої мережі Wi-Fi (whitelist), або навпаки заборонити певним пристроям доступ (blacklist). На жаль, цей метод ефективний лише в теорії, на практиці такий захист проблемно налаштовувати і дуже легко обійти. MAC-адреси можуть легко підробляти (клонувати) в багатьох операційних системах, тому будь-який пристрій може претендувати на одну з дозволених унікальних MAC-адрес. Вони надсилаються повітрям, коли кожен пакет даних переходить до пристрою та з нього, оскільки MAC-адреса використовується для того, щоб кожний пакет даних потрапляв на правильний пристрій. Тож цей метод, хоча і існує, проте не забезпечує ефективного захисту мережі.

Ще одним методом обмеження доступу є режим прихованого SSID. SSID (Service Set Identifier) – це ідентифікатор мережі, який за замовченням надсилається маршрутизатором або точкою доступу бездротової мережі у режимі broadcast, тобто всім. Зазвичай точки доступу мережі Wi-Fi надсилають своє мережеве ім'я як один з інформаційних елементів, які входять до деяких кадрів керування, ці елементи, або маяки, з інформаційним елементом, ідентифікатором якого є 0. Приховати SSID, тобто припинити його транслювати в ефір, також вважається одним із методів захисту. Проте, на мою думку, це ще один не ефективний і скоріше теоретичний метод захисту. Один із фахівців Microsoft Стів Райлі про даний метод висловився так: «SSID – це мережеве ім'я, а не пароль. Бездротова мережа має SSID, щоб відрізняти її від інших бездротових мереж поблизу. SSID ніколи не розроблявся, щоб бути прихованим, і тому не забезпечить вашу мережу будь-яким захистом, якщо ви намагаєтесь сховати його» [3]. Даний метод не є ефективним, через те, що ідентифікатор "прихованої" мережі дуже легко знайти з допомогою короткочасного програмного сканування всіх доступних мереж в радіусі доступу.

Наступним методом обмеження доступу є статична IP-адресація. Цей метод захисту полягає у відключені динамічного призначення локальних IP-адрес центральною станцією (маршрутизатором), натомість вимагаючи від користувачів вручну налаштовувати відповідні параметри мережі (адресу, маску, DNS-сервер, шлюз, тощо). Про те цей метод також не є

досить ефективним, адже не забезпечує достатнього захисту від злому. До того ж, такий спосіб адресації значно ускладнює адміністрування мережі, зокрема в частині додавання нових вузлів та погіршує масштабування мережі, що неприпустимо в бездротових мережах, адже вони, навпаки, мають покращувати цей параметр. Тож загалом вищеописані методи обмеження доступу сьогодні не є ефективними при побудові системи захисту від кіберзагроз бездротових мереж.

Наступна категорія методів захисту - це методи автентифікації. До них належать відкрита автентифікація, автентифікація зі спільним ключем (WEP, WPA) і автентифікація за допомогою RADIUS-сервера.

Відкрита автентифікація дозволяє будь-якому бездротовому пристрою автентифікуватись, а потім намагатися встановити зв'язок з точкою доступу. Це не завжди означає, що одразу після автентифікації буде надано доступ до мережі. Після автентифікації може бути запитано пароль, ключову фразу, додаткові ідентифікаційні дані, тощо. Проте, такий метод автентифікації також не захищає мережу від зловмисників і може використовуватись лише на точках доступу, що відділені від основної мережі додатковими засобами захисту, наприклад брандмауером.

Автентифікація зі спільним ключем (WEP, WPA). Даний метод автентифікації є найпопулярнішим, а його ефективність залежить від стандарту захисту, який використовується для його реалізації. Під час автентифікації за допомогою спільного ключа, ключі клієнта та точки доступу повинні співпадати. Першим стандартом захисту з використанням спільного ключа був WEP (Wired Equivalent Privacy), проте попри свою гучну назву (Захист еквівалентний дротовому) цей стандарт має слабкі місця, через які процес несанкціонованого доступу до мережі стає дуже простим. До переваг даного алгоритму можна віднести лише швидкодію та простоту реалізації. Що ж стосується недоліків, то основним є те, що на сьогодні існують дієві методи атаки на цей алгоритм, що робить його використання не доцільним в сучасних системах. Тому цей стандарт хоч і підтримується більшістю маршрутизаторів, проте з 2004 року офіційно вважається застарілим. На зміну стандарту WEP прийшов стандарт WPA (Wi-Fi Protected Access) і цей стандарт виключив можливість простого способу атаки через прослуховування трафіка і, відповідно, прибрав необхідність повторно використовувати ключі шифрування. В основі стандарту WPA лежить протокол тимчасової цілісності ключів TKIP (Temporary Key Integrity Protocol). TKIP динамічно генерує новий 128-бітний ключ для кожного пакета і тим самим запобігає WEP-скомпрометованим типам атак. TKIP та відповідний стандарт WPA реалізують три нові функції безпеки для вирішення проблем безпеки, що виникали в WEP-захищених мережах [5]. По-перше, TKIP реалізує ключову функцію змішування, яка поєднує таємний корінний ключ з вектором ініціалізації, перш ніж передавати його до ініціалізації. По-друге, WPA реалізує лічильник послідовності, щоб захистити мережу від повторних атак. Пакети, що надходять не по встановленому порядку, будуть відхилені точкою доступу. По-третє, TKIP реалізує 64-розрядну перевірку цілісності повідомлень (MIC). TKIP гарантує, що кожен пакет даних надсилатиметься з унікальним ключем шифрування. Змішування ключів збільшує складність розшифровування ключів, надаючи зловмиснику суттєво менше даних, які були зашифровані за допомогою будь-якого одного ключа. Перевірка цілісності повідомлення запобігає прийняттю підроблених пакетів. У WEP було можливим змінити пакет, вміст якого був відомий, навіть якщо він не був розшифрований. Проте, незважаючи на ці зміни, слабкість захисту деяких з цих доповнень дозволила створити нові, хоч і більш складні, способи атак. Протокол TKIP не вважається надійним і офіційно не підтримується стандартом 802.11 з 2012 року [4].

Із різноманітності методів захисту для побудови бездротової Wi-Fi мережі найбільш ефективним є комбінація використання стандарту захисту WPA2 та протоколу шифрування CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) з використанням складного ключа доступу (наприклад 14-и значного набору випадкових цифр та літер).

WPA2 виправила помилки попереднього стандарту і в основі даного стандарту лежить протокол шифрування CCMP, який в свою чергу базується на принципово новому алгоритмі шифрування AES (Advanced Encryption Standard). AES працює на принципі проектування, відомому як мережа заміщення-перестановки, що поєднує як заміщення, так і перестановку, і швидко працює як у програмному, так і в апаратному забезпеченні. Хоч і дана модель захисту не є досконалою і її ефективно та відносно просто можна атакувати при використанні слабкого кодового слова (паролю), такого як словникове слово, простий набір цифр, тощо. Вдала атака на мережу, захищену за стандартом WPA2 з ключем, розміром 256 біт хоча і можлива теоретично, проте вимагає високої кваліфікації зловмисника, спеціального програмного/технічного забезпечення, та, що найголовніше, значного проміжку часу. Проте, і ці методи організації захисту не є досконалими і, окрім програмного захисту, потрібно також враховувати необхідність постійного моніторингу роботи мережі, організацію технічного та фізичного захисту [6].

Автентифікація за допомогою RADIUS-сервера. Remote Authentication Dial In User Service (RADIUS) або Віддалений ідентифікаційний набір в службі користувача - це протокол, що забезпеує трирівневу систему: автентифікація, авторизація та облік і використовується для віддаленого доступу до мережі. Ідея полягає в тому, що існує сервер, який виконує функції «охоронця», перевіряючи ідентифікацію через ім'я користувача та пароль, які вже заздалегідь визначені користувачем. Сервер RADIUS також може бути налаштований для виконання політик та обмежень користувачів, а також запису облікової інформації, такої як час підключення для таких цілей, як платіж. Такий метод захисту досить надійний, проте вимагає додаткового обладнання, налаштування та може застосовуватись лише в комбінації з іншими методами захисту. Такий підхід захисту бездротових мереж, як правило застосовують у великих корпоративних мережах.

Провівши аналіз та порівнявши особливості методів захисту слід зауважити, що технології обмеження доступу не є надійними при побудові систем захисту комп’ютерних мереж стандарту IEEE 802.11, а що стосується методів авторизації та шифрування, то лише використання комбінації сучасних протоколів/алгоритмів та коректне налаштування мережевого обладнання дозволяє отримати прийнятний рівень безпеки.

Література

1. О. Юдін, Г. Конахович, О. Корченко, Захист інформації в мережах передачі даних: підруч. К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009, 714 с.
2. «Защита беспроводных сетей, WPA: теория и практика» [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://www.ixbt.com/comm/prac-wpa-eap.shtml (дата звернення: 14.04.2019).
3. «S. Riley, Myth vs reality: Wireless SSIDs». [Електронний ресурс] [Веб-сайт]. - Режим доступу: https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids. [дата звернення: 14.04.2019].
4. Щербаков В.Б., Ермаков С.А. «Безопасность беспроводных сетей: стандарт IEEE 802.11». - М: РадиоСофт, 2010, - 255 с.
5. Кіберполіція: захист мереж WI-FI - на дуже низькому рівні, 2017. [Електронний ресурс]. Режим доступу: https://www.ukrinform.ua/rubric-technology/ 2281044-kiberpolicia-zahist-merez-wifi-na-duze-nizkomu-rivni.html [дата звернення: 14.04.2019].
6. Пролетарский А.В., Баскаков И.В., Чирков Д.Н. «Беспроводные сети Wi-Fi». - М:Бином. Лаборатория знаний, 2007,-178 с.