Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту (роботи)

Магістр
(освітній ступінь)

на тему: Методи та технології захисту інформації в Wi-Fi мережах стандарту 802.11

Виконав: студент 6 курсу, групи СБм-61
спеціальності
125 «Кібербезпека»
(шифр і назва спеціальності (напряму підготовки))
(підпис) Мартинюк І.Є.
(прізвище та ініціали)

Керівник (підпис) Александер М.Б.
(прізвище та ініціали)

Нормоконтроль (підпис) Кареліна О.В.
(прізвище та ініціали)

Рецензент (підпис) Гладьо Ю.Б.
(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Методи та технології захисту інформації в Wi-Fi мережах стандарту 802.11 // Дипломна робота освітнього рівня «Магістр» // Мартинюк Іван Євгенович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм–61 //Тернопіль, 2019// С. – , рис. – *45* , табл. – *13* , слайдів – *16* , додат. – *1* , бібліогр. – *18* .

Ключові слова: АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, АУДИТ, БЕЗДРОТОВА МЕРЕЖА, ШИФРУВАННЯ

Дипломна робота присвячена побудові та реалізації комплексного підходу для забезпечення надійного механізму захисту інформації в безпровідній Wi-Fi мережі.

У першому розділі дипломної роботи виконано огляд архітектури комп'ютерної мережі стандарту EEE 802.11 та топологій бездротових мереж. Проаналізовано основні елементи процесу доступу до середовища стандарту.

У другому розділі здійснено огляд алгоритмів аутентифікації в безпровідних мережах, сформульовано основні цілі та завдання аудиту комп'ютерної мережі, описано засоби проведення та методику аудиту мережі, досліджено сервіси захисту RADIUS і TACACS+.

У третьому розділі практично досліджено модель проведення аудиту захищеності безпровідних мереж, запропоновано профіль захисту для мереж стандарту 802.11, описано логічні зв'язки в структурі механізмів захисту. Досліджено використання технологій захисту передачі даних та доступу до мережі Wi-Fi.

У четвертому розділі дипломної роботи описано процеси встановлення та налаштовування сервера контролю безпечного доступу ACS, а також конфігурування точки доступу Wi-Fi для аутентифікації через описаний сервер.

П'ятий розділ дипломної роботи присвячений обґрунтування економічної

ефективності проведеного дослідження.

У шостому розділі висвітлені важливі питання охорони праці та безпеки в надзвичайних ситуаціях.

Сьомий розділ описує екологічні питання, які виникли при розробці.

ANNOTATION

Methods and technologies of information protection in standard 802.11 of wi-fi networks // Martyniuk Ivan // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cibersecurity// Ternopil, 2019 // P. - , Fig. - *45* , Table - *13* , Slide - *16* , References - *18* .

Keywords: AUTHENTICATION, AUTHORIZATION, ACCOUNTING, ENCRYPTION, WIRELESS NETWORK

The diploma thesis is to build and implement a comprehensive approach to provide a reliable mechanism for protecting information on wireless Wi-Fi.

The first section of the thesis examines the architecture of the EEE 802.11 computer network and wireless network topologies. The basic elements of the process of access to the standard environment are analyzed.

The second section reviews the wireless authentication algorithms, outlines the main goals and objectives of the computer network audit, describes the network audit tools and techniques, explores RADIUS and TACACS + security services.

The third section examines the security audit model for wireless networks, proposes a security profile for 802.11 networks, and describes the logical links in the structure of security mechanisms. The use of data protection technologies and access to Wi-Fi has been investigated.

The fourth section of the thesis describes the process of installing and configuring an ACS secure access control server, as well as configuring a Wi-Fi hotspot for authentication through the described server.

Background includes the following tasks:

– technologies of standard 802.11, which are most suitable for the accomplishment of the tasks, have been identified;

– analysis of possible technologies of protection of Wi-Fi networks and their comparative capabilities;

– possibilities of authentication protocols and their characteristics are analyzed;

– modern capabilities of data encryption technologies in wireless networks are considered;

– appropriate software and Wi-Fi devices are configured.

Actuality of the theme. Wireless technology is becoming more and more indispensable in modern life every year. This is primarily due to the increasing demands for employee mobility, which directly affects the speed of decision-making on important issues for the company. Wireless LANs built on IEEE 802.11 standard have been used in the corporate and private areas for several years. The growing popularity shows that they have been able to solve a number of problems: for example, "mobile computing" with acceptable data rates has finally become possible on local networks, though still an order of magnitude smaller than the wired networks, but already high enough to meet a large proportion of mobile needs. However, with significant advantages, wireless data technologies have one main disadvantage: having an open data transmission environment. Accordingly, it is possible to intercept data transmitted over the network. An increase in the amount of information transmitted over wireless networks leads to an increase in the number of attacks on these networks. That is why it is extremely important to conduct a quality audit of computer networks and to protect information when transmitted over encrypted data channels.

The purpose of the research is to implement a comprehensive approach to provide a reliable mechanism for protecting information from unauthorized access on Wi-Fi networks (based on researched technologies and methods of protection).

Object of research – the process of securing information on a computer network based on Wi-Fi devices.

Subject of research – mechanisms and means for securing information on a computer network based on Wi-Fi devices.

The implementation of the results will provide the necessary protection of wireless networks in organizations and institutions using Wi-Fi technology.

ЗМІСТ

Додаток А. Тези конференції

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

AAA (Authentication, Authorization, Accounting) - Автентифікація, Авторизація, Аудит

ACS (Access Control Server) - сервер управління доступом

CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множинний доступ з контролем несучої та виявленням колізій) - технологія множинного доступу до загального передавального середовища в локальній комп'ютерній мережі, а також у бездротовій мережі з контролем колізій

EAP (Extensible Authentication Protocol) - розширений протокол автентифікації

IEEE (The Institute of Electrical and Electronics Engineers, Inc) - Інститут інженерів електротехніки та електроніки

Kerberos (з англ. Цербер) — протокол, орієнтований в основному на клієнт-серверну архітектуру, пропонує механізм взаємної автентифікації двох співрозмовників (хостів) перед встановленням зв'язку між ними в умовах незахищеного каналу

MAC-адреса (Media Access Control - управління доступом до носія) - це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж

MIMO (Multiple Input Multiple Output) - системи зв'язку з рознесеними передавальними і приймальними антенами

OFDM (Orthogonal Frequency-Division Multiplexing) - це метод мультиплексування (поєднання кількох потоків даних в один спільний простір), який підрозподіляє даний радіо спектр на набір ортогональних підчастот, через які передається інформація

RADIUS (Remote Authentication Dial-In User Service) - сервіс ідентифікації віддалених абонентів (протокол передачі даних що використовується в комп'ютерних мережах для автентифікації, авторизації та аудиту різноманітних сервісів)

SSID (Service Set Identifier) - ідентифікатор мережі

SSH (Secure SHell — «безпечна оболонка») - мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів)

TACASC (Terminal Access Controller Access Control System) - система керування доступом до контролера термінального доступу (відноситься до сімейства відповідних протоколів, що управляють віддаленою автентифікацією та пов'язаними послугами для управління мережевим доступом через централізований сервер)

Wi-Fi (Wireless-Fidelity) - бездротова точність, загальновживана назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалах

WEP (Wired Equivalent Privacy) – найстаріший стандарт захисту бездротового трафіку

WLAN (Wireless Local Area Network; WirelessLAN) - бездротова локальна комп’ютерна мережа

WPA (Wi-Fi Protected Access) - захищений доступ до бездротових мереж

АВТЕНТИФІКАЦІЯ - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора; частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації

АВТОРИЗАЦІЯ - процедура керування рівнями та засобами доступу до певного захищеного ресурсу та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних.

АУДИТ - системний процес одержання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки компанії чи системи у відповідності з визначеними критеріями та показниками безпеки

НСД (несанкціонований доступ, англ. unauthorized access) - одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових завдань

ВСТУП

Актуальність теми. Бездротові технології з кожним роком стають все більш незамінними в сучасному житті людини. В першу чергу це пов'язано зі зростаючими вимогами до мобільності співробітників, яка безпосередньо впливає на швидкість прийняття рішень з важливих для компанії питань. Бездротові локальні мережі, побудовані відповідно до стандарту IEEE 802.11, ось уже кілька років використовуються як в корпоративній, так і в приватній сферах. Зростаюча популярність свідчить, що з їх допомогою вдалося вирішити цілий ряд проблем: наприклад, в локальних мережах нарешті стали можливі «мобільні обчислення» з прийнятною швидкістю передачі даних, нехай все ще на порядок меншою в порівнянні з провідними мережами, але вже досить високою для задоволення великої частки мобільних потреб.

Проте, за наявності значних переваг, бездротові технології передачі даних мають один суттєвий недолік: наявність відкритого середовища передачі інформації. Відповідно, є можливість перехоплення даних, які передаються по мережі. Зростання обсягів інформації, яка передається по бездротових мережах, веде до зростання кількості атак на ці мережі. Саме тому надзичайно важливим є питання проведення якісного аудиту комп’ютерних мереж та захисту інформації при її передачі по кодованих каналах даних.

Зв’язок із науковими програмами, планами, темами. Дипломна робота виконана відповідно до наукової тематики Тернопільського національного технічного університету імені Івана Пулюя, кафедри кібербезпеки.

Мета роботи: реалізувати комплексний підхід для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі (на основі досліджених технологій та методів захисту).

Для досягнення вказаної мети, в роботі поставлено та розв’язано наступні задачі:

– визначено технології стандарту 802.11, що найбільше підходять для реалізації поставлених задач;

– проведено аналіз можливих технологій захисту Wi-Fi мереж та порівняно їх можливості;

– проаналізовано можливості протоколів автентифікації та їх характеристики;

– розглянуто сучасні можливості технологій шифрування даних в бездротових мережах;

– налаштовано відповідне програмне забезпечення та Wi-Fi пристрої.

Об’єкт дослідження: процес забезпечення захисту інформації в комп'ютерній мережі на базі Wi-Fi пристроїв.

Предмет дослідження: механізми і засоби для забезпечення захисту інформації комп'ютерній мережі на базі Wi-Fi пристроїв.

Методи дослідження. Метод теоретичного дослідження та експериментальний з використання персонального комп’ютера. Методика проведення аудиту захищеності безпровідної мережі розробляється з використанням теорії надійності, методів автентифікації, авторизації та аудиту. Методика дослідження базується на теоретичних і прикладних результатах, досягнутих у комп’ютерних науках та кібербезпеці.

Наукова новизна отриманих результатів:

– проведено аналіз та порівняння сервісів та служб аутентифікації;

– сформульовано систему критеріїв оцінки захищеності безпровідної мережі на основі реалізованих в ній механізмів;

– розроблено систему рівня довіри до безпровідної мережі;

– розроблено метод побудови профілів захисту для безпровідної мережі.

Практичне значення одержаних результатів. Впровадження результатів роботи дозволить забезпечити необхідний захист безпровідних мереж в організаціях та закладах, де використовується Wi-Fi технологія.

Апробація. Окремі результати дослідження доповідалися на VII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (11-12 грудня 2019р.).

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд архітектури комп'ютерної мережі стандарту EEE 802.11

Основне призначення WLAN - організація доступу до інформаційних ресурсів всередині будівлі. Друга за значимістю сфера застосування - це організація громадських комерційних точок доступу (hotspots) в людних місцях - готелях, аеропортах, кафе, а також організація тимчасових мереж на період проведення заходів (виставок, семінарів). Бездротові локальні мережі створюються на основі сімейства стандартів IEEE 802.11. Ці мережі відомі також як Wi-Fi, і хоча сам термін Wi-Fi, в стандартах явно не прописаний, бренд Wi-Fi отримав в світі найширшого розповсюдження. Стандарт IEEE 802.11 є базовим для всіх наступних специфікацій (802.11a, 802.11b, 802.11g, 802.11n). Комерційна назва цих мереж - Wi-Fi. Ця технологія використовується в таких областях, як бездротовий доступ в інтернет, безпровідне телебачення.

Різні стандарти сімейства Wi-Fi визначають фізичний рівень (PHY) і підрівень управління доступом до середовища MAC. Верхні рівні співпадають за своєю структурою як для бездротових, так і для провідних локальних мереж. Фізичний рівень визначає спосіб роботи з середовищем передачі, швидкість і методи модуляції. Підрівень MAC відповідає за розподіл каналу, тобто за те, яка станція буде передавати дані наступної станції локальної мережі. На MAC-рівні визначено принцип, за яким пристрої використовують загальний канал, механізм аутентифікації користувача, механізм шифрування даних. Стандарт 802.11 передбачає пакетну передачу з 48-бітовими адресами пакетів, як і будь-яка мережа Ethernet. Комітет IEEE 802 забезпечив сумісність усіх своїх стандартів. Бездротові мережі 802.11 легко сполучаються з провідними мережами Ethernet. Як і всі стандарти IEEE 802.11 працює на нижніх двох рівнях моделі ISO/OSI, фізично і канальному рівні (рис. 1.1). Будь-який мережевий додаток, мережева операційна система, або протокол, будуть так само добре працювати в мережі 802.11, як і в мережі Ethernet.

Рисунок 1.1 – Рівні моделі ISO / OSI і їх відповідність стандарту 802.11

Стандарт 802.11 визначає два типи обладнання - клієнт, яким зазвичай є комп'ютер, укомплектований бездротовою мережевою інтерфейсною картою (Network Interface Card), і точку доступу (Access point), яка виконує роль моста між бездротовими і дротовими мережами. Точка доступу зазвичай містить в собі приймач, інтерфейс провідної мережі, а також програмне забезпечення, що займається обробкою даних. В якості бездротової станції може виступати ISA, PCI або PC Card мережева карта в стандарті 802.11, або вбудовані рішення, наприклад, телефонна гарнітура 802.11. Стандарт IEEE 802.11 визначає два режими роботи мережі - режим "Adhoc" і клієнт-сервер. У режимі клієнт-сервер (рис. 1.2) бездротова мережа складається з як мінімум однієї точки доступу, підключеної до провідної мережі, і деякого набору бездротових кінцевих станцій. Так як більшості бездротових станцій потрібно отримувати доступ до файлових серверів, принтерів, інтернету, доступним в дротової локальної мережі, вони будуть працювати в режимі клієнт-сервер.

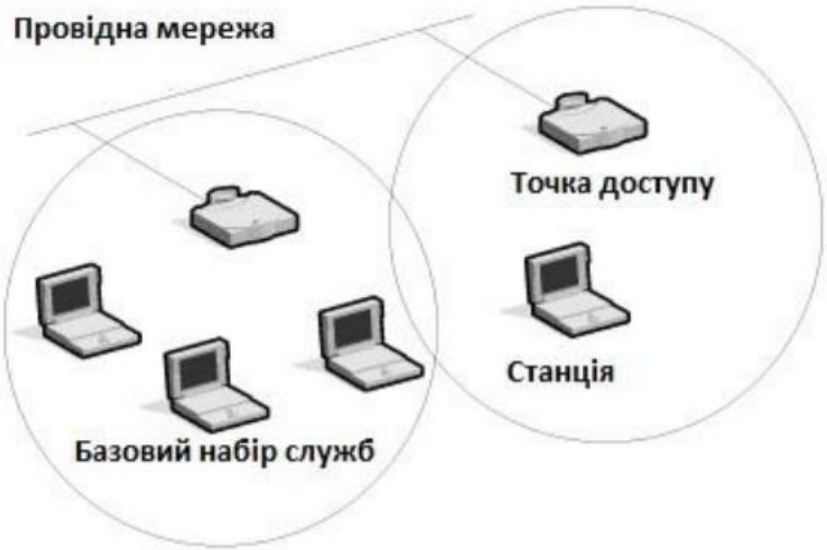

Рисунок 1.2 – Архітектура мережі “клієнт-сервер”

1.1.1 Фізичний рівень стандарту EEE 802.11

На фізичному рівні визначені два широкосмугових радіочастотних методи передачі і один - в інфрачервоному діапазоні. Радіочастотні методи працюють в ISM діапазоні 2,4 ГГц і зазвичай використовують смугу 83 МГц від 2,400 ГГц до 2,483 ГГц. Технології широкосмугового сигналу, що використовуються в радіочастотних методах, збільшують надійність, пропускну здатність, дозволяють багатьом непов'язаним один з одним пристроїв розділяти одну смугу частот з мінімальними перешкодами один для одного.

Стандарт 802.11 використовує метод прямої послідовності (Direct Sequence Spread Spectrum) і метод частотних стрибків (Frequency Hopping Spread Spectrum). Ці методи кардинально відрізняються, і несумісні один з одним. Для модуляції сигналу FHSS використовує технологію Frequency Shift Keying. При роботі на швидкості 1 Mbps використовується FSK модуляція по Гауса другого рівня, а при роботі на швидкості 2 Mbps - четвертого рівня. Метод DSSS використовує технологію модуляції Phase Shift Keying. При цьому на швидкості 1 Mbps використовується диференціальна двійкова PSK, а на швидкості 2 Mbps - диференціальна квадратична PSK модуляція. Заголовки фізичного рівня завжди передаються на швидкості 1 Mbps, в той час як дані можуть передаватися зі швидкостями 1 і 2 Mbps

1.1.2 Основні стандарти IEEE 802.11

Історія стандарту IEEE 802.11 почалася в 1997 році, коли була прийнята початкова специфікація побудови локальних мереж на основі бездротових технологій. Вона передбачала організацію обміну даними за допомогою інфрачервоного випромінювання і радіохвиль. Зараз IEEE 802.11 являє собою сімейство специфікацій, які всебічно описують принципи і параметри функціонування бездротових мереж. В даний час широко використовується переважно три стандарти групи IEEE 802.11 (представлені в таблиці 1.1). Стандарт IEEE 802.11g, прийнятий в 2003 році, є логічним розвитком стандарту 802.11b і передбачає передачу даних в тому ж частотному діапазоні, але з більш високими швидкостями. Крім того, стандарт 802.11g повністю сумісний з 802.11b. Максимальна швидкість передачі даних в стандарті 802.11g становить 54 Мбіт/с. При розробці стандарту 802.11g розглядалися дві конкуруючі технології: метод ортогонального частотного поділу OFDM, запозичений зі стандарту 802.11a і запропонований до розгляду компанією Intersil, і метод двійкового пакетного згорткового кодування PBCC,

Таблиця 1.1 – Основні характеристики стандартів групи IEEE 802.11

Стандарт	802.11g	802.11a	802.11n
Частотний діапазон, ГГц	2,4 – 2,483	5,15-5,25	2,4 або 5,0
Метод передачі	DSSS, OFDM	DSSS, OFDM	MIMO
Швидкість, Мбіт/с	1-54	6-54	6-300
Сумісність	802.11 b/n	802.11n	802.11 a/b/g
Метод модуляції	BPSK,QPSK,OFDM	BPSK,QPSK,OFDM	BPSK, 64-QAM
Дальність зв'язку в приміщенні	20-50	10-20	50-100
Дальність зв'язку на відкритому просторі	250	150	500

В результаті стандарт 802.11g містить компромісне рішення: в якості

базових застосовуються технології OFDM і CCK, а опціонально передбачено використання технології PBCC. Опціонально в протоколі 802.11g технологія PBCC може використовуватися при швидкостях передачі 22 і 33 Мбіт / с. Технологія PBCC є опціональною в стандарті IEEE 802.11g, а технологія OFDM - обов'язковою. Для того щоб зрозуміти суть технології OFDM, розглянемо більш докладно багатопроменеву інтерференцію, що виникає при поширенні сигналів у відкритому середовищі. Ефект багатопроменевої інтерференції сигналів полягає в тому, що в результаті багаторазових відображень від природних перешкод один і той же сигнал може потрапляти в приймач різними шляхами. Різні шляхи поширення відрізняються один від одного по довжині, тому послаблення сигналу буде для них неоднаковим. Отже, в точці прийому результуючий сигнал являє собою інтерференцію багатьох сигналів, що мають різні амплітуди і зміщених одна відносно одної за часом, що еквівалентно додаванню сигналів з різними фазами. Наслідком багатопроменевої інтерференції є спотворення сигналу. Багатопроменева інтерференція властива будь-якому типу сигналів, але особливо негативно вона позначається на широкосмугових сигналах, оскільки при використанні широкосмугового сигналу в результаті інтерференції певні частоти складаються синфазно, що призводить до збільшення сигналу, а деякі, навпаки, противофазно, викликаючи ослаблення сигналу на даній частоті. Найбільш негативно на спотворення сигналу впливає саме міжсимвольного інтерференція. Оскільки символ - це дискретне стан сигналу, що характеризується значеннями частоти несучої, амплітуди і фази, для різних символів змінюються амплітуда і фаза сигналу, а отже, відновити вихідний сигнал вкрай складно.

З цієї причини при високих швидкостях передачі застосовується метод кодування даних OFDM. Суть його полягає в тому, що потік переданих даних розподіляється по безліч частотних підканалов і передача ведеться паралельно на всіх таких підканалах. При цьому висока швидкість передачі досягається саме за рахунок одночасної передачі даних по всіх каналах, тоді як швидкість передачі в окремому підканалі може бути і невисокою. Стандарт IEEE 802.11a передбачає швидкість передачі даних до 54 Мбіт / с. На відміну від базового

стандарту специфікаціями 802.11a передбачена робота в новому частотному діапазоні 5ГГц. В якості методу модуляції сигналу вибрано ортогонально частотне мультиплексування OFDM, що забезпечує високу стійкість зв'язку в умовах багатопроменевого поширення сигналу. Частотний діапазон UNII розбитий на три 100-мегагерцеві піддіапазони, що розрізняються обмеженнями по максимальній потужності випромінювання.

Нижчий діапазон (від 5,15 до 5,25 ГГц) передбачає потужність всього 50 мВт, середній (від 5,25 до 5,35 ГГц) - 250 мВт, а верхній (від 5,725 до 5,825 ГГц) - 1 Вт. Використання трьох частотних піддіапазонів із загальною шириною 300 МГц робить стандарт IEEE 802.11a найбільш широкосмуговим з сімейства стандартів 802.11 і дозволяє розбити весь частотний діапазон на 12 каналів, кожен з яких має ширину 20 МГц, причому вісім з них лежать в 200-мегагерцовому діапазоні від 5 , 15 до 5,35 ГГц, а решта чотири канали - в 100-мегагерцовому діапазоні від 5,725 до 5,825 ГГц (рис. 1.3). При цьому чотири верхніх частотних каналу, що передбачають найбільшу потужність передачі, використовуються переважно для передачі сигналів поза приміщеннями.

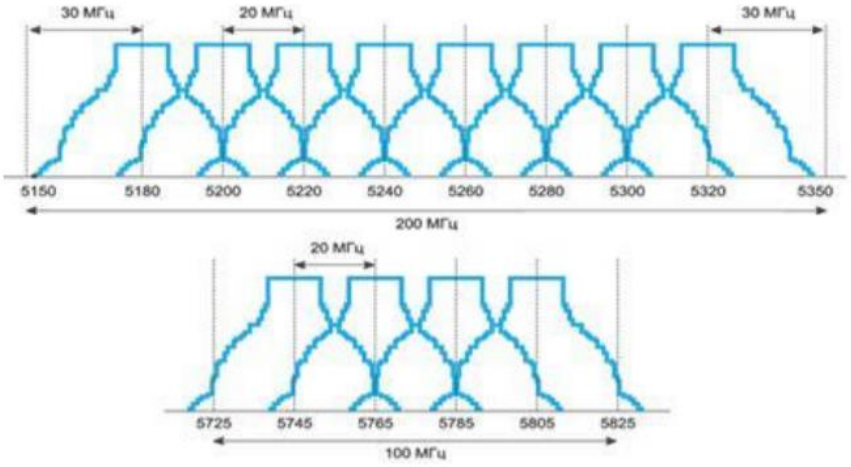

Рисунок 1.3 – Поділ діапазону UNII на 12 частотних діапазонів

Послідовність обробки вхідних даних в стандарті IEEE 802.11a виглядає наступним чином. Спочатку вхідний потік даних піддається стандартної операції скремблювання. Після цього потік даних надходить на кодер. Швидкість кодування може становити 1/2, 2/3 або 3/4. Оскільки швидкість кодування може

бути різною, то при використанні одного і того ж типу модуляції швидкість передачі даних виявляється різною. Розглянемо, наприклад, модуляцію BPSK, при якій швидкість передачі даних становить 6 або 9 Мбіт/с. Тривалість одного символу дорівнює 4 млс, а значить, частота проходження імпульсів складе 250 кГц. З огляду на те, що в кожному підканалі кодується по одному біту, а всього таких підканалів 48, отримуємо, що загальна швидкість передачі даних складе 250 кГц х 48 каналів = 12 МГц. При швидкості кодування 3/4 на кожні три інформаційних біта додається один службовий, тому в даному випадку корисна (інформаційна) швидкість становить 3/4 від повної швидкості, тобто 9 Мбіт/с.

Потім слідує другий етап перестановки бітів, мета якого полягає в тому, щоб сусідні біти не опинилися одночасно в молодших розрядах груп, що визначають модуляційний символ. Тобто після другого етапу перестановки сусідні біти виявляються поперемінно в старших і молодших розрядах груп. Робиться це з метою покращення завадостійкості сигналу, що передається. Стандарт IEEE 802.11n по швидкості передачі можна порівняти з провідними стандартами. Максимальна швидкість передачі стандарту 802.11n приблизно в 5 разів перевищує продуктивність класичного Wi-Fi. Можна відзначити наступні основні переваги стандарту 802.11n: велика швидкість передачі даних; відсутність непокритих ділянок; сумісність з попередніми версіями.

Стандарт IEEE 802.11n заснований на технології OFDM-MIMO. Дуже багато реалізованих в ньому технічних деталей запозичено зі стандарту 802.11a, проте в стандарті IEEE 802.11n передбачається використання як частотного діапазону, прийнятого для стандарту IEEE 802.11a, так і частотного діапазону, прийнятого для стандартів IEEE 802.11b / g. Принцип реалізації технології MIMO зображено на рисунку 1.4.

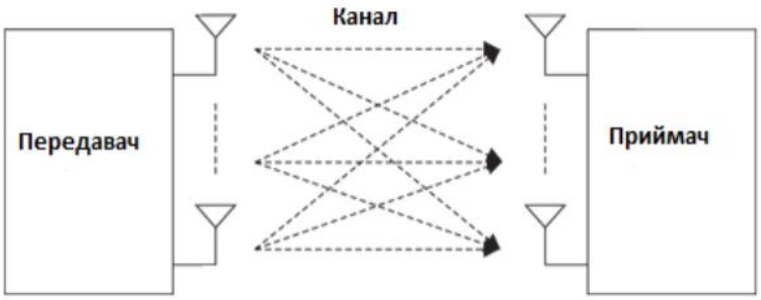

Рисунок 1.4 – Принцип реалізації технології MIMO

1.2 Огляд топології WLAN

Мережі стандарту 802.11 можна конструювати по-різному. Розробник може вибрати сам одну з наступних топологій: незалежні базові зони обслуговування; базові зони обслуговування; розширені зони обслуговування.

Зони обслуговування в даному випадку це логічно згруповані об’єкти. Технологія WLAN забезпечує доступ до мережі шляхом передачі широкомовних сигналів через ефір на несучій в діапазоні радіочастот. Приймаюча станція може отримувати сигнали в діапазоні роботи декількох передаючих станцій. Передаюча станція спочатку передає ідентифікатор зони обслуговування SSID. Станція-приймач використовує SSID для фільтрації отримуваних сигналів, та виділення того яких їй потрібен.

Незалежні базові зони обслуговування(IBSS). IBSS являють собою групу працюючих у відповідності до стандарту 802.11 станцій, що зв’язані безпосередньо одна з іншою. IBSS також називають спеціальною, або безплановою мережею, тому що вона являє собою просту однорангову мережу як показано на рис. 1.5.

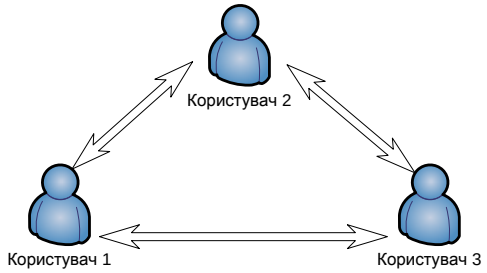

Рисунок 1.5 – Приклад незалежної зони обслуговування

Спеціальна мережа, або IBSS виникає, коли окремі пристрої клієнти формують самопідтримуючу мережу, без використання окремою точки доступу. При створенні таких мереж не розроблюються карти місцевості тому що зазвичай такі мережі невеликі та мають обмежену протяжність. На відміну від варіанту використання розширеної зони обслуговування (ESS), клієнти безпосередньо встановлюють з'єднання один з одним, в результаті чого створюється тільки одна базова зона обслуговування (BSS), що не має відповідного інтерфейсу для підключення до дротової кабельної мережі (тобто відсутня будь-яка розподільча система, яка необхідна для об'єднання BSS та створення таким чином ESS). Не існує будь-яких обумовлених стандартом обмежень на кількість пристроїв, котрі можуть належати одній незалежній базовій зоні обслуговування.

Оскільки в IBSS відсутня точка доступу, розподіл часу виконується не централізовано. Клієнт, що починає передачу в IBSS, задає сигнальний інтервал для створення набору моментів часу передачі маякового сигналу. Коли закінчується час передачі маякового сигналу, кожен клієнт IBSS виконує наступне: призупиняються всі таймери затримки з часу передачі попереднього маякового сигналу; визначається значення нової випадкової затримки; якщо жоден маяковий сигнал не поступає до закінчення випадкової затримки, відправляється маяковий сигнал та відновлюється робота таймеру затримки.

Як ми бачимо, розподіл часу для передачі маякових сигналів виконується в спеціальних мережах не точкою доступу, та не одним з клієнтів. Оскільки в такій схемі зв'язку існує проблема прихованого вузла , можливо, що на протязі сигнального інтервалу буде передано велику кількість маякових сигналів від різних клієнтів. Але стандарт допускає таку ситуацію і ніяких проблем не виникає, оскільки клієнти чекають прийому тільки першого маякового сигналу, що відноситься до їх власного таймеру випадкової затримки. В маякові сигнали вбудована функція синхронізації таймеру. Кожен клієнт порівнює порівнює значення функції в маяковому сигналі з своїм власним таймером, і якщо отримане значення більше, вважається, що годинник передаючої станції йде швидше і підстроюється свій власний таймер в відповідності з отриманим

значенням. Це має довгочасний ефект синхронізації роботи всієї неплановоі мережі по клієнту з самим швидким таймером. В значних розподілених неплановых мережах, коли клієнти не можуть спілкуватися напряму, може знадобитися певних час для синхронізації всіх клієнтів.

Базові зони обслуговування (BSS). BSS – це група працюючих по стандарту 802.11 станцій, що зв'язуються одна з одною. Технологія BSS передбачає наявність особливої станції, яка називається точкою доступу, як показано на рис.1.6. Точка доступу – це центральний пункт зв'язку всіх станцій. Клієнтські станції не зв'язуються безпосередньо одна з одною, замість цього вони зв'язуються з точкою доступу, а вона переправляє фрейми станції-адресату. Точка доступу може мати порт вхідного каналу, через який BSS підключається до дротової мережі.

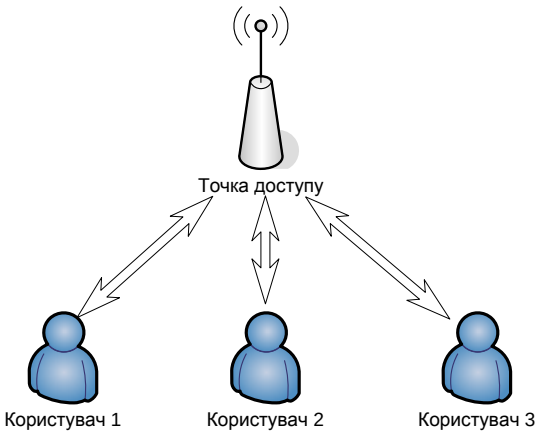

Рисунок 1.6 – Приклад типової інфраструктури BSS

Розширені зони обслуговування. Декілька інфраструктур BSS можуть бути з'єднані через їх інтерфейси вихідного каналу. Там де діє стандарт 802.11, інтерфейс вихідного каналу з'єднує BSS з розподільною системою. Декілька BSS, що з'єднані між собою через розподільчу систему, являють собою розширену зону обслуговування (ESS), яка показана на рис.1.7. Вихідний канал до розподільчої системи не обов'язково повинен використовувати дротове з'єднання. Специфікація стандарту 802.11 залишає можливість реалізації цього каналу в вигляді бездротового, хоча частіше використовується дротовий вид зв'язку.

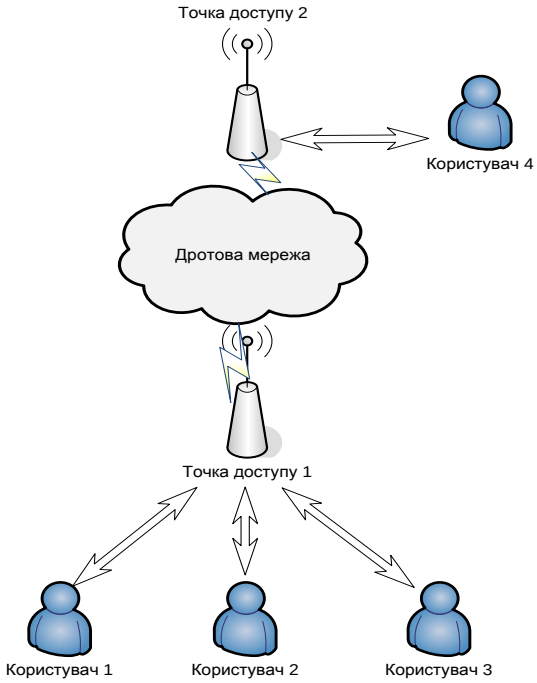

Рисунок 1.7 – Приклад типової інфраструктури ESS

1.3 Механізм доступу до середовища стандарту 802.11

Технологія CSMA/CA базується на використанні декількох правил:

- перед тим як учасник почне передавати дані, він повинен сповістити, скільки саме часу йому потрібно на передачу даних. Це повідомлення дає можливість іншим учасникам дізнатися час коли передавати дані буде неможливо;

- учасники не можуть передавати дані до тих пір, доки не закінчиться час зарезервований попереднім учасником передачі даних;

- учасники не знають чи були отримані їх дані, під час передачі, доки вони не отримають підтвердження про закінчення передачі.

- якщо два учасники почали передавати дані одночасно, то вони дізнаються про це лише тоді коли не отримають підтвердження про те що їх дані були отримані;

- учасники чекають деякий невизначений (випадковий) час і знову намагаються передавати, якщо не отримають підтвердження про отримання.

Як ми бачимо технологія CSMA/CA має дещо суворіші правила ніж CSMA/CD, який використовується у дротових видах зв’язку, ці правила

дозволяють уникати колізій. Уникнення колізій є ключовим моментом для бездротових мереж, оскільки останні не мають спеціального механізму для їх виявлення. При використанні технології CSMA/CA колізія виявляється тільки у випадку неотримання підтвердження від станції що отримувала дані.

Реалізація технології CSMA/CA стандартом 802.11 виконується за допомогою розподіленої функції координації.

Перед тим як описувати роботу CSMA/CA, спочатку опишемо найважливіші для CSMA/CA компоненти: контроль несучої; розподілена функція координації; фрейми підтвердження; резервування середовища за допомогою механізму «готовність до передачі \ готовність до прийому(RTS\CTS)».

Крім цього два інших механізми характерні для доступу до середовища по стандарту 802.11, але не зв'язані на пряму з технологією CSMA/CA: фрагментація фреймів; точкова функція координації.

Станція, що має намір передати інформацію в дротовому середовищі, повинна спочатку перевірити чи використовується несуча. Якщо це є так, то станція повинна відкласти передачу даних, доки середовище не стане вільним.

Станція дізнається про стан середовища за допомогою двох методів:

- перевірка фізичного рівня на предмет наявності несучої;

- використання віртуальної функції контролю несучої, вектору розподілення мережі.

Станція може перевірити фізичний рівень та впевнитися в тому, що несуча вільна. Але в деяких випадках середовище все ще може бути зайнятим іншою станцією через вектор розподілу мережі. Це таймер, значення якого оновлюється даними фреймів, що передаються через середовище. Наприклад, припустимо, що в інфраструктурі BSS користувач_1 передає фрейм користувачу_2, Рис.1.8. Оскільки бездротове середовище – це середовище що використовуються спільно з широкомовленням, отже користувач_3 також отримає цей фрейм. Фрейми стандарту 802.11 мають поле тривалості. Значення тривалості достатньо велике для того щоб виконати передачу фрейму і отримати підтвердження його прийому. Користувач_3 оновлює свій вектор розподілу мережі значенням поля

тривалості і не намагається почати передачу, доки вектор розподілу не зменшиться до нуля.

Потрібно звернути увагу на те що ця станція оновлює значення вектору розподілення мережі тільки тоді, коли отримане значення поля тривалості перевищую те, що зберігається в її векторі розподілу мережі. Так, у випадку, якщо значення вектору розподілу мережі станції користувача_3 складає 10 мс, вона не буде оновлювати свій вектор розподілу мережі, якщо отримає фрейм з значенням зі значенням поля тривалості 5 мс. Вона оновить свій вектор розподілу мережі, якщо отримає фрейм зі значенням поля тривалості 20 мс.

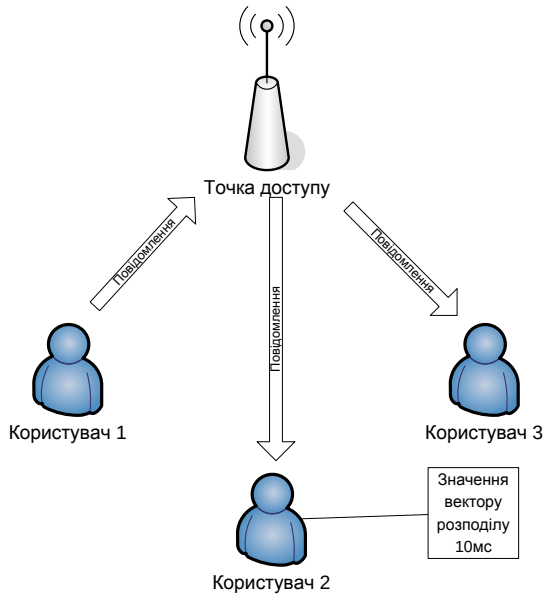

Рисунок 1.8 – Процес оновлення вектору розподілу мережі

Фрейм підтвердження. Станція, що отримала фрейм, підтверджує факт його безпомилкового приймання станції що передавала фрейму підтвердження. Дізнавшись, що станція-приймач повинна отримати доступ до середовища та передати фрейм підтвердження, можна було б припустити, що передача фрейму підтвердження може затриматися внаслідок конкуренції станцій за середовище. Проте передача фрейму підтвердження – це особливий випадок. Фреймам підтвердження дозволяється не приймати участь в процесі випадкової затримки. Короткий проміжок часу, який станція що приймає проводить в чеканні такої нагоди, називається короткий між фреймовий зазор (SIFS).

Інтервал SIFS коротший за DIFS на два канальних інтервали. Це гарантує приймаючій станції найбільший шанс доступу до середовища передачі в порівнянні з іншими станціями.

Повертаючись до випадку передачі інформацій від Користувача_1 до Користувача_2 відмітимо, що станція першою відклала спробу передачі на чотири канальні інтервали. Середовище стало доступним, тому з'явилася можливість передати свій фрейм Користувачу_2. Точка доступу отримує фрейм та чекає на протязі часу, що дорівнює інтервалу SIFS, перед передачею фрейму підтвердження (див. рис.1.9).

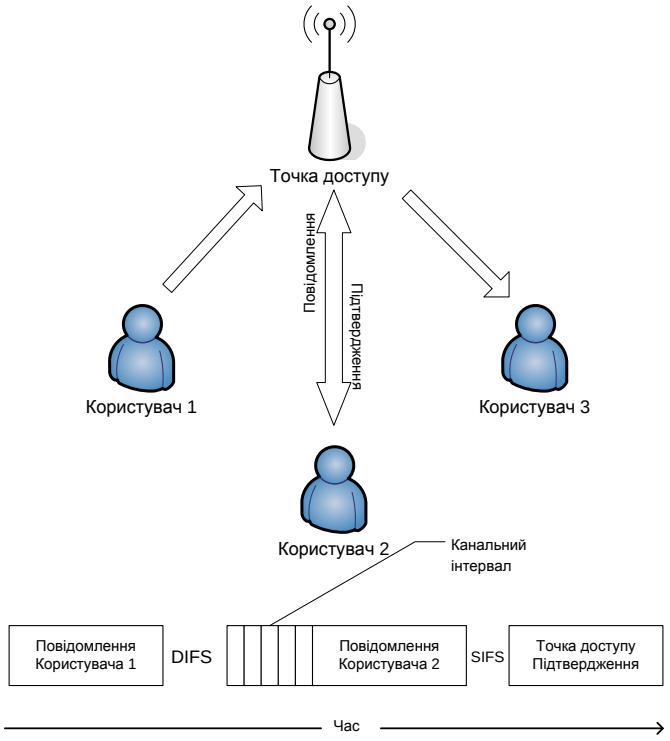

Рисунок 1.9 – Передача фрейму підтвердження.

Припустимо, що станція першого користувача фрейм підтвердження не отримала. Тоді вона подвоює ширину вікна конкуренції до 15 та повторює процес затримки. При кожній невдалій спробі доступу до середовища станція, що працює по стандарту 802.11, збільшує значення лічильники числа спроб.

Ширина вікна конкуренції кожного разу подвоюється, доки не досягає максимального значення. MAC рівень може продовжувати спроби передачі фрейму, але коли значення лічильника досягне максимального порогу, станція

користувача буде намагатися зарезервувати середовище.

Проблема прихованого вузла RTS/CTS. Перший користувач може бути не в змозі отримати доступ до середовища через іншу станцію, що знаходиться в зоні досяжності точки доступу, але за межами досяжності станції першого користувача. Ця ситуація показана на рис.1.10. Станції першого та другого користувача знаходяться в зоні дії одно одної та точки доступу. При цьому жодна з них не знаходиться в дії станції третього користувача. Проте станція третього користувача знаходиться в зоні дії точки доступу і також намагається виконати передачу даних. Ця ситуація відома як проблема прихованого вузла, оскільки станція третього користувача не видна для першого та другого користувача.

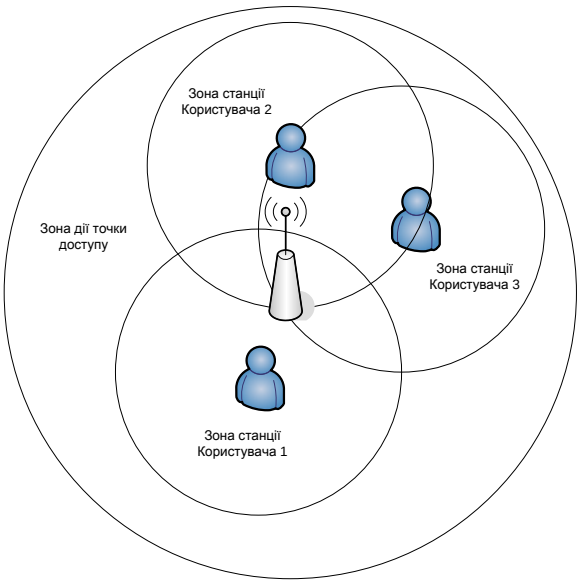

Рисунок 1.10 – Проблема прихованого вузла

Перший користувач намагається зарезервувати середовище за допомогою спеціального управляючого фрейму, що називається фрейм RTS(фрейм готовності до передачі). Фрейм RTS відправляється точці доступу, і всі станції, що знаходяться в зоні дії станції першого користувача, чекають на протязі часу, вказаного в полі тривалості. Обмін фреймами включає той фрейм, котрий станція першого користувача намагалась передати, а також фрейм підтвердження.

Фрагментація фрейму згідно стандарту 802.11– це функція, що

виконується на MAC рівні, призначення якої – збільшити надійність передачі фреймів через бездротове середовище. Під фрагментацією розуміють розбивання фрейму на менші фрагменти, та передача кожного з них окремо. Передбачається, що ймовірність вдалої передачі фрагменту малого розміру, через зашумлену бездротову мережу більша. Отримання кожного фрагменту підтверджується окремо, відповідно, якщо будь-який фрагмент фрейму буде передано з помилкою або вступить в колізію, лише його потрібно буде передавати повторно, а не весь фрейм. Це збільшує пропускну здатність середовища.

Фрагментації піддаються тільки одноадресні фрейми, фрейми широкомовлення, або багато адресні фрейми передаються цілком. Крім того, фрагменти фрейму передаються пакетом, з використанням тільки однієї ітерації механізму доступу до середовища DSF.

Хоча за рахунок фрагментації можна збільшити надійність передачі фреймів в бездротових локальних мережах, вона призводить до збільшення витрат MAC протоколу стандарту 802.11. Кожен фрагмент фрейму включає інформацію, що міститься в заголовку MAC 802.11, а також потребує передачі відповідного фрейму підтвердження. Це збільшує число службових сигналів MAC-протоколу, та знижує реальну продуктивність бездротових станцій.

Формати фреймів MAC стандарту 802.11. На рівні MAC стандарту 802.11 використовуються фрейми трьох категорій:

- управляючі фрейми. Сприяють передачі фреймів даних при нормальному обміні інформацією між станціями стандарту 802.11;

- службові фрейми. Забезпечують з’єднання бездротових локальних мереж;

- фрейми даних. Переносять дані станцій від передавача до приймача.

Всі фрейми стандарту 802.11 схожі на основний фрейм цього стандарту. Вищеназвані три типи фреймів розширюють та використовують специфічні ділянки основного фрейму MAC для своїх цілей. На рис.1.11 представлений основний фрейм MAC та його поля.

Контроль фрейму	Тривалість	Адреса 1	Адреса2	Адреса 3	Керування чергою	Адреса4	Тіло фрейму	FCS
2 байти	2 байти	6 байт	6 байт	6 байт	2 байти	6 байт	0-2312 байт	4 байти

Рисунок 1.11 – Основний фрейм MAC стандарту 802.11

Поле контролю фрейму**.** Розмір якого дорівнює двом байтам, складається з одинадцяти підполів. Підполя поля контролю фрейму:

- Версія протоколу. Вказує версію протоколу MAC 802.11. На сьогоднішній день існує тільки одна версія протоколу, тому це значення «0», всі інші значення зарезервовані.

- Тип. Вказує тип фрейму MAC : управляючий, службовий та фрейм даних, четверте значення зарезервовано.

- Підтип. Вказує на підтип фрейму: запит на зєднання, відповідь на запит на зєднання, зондуючий запит, розєднання, аутентифікації, підтвердження та зарезервовані значення.

- До розподільної системи. Вказує, чи призначений даний фрейм для розподільної системи.

- Від розподільної системи. Вказує, чи отриманий фрейм від розподільної системи.

- Більше фрагментів. Вказує, чи є даний фрейм тільки службовим чи тільки фреймом даний, чи потрібно чекати інших фрагментів.

- Повторна передача. Вказує, чи передається даний фрейм повторно.

- Управління джерелом. Вказує на режим енергоспоживання, значення «1» - станція працює в режимі економії енергозбереження, «0» - в звичайному режимі.

- Більше даних. Якщо біт встановлено, приймаюча станція сповіщається про те, що маються дані призначені для неї, буферизовані в точці доступу.

- Захищеність. Вказує, чи використовується шифрування фреймів WEP.

- Параметр впорядкування. Значення поля «1» у випадку використання служби жорстого впорядкування, в всіх інших випадках значення буде «0».

Тривалість/ID. Вказує в мікросекундах тривалість обміну фреймами,

значення може приймати в діапазоні від «0» до «32767».

Управління порядком**.** В цьому полі міститься порядковий номер та номер порядку фрейму.

FCS. Це контрольна сума фрейму. В даному полі міститься 32-значення циклічного надлишкового контролю, що вираховується для всіх полів заголовку та тіла фрейму.

Управляючі фрейми. В специфікації стандарту 802.11 описано шість унікальних управляючих фреймів:

- PS-Poll – вказує точці доступу на те, що бездротова станція, що працює в режимі енергозбереження, потребує щоб їй були доставлені, буферизовані фрейми;
- RTS – це запит на резервування середовища, він являється частиною механізму доступу стандарту 802.11; Даний фрейм включає в себе: час, який є необхідним для обміну фреймами, та MAC-адреси відправника та отримувача;
- CTS – це відповідь на фрейм RTS, це відповідь станції-приймача що середовище було зарезервоване на певний час, крім часу включає ще MAC-адресу станції приймача;
- ACK – підтверджує передачу фрейму, отримувач фрейму відсилає фрейм ACK відправнику, щоб підтвердити успішний прийом даних;
- CF-End – вказує на кінець періоду вільного від конкуренції;

Службові фрейми. Службові фрейми стандарту 802.11 мають поля, що відрізняються від описаного вище початкового фрейму MAC, та використовуються структури даних, що називаються інформаційні елементи та фіксовані поля. Службові фрейми стандарту 802.11 побудовані з використанням відповідних полів формату основного фрейму MAC, з додаванням підходящих інформаційних елементів і фіксованих полів.

Інформаційні елементи, що передбачені стандартом 802.11:

- SSID – має розмір до 32 біт, якщо розмір рівний нулю то SSID є широкомовний;
- швидкості передачі, що підтримуються – швидкість передачі в шістнадцятковому вигляді;

- набір параметрів стрибкоподібного перемикання частоти – час перемикання, набір схем скачків, схема скачків, індекс каналу;

- набір параметрів розподільної системи – вказує канал, що використовує бездротова станція.

- елемент набору параметрів IBSS – поле вказує ширину вікна в тактах;

- елемент тексту, що змінюється – вказує текст для використання у фреймах аутентифікації.

Фрейми даних стандарту 802.11. Стандартом передбачено 8 унікальних фреймів даних, структура типового фрейму даних представлена на рис.1.12: дані; нульові дані; дані+CF-ACK; дані+CF-Poll; дані+CF-ACK+ CF-Poll; CF-ACK; CF-Poll; CF-ACK+ CF-Poll.

Контроль фрейму	Тривалість	Адреса призначення	BSSID	Адреса джерела	Керування чергою	Корисне навантаження	FCS
2 байт	2 байт	6 байт	6 байт	6 байт	2 байт	0-2312байт	4 байт

Рисунок 1.12 – Формат фрейму даних

Фрейм нульових даних називається тому, що він не має поля «корисного навантаження», його мета – вказати на зміну біту режиму енергозбереження в контрольному полі фрейму.

1.4 Висновки до розділу

У першому розділі дипломної роботи виконано огляд архітектури комп’ютерної мережі стандарту EEE 802.11 та топологій бездротових мереж. Проаналізовано основні елементи процесу доступу до середовища стандарту.

2 ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ У WI-FI МЕРЕЖІ

2.1 Огляд алгоритмів аутентифікації в безпровідних мережах

На сьогоднішній день для забезпечення безпеки будь-якої мережі, як провідної, так і безпровідної, необхідно забезпечити рішення трьох основних проблем: конфіденційність (дані повинні бути надійно зашифровані); цілісність (дані гарантовано не повинні бути змінені третіми особами); автентичність (надійна перевірка того, що дані отримані від правильного джерела).

Безпровідні мережі потребують реалізації додаткових механізмів для аутентифікації абонентів з ціллю запобігання НСД до мережевих ресурсів та забезпечення конфіденційності даних з ціллю забезпечення цілісності і захисту при передачі по загальнодоступним каналам.

Стандарт IEEE 802.11 передбачає такі механізми аутентифікації безпровідних абонентів: відкриту аутентифікацію; аутентифікацію з загальним ключем; аутентифікацію за MAC-адресою; WPA; WPA2, 802.11i.

Процес аутентифікації абонента безпровідної мережі складається з наступних етапів:

1. Абонент відправляє пакет запиту стану (probe request) на всі радіоканали.

2. Кожна точка доступу, в зоні видимості якої знаходиться абонент, відправляє у відповідь пакет стану(probe response).

3. Абонент вибирає зручну для нього точку доступу і відправляє в обслуговуючий нею радіоканал запит на утентифікацію (authentication request).

4. Відправляється підтвердження точкою доступу (authentication reply).

5. У випадку успішної аутентифікації абонент відправляє пакет з запитом асоціювання (association request).

6. Точка доступу відправляє пакет асоціювання (association response).

7. Абонент може тепер здійснювати обмін користувацьким трафіком з точкою доступу і провідною мережею.

Процес аутентифікації абонента зображений на рисунку 2.1.

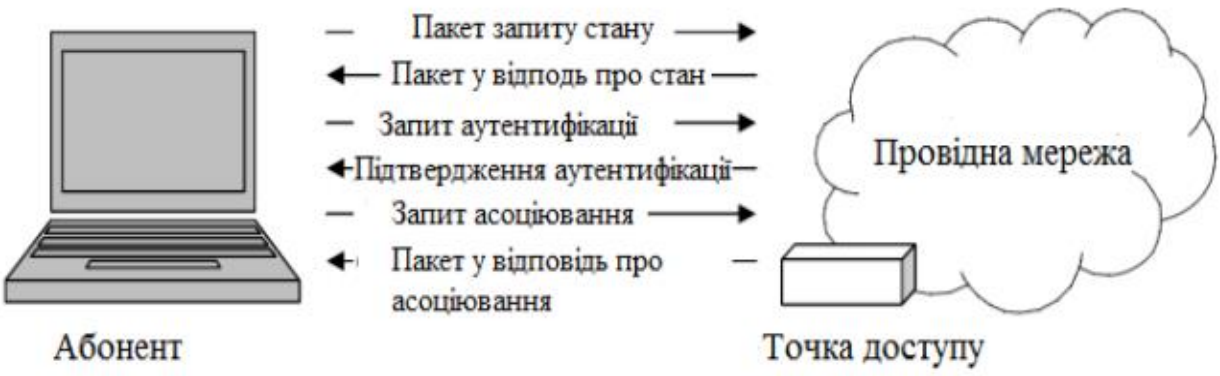

Рисунок 2.1 – Процес аутентифікації абонента в безпровідну мережу

При активізації в безпровідну мережу абонент починає пошук точок доступу в своїй зоні радіовидимості за допомогою керуючих пакетів запиту стану. Фрейми probe request надсилаються в кожен з радіоканалів, підтримуваних абонентським радіоінтерфейсом, в спробі знайти всі точки доступу з необхідними клієнтові ідентифікатором SSID (service set identifier) і підтримуваними швидкостями радіообміну. Кожна точка доступу, яка знаходяться в зоні радіовидимості абонента і задовільніє запитуваною в пакеті probe request параметрам, відповідає пакетом probe response, що містить синхронізує інформацію і дані про поточне завантаження активної радіостанції. абонент визначає, з якою точкою доступу він буде працювати. Після того як краща активна радіостанція визначена, абонент переходить в фазу аутентифікації. Відкрита аутентифікація по суті не є алгоритмом аутентифікації в звичному розумінні. На перший погляд, використання цього алгоритму може здатися безглуздим, однак слід враховувати, що розроблені методи аутентифікації IEEE 802.11 орієнтовані на швидке та логічне підключення до Wi-Fi мережі. При відкритій аутентифікації здійснюється обмін запитом аутентифікації та підтвердженням аутентифікації.

При відкритій аутентифікації можливий доступ будь-якого абонента до мережі Wi-Fi. Коли в wi-fi мережі відсутнє шифрування, тоді який-небудь абонент, котрому відомий ідентифікатор SSID AP, може мати доступ до мережі.

Якщо точки доступу використовують шифрування WEP, тоді ці ключі шифрування виступають засобом контролю доступу. Коли абонент не має правильного WEP-ключа, навіть у разі вдалої аутентифікації він не зможе ані передавати дані через точку доступу, ані виконати їх розшифрування (рис. 2.2).

Рисунок 2.2 – Процес відкритої аутентифікації

Один з методів аутентифікації в Wi-Fi мережі – аутентифікація з відкритим ключем доступу. Аутентифікація з загальним ключем вимагає налаштування у абонента статичного ключа шифрування WEP. Процес аутентифікації з використанням загального ключа зображений на рисунку 2.3.

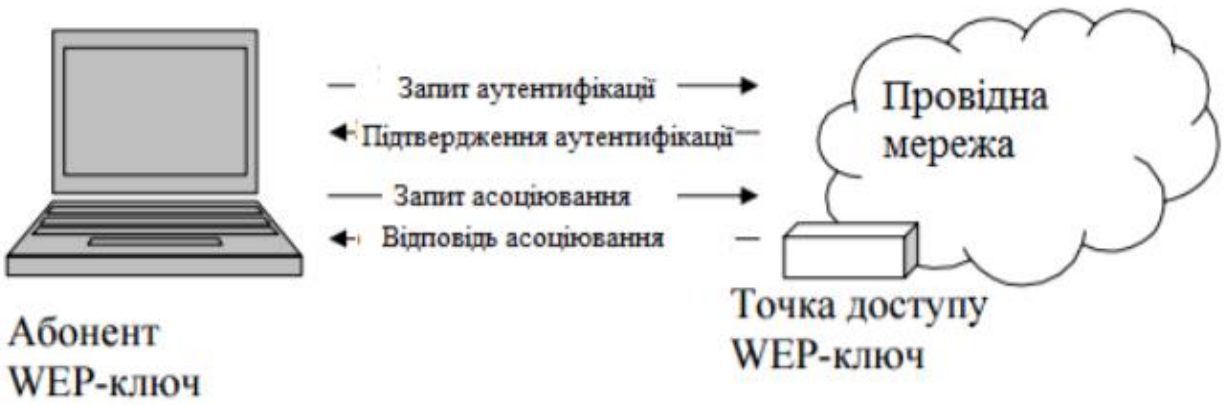

Рисунок 2.3 – Процес аутентифікації з загальним ключем

Початкові варіанти модифікації WPA були, фактично, вдосконаленим WEP. Візьмемо, для прикладу, WPA-TKIP. Тут використовується 48-бітний вектор ініціалізації, і змінені правила побудови вектора. Використовується MIC для підрахунку контрольної суми, замість застарілого і ненадійного CRC32. Основний момент – довжина ключа шифрування замість 40 біт становить 128. WPA2 забезпечує найвищий рівень захисту даних і контроль доступу до бездротової мережі для корпоративних (WPA2-Enterprise) і індивідуальних користувачів (WPA2-Personal). Механізм роботи WPA2 наведено на рисунку 2.5.

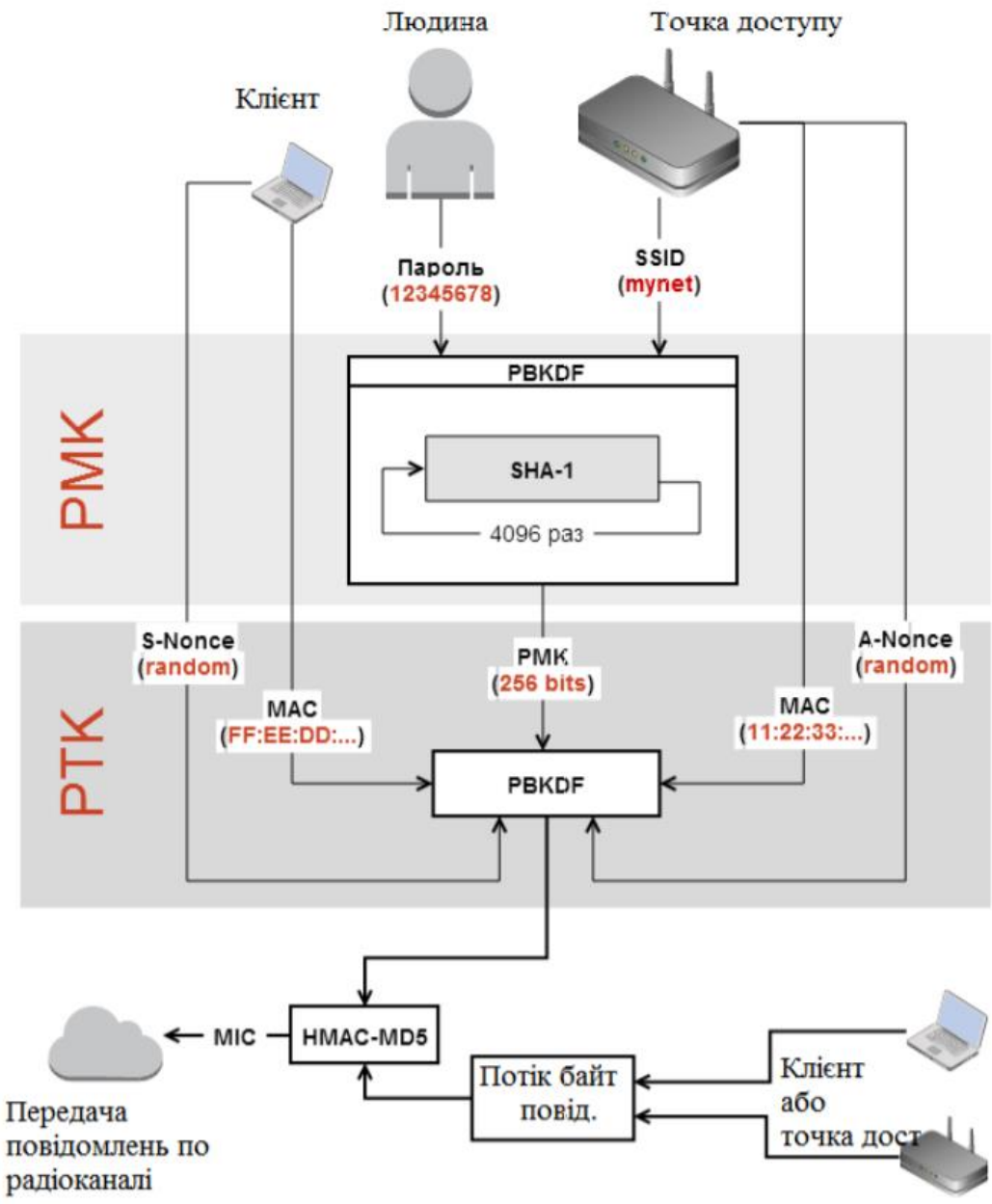

Рисунок 2.5 – Механізм роботи WPA2 IEEE 802

Стандарт IEEE 802.1x застосовується для авторизації і аутентифікації користувачів, з метою перевірки можливості надання доступу до мережі. 802.1x призначений для роботи зі сторонніми засобами, такими як сервер RADIUS і протокол EAP. Для аутентифікації в мережі на базі 802.1x використовується протокол EAP. Різні виробники підтримують різні типи EAP, а також кілька типів одночасно. Процес EAP аналогічний для всіх типів зображений на рисунку 2.6.

Рисунок 2.6 – Процес аутентифікації за алгоритмом EAP

Сервер RADIUS - свого роду засіб, який вирішує, надати користувачу доступ в мережу чи ні (докладніше його робота буде представлена в п. 2.3.3).

2.2 Основні цілі та завдання аудиту комп’ютерної мережі

У сучасних умовах бізнес-процеси будь-якої компанії залежать не тільки від рівня кваліфікації її співробітників, але і від роботи інформаційної структури

підприємства, яку необхідно підтримувати в належному стані. З цією метою треба постійно виконувати заходи щодо аудиту комп'ютерної мережі. Аудит інформаційної безпеки (ІБ) – це незалежна перевірка інформаційної системи будь-якого підприємства, установи або організації на предмет забезпечення безпеки з використанням спеціально розроблених критеріїв і показників.

Основними завданнями проведення такого аудиту є:

– перевірка об’єктів, які задіяні в різних процесах (комп’ютерні мережі та системи, засоби комунікації, прийому та обробки даних);

– виявлення можливих каналів витоку інформації і потенційних дір в системі безпеки;

– перевірка всіх електронних пристроїв і локальних комп’ютерних мереж та систем на дію електромагнітного випромінювання;

– робота по створенню концепції безпеки і застосування на практиці.

Головні задачі проведення аудиту безпровідної мережі:

– оцінка стану захищеності інформації в комп’ютерній мережі;

– аналіз можливих ризиків пов’язаних з загрозою можливості проникнення в комп’ютерну мережу сторонніми користувачами;

– аналіз відповідності рівня безпеки мережі діючим стандартам і нормативно-правовим актам;

– розробка та видача рекомендацій, які пропонують варіант позбавлення проблем в разі необхідності.

2.3 Технології захисту доступу до Wi-Fi-пристроїв засобами AAA

2.3.1 Опис та порівняння віддаленої та локальної баз захисту

Засоби AAA підтримують контроль доступу за допомогою локальної БД на сервері мережного доступу, або за допомогою віддаленої БД захисту, що використовує протокол захисту AAA.

Якщо потрібно забезпечити доступ до мережі невеликому числу віддалених користувачів через один-два сервери мережного доступу, можна зберігати інформацію про їхні імена й паролі на сервері мережного доступу.

Такий підхід називають локальною аутентифікацією, або аутентифікацією за допомогою локальної БД захисту. Нижче зазначені особливості використання засобів ААА з локальною БД захисту.

1. Локальна аутентифікація підходить для малих мереж з невеликою кількістю віддалених користувачів і серверів мережного доступу.

2. Імена користувачів, паролі й параметри авторизації зберігаються в локальній БД захисту на сервері мережного доступу.

3. Віддалені користувачі проходять аутентифікацію і авторизацію за допомогою локальної бази дані захисти.

4. Авторизація й аудит при використанні локальної БД захисту мають обмежену підтримку.

5. Контроль доступу за допомогою локальної БД захисту дозволяє заощадити на установці й підтримці віддаленої БД захисту.

Аутентифікація з використанням локальної БД захисту часто виконується так, як показано на рис.2.7. Спочатку за допомогою команд ААА необхідно в локальній БД захисту кожного сервера мережного доступу вказати відповідні параметри для кожного з можливих користувачів.

Процес ААА складається з наступних кроків:

1. Віддалений користувач встановлює з'єднання PPP із сервером мережного доступу.

2. Сервер мережного доступу запитує в користувача ім'я та пароль.

3. Сервер мережного доступу виконує аутентифікацію імені та паролю за допомогою локальної бази.

4. Сервер мережного доступу виконує процедуру авторизації, у результаті чого користувач одержує право доступу до мережних ресурсів у відповідності зі значеннями, заданими в локальній БД.

5. Сервер мережного доступу стежить за трафіком користувача й створює запису аудиту у відповідності зі значеннями, заданими в локальній БД.

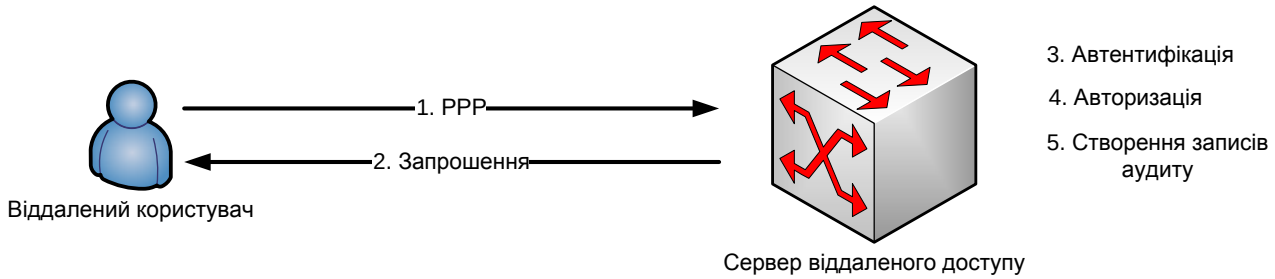

Рисунок 2.7 – Локальна БД захисту

ААА та віддалена БД захисту. У міру росту мережі усе більш гостро встає питання про необхідність використання віддаленої БД захисту, що забезпечувала б інформацію про імена користувачів і паролях всім серверам мережного доступу та маршрутизаторам або точкам доступу мережі. Віддалена БД захисту розміщується на сервері захисту.

Віддалену БД захисту зручно використати тоді, коли є велика кількість серверів мережного доступу, що контролюють доступ до мережі. Така БД дозволяє централізовано управляти файлами профілів (параметрами доступу) віддалених користувачів, що рятує від необхідності змінювати файли профілів кожного віддаленого користувача на всіх серверах мережного доступу. Віддалена БД захисту допомагає створити та реалізувати погоджену політику захисту віддаленого доступу для всіх користувачів.

Розглянемо особливості використання засобів ААА з віддаленою БД захисту:

- аутентифікація за допомогою віддаленої БД захисту оптимальна для середніх і великих мереж з більшим числом віддалених користувачів і безліччю серверів мережного доступу, коли витрати на утримання сервера захисту можуть бути виправдані;

- імена користувачів, паролі й параметри авторизації централізовано зберігаються у віддаленій БД зашиті на сервері захисту;

- віддалені користувачі проходять процедури аутентифікації та авторизації за допомогою віддаленої БД;

- авторизація й аудит підтримуються сервером мережного доступу з використанням віддаленої бази дані захисти;

- віддалена БД захисту може використовуватися для контролю доступу до сервера мережного доступу або до мережі через сервер мережного доступу. Деякі протоколи віддаленої БД захисту підтримують контроль доступу до маршрутизаторів, комутаторів, точок доступу і брандмауерам;

- централізований контроль за допомогою віддаленої БД захисту дозволяє заощадити засоби, рятуючи від необхідності керувати кожним сервером мережного доступу окремо. Для захисту БД необхідно, щоб утримуючий її вузол був захищений з максимальним ступенем надійності.

Аутентифікація з використанням віддаленої БД захисту звичайно виконується як показано рис.2.8.

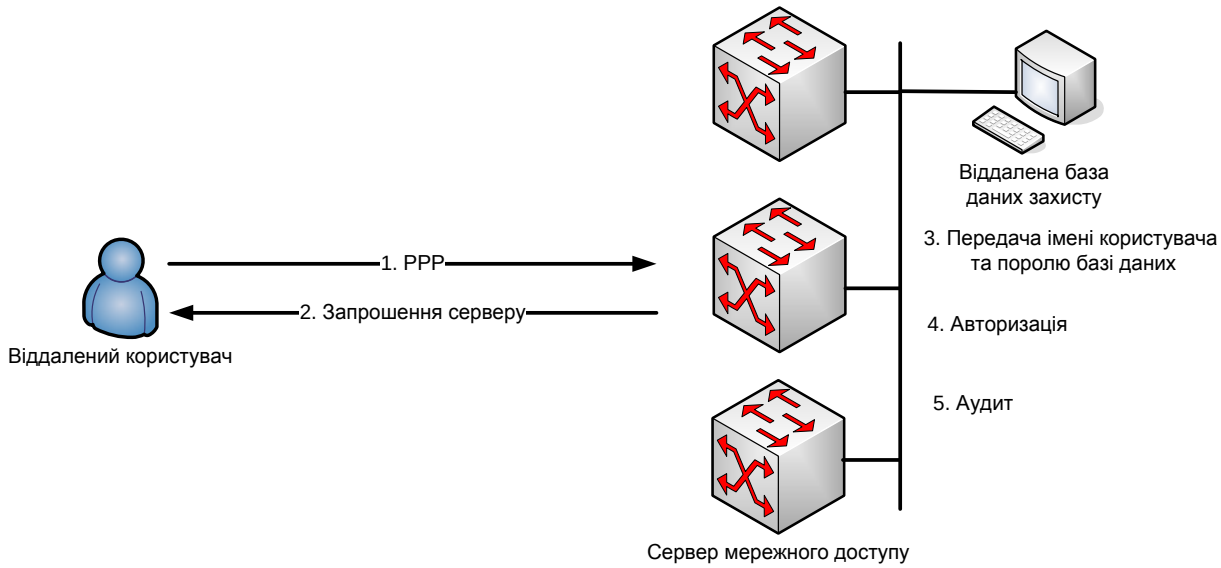

Рисунок 2.8 – Віддалена БД захисту

Спочатку необхідно заповнити локальну БД захисту кожного сервера мережного доступу, описавши відповідні параметри для кожного з можливих користувачів. Крім того, необхідно настроїти сервер мережного доступу на взаємодію з віддаленою БД захисту при виконанні операцій AAA. Процес AAA в цьому випадку складається з наступних кроків:

1. Користувач установлює з'єднання PPP із сервером мережного доступу.

2. Сервер мережного доступу запитує в користувача ім'я й пароль, і користувач пред'являє відповідні дані.

3. Сервер мережного доступу передає ім'я користувача й пароль серверу захисту.

4. Віддалена БД захисту виконує процедуру аутентифікації та авторизації для даного користувача й надає йому відповідні права доступу в мережі. БД насправді змінює конфігурацію сервера мережного доступу відповідно до параметрів аутентифікації, завантажуючи необхідні команди в сервер мережного доступу й активізуючи відповідні списки доступу.

5. Сервер мережного доступу створює запис аудиту відповідно до параметрів віддаленої БД захисту й відправляє ці записи серверу захисту. Сервер захисту теж може створювати записи аудиту.

Основною перевагою використання віддаленої БД захисту є те, що внаслідок централізованого керування спрощується адміністрування й забезпечується погоджена реалізація політики захисту відносно віддаленого доступу та керуванням точками доступу.

Мережне устаткування Cisco підтримує три протоколи сервера захисту TACACS+, RADIUS та Kerberos. TACACS+ і RADIUS є головними протоколами сервера захисту, використовуваними для рішення завдань AAA із серверами доступу по мережі, маршрутизаторами та точками доступу. Ці протоколи необхідно використовувати для обміну даних про керування доступом між сервером захисту й мережним устаткуванням.

Сервери захисту TACACS+ або RADIUS взаємодіють із мережним устаткуванням так, ніби вони це сервери доступу по мережі. На рис.2.9 сервер мережного доступу виступає в ролі клієнта TACACS+ або RADIUS стосовно сервера захисту TACACS+ або RADIUS. Для обміну інформацією про події AAA між клієнтом і сервером використається протокол TACACS+ або RADIUS.

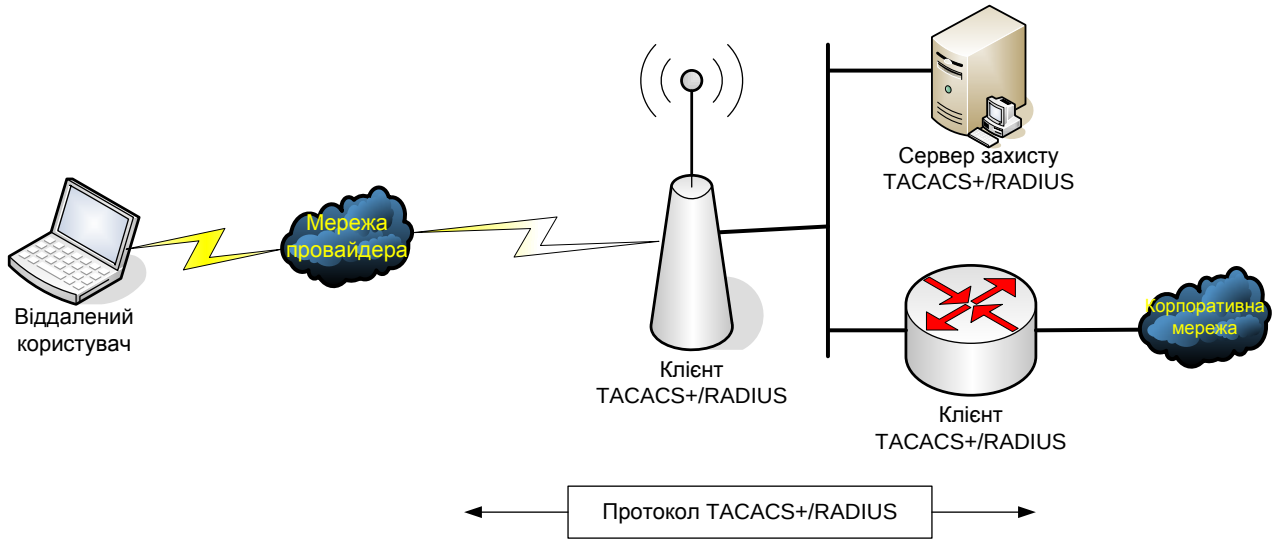

Рисунок 2.9 – Підтримка TACACS+ або RADIUS сервером мережного доступу

2.3.2 Принципи роботи серверу TACACS+

TACACS+ є додатком сервера захисту, який має змогу виконати загальне керування доступом користувачів до сервера мережного доступу, Wi-Fi – пристрою, маршрутизатора або іншого устаткування мережі, що підтримує TACACS+.

Дані про користувачів та сервіс TACACS+ зберігаються в БД на комп'ютері, що керується ОС Windows NT або UNIX. TACACS+ дозволяє за допомогою одного сервера керування додатками (демона TACACS+) реалізувати незалежну підтримку сервісів AAA. TACACS+ є поліпшеною версією. TACACS надає можливість серверу TACACS+ підтримувати незалежне застосування сервісів AAA.

При процесі аутентифікації TACACS+ використовуються пакети трьох типів: START, CONTINUE, REPLY (початогк, продовження, відповідь). Процес аутентифікації TACACS+, у якому сервер мережного доступу обмінюється пакетами аутентифікації із сервером TACACS+, наведено на рис.2.10.

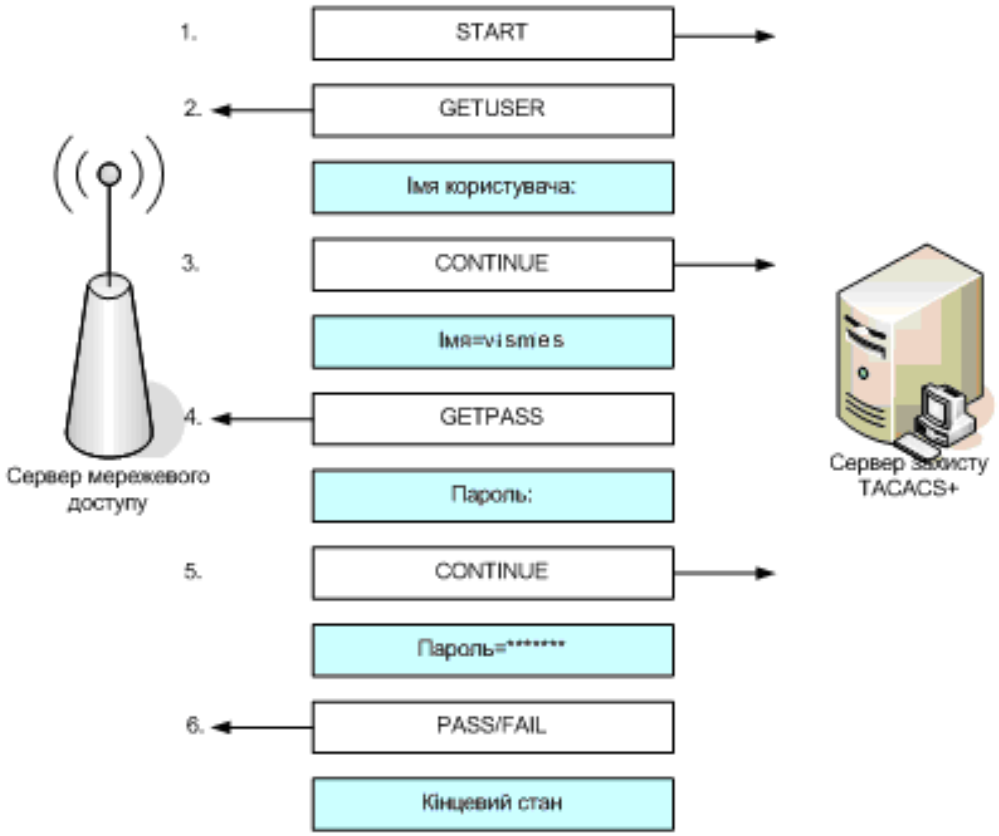

Рисунок 2.10 – Процес аутентифікації TACACS+

При виконанні процесу авторизації TACACS+ є пакети двох типів: REQUEST і RESPONSE (запит і відповідь). Процес авторизації TACACS+, у якому сервер мережного доступу обмінюється пакетами авторизації із сервером TACACS+, наведено на рис.2.11.

Рисунок 2.11 – Процес авторизації TACACS+

При виконанні процесу аудиту TACACS+ використовує пакети двох типів - REQUEST і RESPONSE (запит і відповідь). Цей процес схожий з процесом авторизації. Процес аудиту TACACS+, у якому сервер мережного доступу обмінюється пакетами аудиту із сервером TACACS+, наведено на рис.2.12.

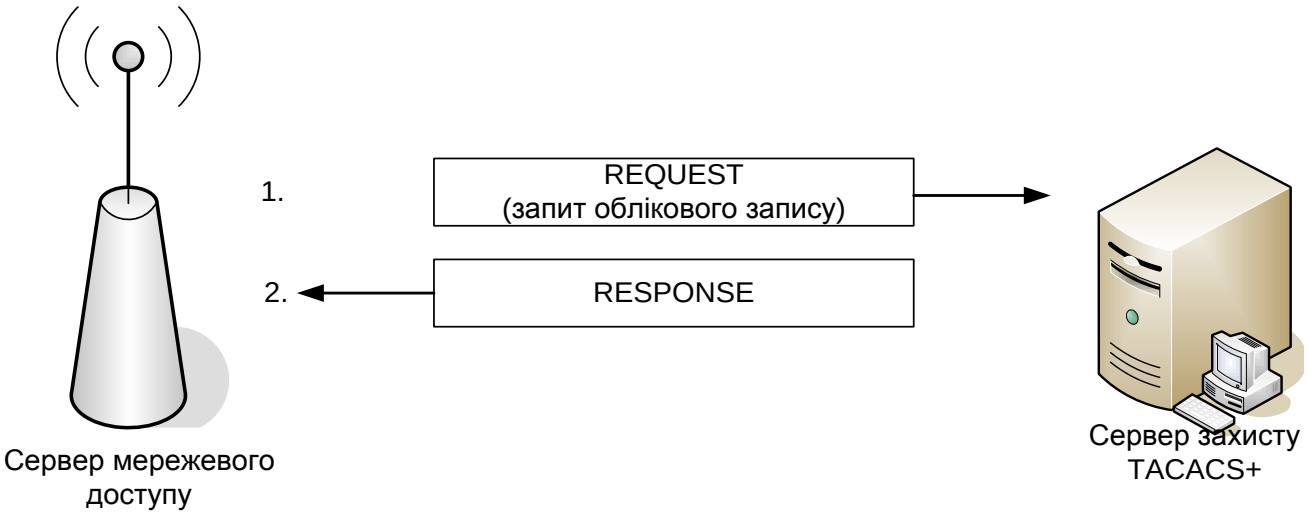

Рисунок 2.12 – Процес аудиту TACACS+

2.3.3 Принцип роботи серверу RADIUS

RADIUS являє собою розподілений протокол, використовуваний у рамках технології клієнт/сервер, що забезпечує захист мережі від НСД. Cisco підтримує цей протокол як складову системи захисту AAA.

RADIUS можна застосовувати з іншими протоколами захисту AAA, наприклад з TACACS+, Kerberos і локальними базами дані захисти. Протокол RADIUS описується в документі RFC 2865, а аудит RADIUS - в RFC 2866.

Протокол RADIUS реалізований у багатьох мережних середовищах, що вимагають високого рівня захисту за умови підтримки мережного доступу для віддалених користувачів. Він являє собою повністю відкритий протокол, що поставляє у форматі вихідного тексту, якому можна змінити для того, щоб він міг працювати з будь-якою доступної в даний момент системою захисту. Широку популярність RADIUS забезпечує можливість додавати нові пари "атрибут/значення" на додаток до тих, які описані в документі RFC 2865.

Внаслідок використання пар "атрибут/значення" конкретних

постачальників можуть виникати труднощі при інтеграції серверних продуктів захисту RADIUS в інші системи захисту. Сервери захисту RADIUS і відповідні клієнти повинні ігнорувати нестандартні пари «атрибут/значення».

Існує безліч версій RADIUS, основними з яких є наступні:

- Реалізація IETF, описується в документі RFC 2865, а аудит RADIUS - в документі RFC 2866. Підтримує приблизно 63 атрибута.

- Реалізація Cisco. Починаючи з Cisco IOS Release 11.2, з кожною новою версією Cisco IOS та Cisco Secure ACS число підтримуваних цією реалізацією атрибутів росте, а її функціональні можливості постійно розширюються. У цей час підтримується приблизно 58 атрибутів.

- Реалізація Ascend. Компанія Ascend постійно додає атрибути постачальника, що забезпечують, наприклад, підтримку кешування маркерів доступу зміни пароля. Програмний інтерфейс додатка (API) дає можливість швидкої розробки нових розширень, у результаті чого іншим постачальникам важко конкурувати із цією компанією в області пропозиції новинок. Ця реалізація підтримує більше 254 атрибутів.

RADIUS надає такі можливості сервера захисту:

- Пакети UDP. Для зв'язку RADIUS між сервером мережного доступу та сервером захисту використається протокол UDP та UDP - порт 1812, офіційно призначений для цього. Деякі реалізації RADIUS використають UDP -порт 1645.

- Об'єднання аутентифікації й авторизації та виділення аудиту. Сервер RADIUS одержує запити користувача, виконує аутентифікацію та забезпечує клієнтові інформацію про конфігурації. Аудит виконується сервером RADIUS.

- Шифрування паролів користувачів. Всі паролі, що знаходяться в пакетах RADIUS (користувальницькі), шифруються за допомогою хешування MD5.

- Аутентифікація PAP та CHAP. Керує аутентифікацією при допомозі засобів виклику/відповіді PAP і CHAP, а також діалогу початку сеансу та введення паролю (схоже на вхід в UNIX).

- Захист глобальної мережі. Забезпечує підтримку засобів AAA віддаленого доступу для серверів мережного доступу багатьох постачальників,

що підтримують клієнтів RADIUS. Дає можливість централізувати керування віддаленим доступом.

- Розширюваність. Всі транзакції припускають використання пар "атрибут/значення" змінної довжини. Нові атрибути можуть бути додані в існуючі реалізації протоколу.

- Гарантований мережний захист. Аутентифікація транзакцій між клієнтом і сервером захисту припускає використання загального секретного значення.

Процес аутентифікації й авторизації RADIUS. Клієнт RADIUS і сервер захисту RADIUS обмінюються пакетами Access-Request (доступ-запит), Access-Accept (доступ-підтвердження), Access-Reject (доступ-відмова) і Access-Challenge (доступ-виклик). Як показано на Рис.2.13, при спробі підключитися до серверу мережного доступу, що має конфігурацію клієнта RADIUS, виконуються наступні кроки:

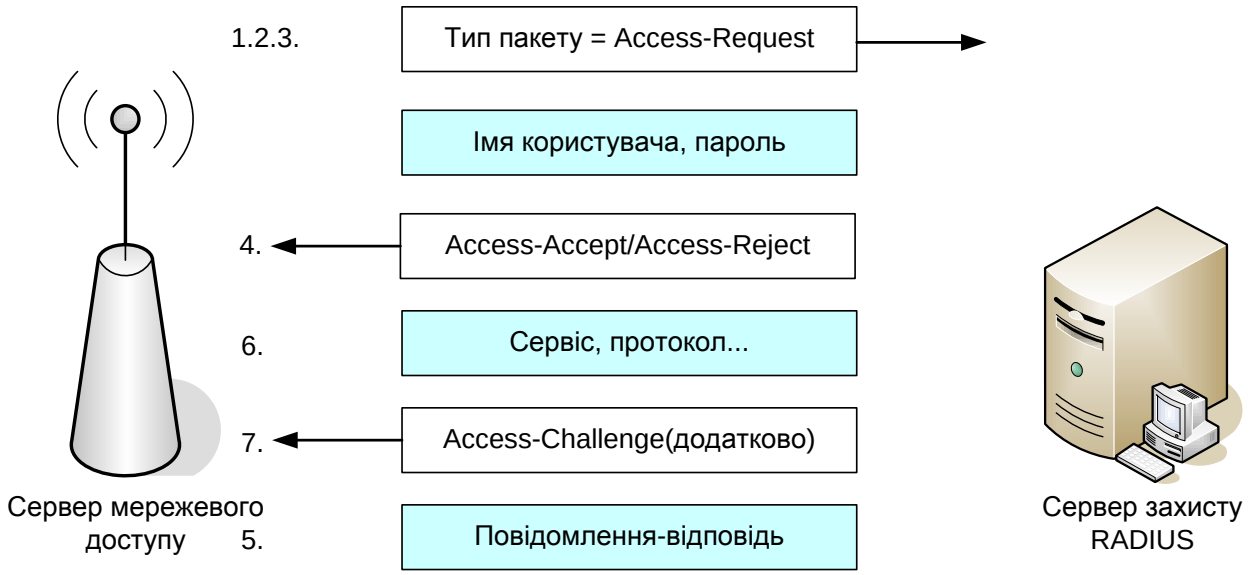

Рисунок 2.13 – Процес аутентифікації та авторизації RADIUS

1. Користувач ініціалізує запит аутентифікації PPP до сервера доступу.

2. У користувача запитується ім'я й пароль, та він вводить їх.

3. Сервер мережного доступу надсилає на сервер захисту RADIUS пакет Acces-Request з ім'ям користувача, шифрованим паролем та інше.

4. Сервер захисту RADIUS ідентифікує клієнта, що посилає, виконує

аутентифікацію користувача, перевіряє параметри авторизації користувача і повертає один з наступних відповідей:

- Access-Accept - користувач аутентифікований;

- Access-Reject - користувач неаутентифікований, і сервер мережного доступу або пропонує ввести ім'я користувача й пароль знову, або забороняє доступ.

- Access-Challenge - виклик є додатковою можливістю сервера захисту RADIUS, що дозволяє одержати додаткові дані про користувача, щоб переслати їх серверу захисту RADIUS.

5. Сервер мережного доступу звертається до параметрів аутентифікації, що дозволяють використання конкретних служб.

6. Відповідь Access-Accept або Access-Reject зв'язується з додатковими даними (парами "атрибут/значення"), використовуваними для сеансів EXEC та авторизації. Процес аутентифікації RADIUS повинен бути завершений до початку процесу авторизації. Додаткові дані в пакетах Accept або Reject складаються з пари "атрибут/значення" для наступних об'єктів: сервіси, до яких дозволяється доступ користувачеві, включаючи Telnet та rlogin; сервіси EXEC і SLIP; параметри з'єднання, включаючи IP-адреса клієнта та вузла, список доступу і обмеження часу.

7. Сервер захисту RADIUS може періодично посилати пакети Access-Challenge серверу мережного доступу, щоб запросити повторного введення імені та паролю користувачем, інформувати про стан сервера мережного доступу або виконати якісь інші дії, передбачені розроблювачами сервера RADIUS. Клієнт RADIUS не може посилати пакети Access-Challenge.

Процес аудиту RADIUS. RADIUS удосконалили з метою забезпечення доставки інформації аудиту від клієнта RADIUS до серверу аудиту RADIUS через UDP-порт 1813. Клієнт RADIUS відповідає за відправлення інформації аудиту користувача відповідному серверу аудиту RADIUS, для чого використається пакет типу Accounting-Request (аудит-запит) з відповідним набором пар "атрибут/значення".

Сервер аудиту RADIUS повинен прийняти запит аудиту та повернути

відповідь, що підтверджує успішне одержання запиту. Для цього використається пакет типу Accounting-Response (аудит-відповідь).

Як показано на рис.2.14, при спробі підключитися до сервера мережного доступу, що має конфігурацію клієнта RADIUS, виконуються наступні кроки:

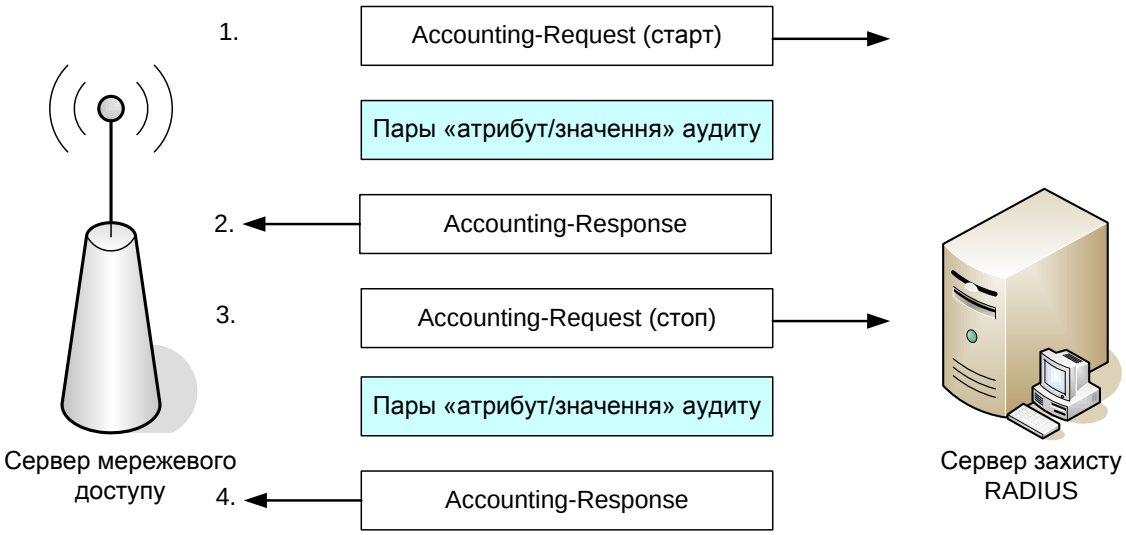

Рисунок 2.14 – Процес аудиту RADIUS

1. Після початкової аутентифікації сервер мережного доступу посилає серверу захисту RADIUS старт-пакет Accounting-Request.

2. Сервер захисту RADIUS підтверджує одержання старт-пакету, повертаючи пакет Accounting-Response.

3. По закінченні використання сервісу сервер мережного доступу посилає стоп-пакет Accounting-Request; у цьому пакеті вказуються тип представленого сервісу та додаткові статистичні дані.

4. Сервер захисту RADIUS підтверджує одержання стоп-пакета, повертаючи пакет Accounting-Response.

2.3.4 Порівняння роботи серверів аутентифікації

Хоча TACACS+ та RADIUS дуже схожі за своїми функціональним можливостями, є кілька важливих відмінностей, зазначених у таблиці 2.1.

Таблиця 2.1 – Порівняння TACACS+ та RADIUS

Функціональні можливості	TACACS+	RADIUS
Підтримка AAA	Розподіл трьох сервісів	Аутентифікація і авторизація разом, аудит окремо
Транспортний протокол	TCP	UDP
Виклик/ відповідь	Двонаправлений	Однонаправлений
Підтримка протоколів	Повна підтримка	NetBEUI
Цілісність даних	Шифрується весь пакет	Шифруються тільки паролі користувачів

Функціональні можливості. TACACS+ розділяє функції AAA відповідно до архітектури AAA, тим самим забезпечуючи модульність реалізації сервера захисту. RADIUS поєднує аутентифікацію та авторизацію, а аудит розглядається окремо, що означає меншу гнучкість реалізації.

Транспортний протокол. Використання протоколу UDP для RADIUS (замість TCP, як в TACACS+) було обрано з метою спрощення реалізації клієнта й сервера. Але це робить протокол RADIUS менш стійким і вимагає додаткових заходів надійності від сервера (ретрансмісії пакетів і використання обмежень за часом, замість того щоб покладатися на протокол 4-го рівня (модель OSI)).

Виклик/відповідь. TACACS+ підтримує двонаправлений потік викликів/відповідей між серверами мережного доступу подібно тому, як це зроблено в CHAP. RADIUS підтримує односпрямований виклик/відповідь від сервера захисту RADIUS до клієнта RADIUS.

Підтримка протоколів. TACACS+ забезпечує більше повну підтримку протоколів віддаленого та міжмережного доступу.

Цілісність даних. TACACS+ припускає шифрування вмісту пакетів. RADIUS передбачає шифрування тільки атрибутів пароля в пакеті.

Access-Request. Це означає кращу захищеність TACACS+. Крім того,

порівнюючи TACACS+ та RADIUS, можна відзначити наступне:

Можливості настроювання. Гнучкість протоколу TACACS+ забезпечує можливість настроювання безлічі параметрів відповідно до вимог окремих користувачів (наприклад, настроювання запиту імені користувача й пароля). Через недостатню гнучкість RADIUS багато можливостей, доступні в рамках TACACS+, при використанні RADIUS недоступні. З іншого боку, RADIUS підтримує можливість зміни наборів пара "атрибут/значення".

Процес авторизації. При використанні TACACS+ сервер приймає або відкидає запит аутентифікації на підставі даних користувальницького профілю. Клієнтові (серверу мережного доступу) зміст користувальницького профілю залишається невідомим. У системі RADIUS всі атрибути користувальницького профілю, що посилають із відповіддю, передаються серверу мережного доступу. Сервер мережного доступу приймає або відкидає запит аутентифікації на підставі отриманих їм значень атрибутів.

Аудит. Аудит TACACS+ припускає використання обмеженого числа інформаційних полів. Аудит RADIUS може надати більше інформації, ніж можна було б одержати із записів аудиту TACACS+, що є головною перевагою RADIUS.

2.4 Висновки до розділу

В цьому розділі проведено огляд алгоритмів аутентифікації в безпровідних мережах, сформульовано основні цілі та завдання аудиту комп’ютерної мережі, досліджено технології захисту доступу до Wi-Fi-пристроїв за допомогою засобів AAA (сервери TACACS+, RADIUS).

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ПРОВЕДЕННЯ АУДИТУ ЗАХИЩЕНОСТІ БЕЗПРОВІДНИХ МЕРЕЖ

3.1 Механізм проведення аудиту захищеності безпровідних мереж

Аудит ІБ - це незалежна перевірка ІС будь-якого підприємства, установи або організації на предмет забезпечення безпеки з використанням спеціально розроблених критеріїв і показників. Мета проведення аудиту – надати об'єктивну незалежну комплексну оцінку поточному стану захищеності ІС, що дозволить провести систематизацію загрози ІБ і розробити рекомендації усунення цих загроз.

Модель збору даних для проведення аудиту. Якість проведеного аудиту безпеки багато в чому залежить від повноти і точності інформації, яка була отримана в процесі збору вихідних даних. Тому виникає необхідність побудови загальної моделі збору інформації для проведення аудиту в безпровідних мережах.

Модель представлена в таблиці 3.1.

Таблиця 3.1 – Модель збору інформації для проведення аудиту

№ з/п	Тип інформації	Опис складу вхідних даних
1.	Організаційно-розпорядча інформація відповідна питанням безпеки	Політика інформаційної безпеки безпровідної мережі у відповідності до стандартів
2.	Інформація про апаратне заберезпення безпровідної мережі	Перелік серверів, робочих станцій, інформація про апаратну конфігурацію серверів
3.	Інформація про прикладне забезпечення	Перелік прикладного програмного забезпечення, опис функціональних задач
4.	Інформація про методи захисту	Інформація про виробника методів захисту, конфігураційні налаштування методів захисту, схема установки методів захисту
5.	Інформація про топологію мережі	Карта безпровідної мережі, інформація про типи каналів зв’язку, інформація про використовувані протоколи

Збір вихідних даних може здійснюватися з використанням таких методів:

– інтерв'ювання працівників установи, які володіють необхідною інформацією (перелік винесених питань складається і узгоджується зарання);

– надання опитувальних листів з певної тематики, які самостійно заповнюються співробітниками;

– аналіз існуючої організаційно-технічної документації;

– використання спеціалізованих програмних засобів, які дозволяють отримати необхідну інформацію про склад і налаштування безпровідної мережі та її програмно-апаратного забезпечення.

Побудова моделі загроз ІБ безпровідної мережі. Метою визначення та побудови моделі загроз безпеці безпровідної мережі є установлення того, чи існує можливість порушення конфіденційності, цілісностіності або доступності інформації, що міститься в безпровідній мережі, і призведе порушення хоча б одного із зазначених властивостей безпеки інформації до настання неприйнятних негативних наслідків.

Загрози інформаційної і технічної безпеки представлені на рисунку 3.1.

Рисунок 3.1 – Класифікація загроз в безпровідних мережах

Аналіз відомих порушень безпеки функціонування систем безпровідного зв’язку дозволяє побудувати модель загроз ІБ безпровідної мережі та механізмів протидії (рис. 3.2) та виділити ряд загроз, яким повинні бути протиставлені механізми захисту.

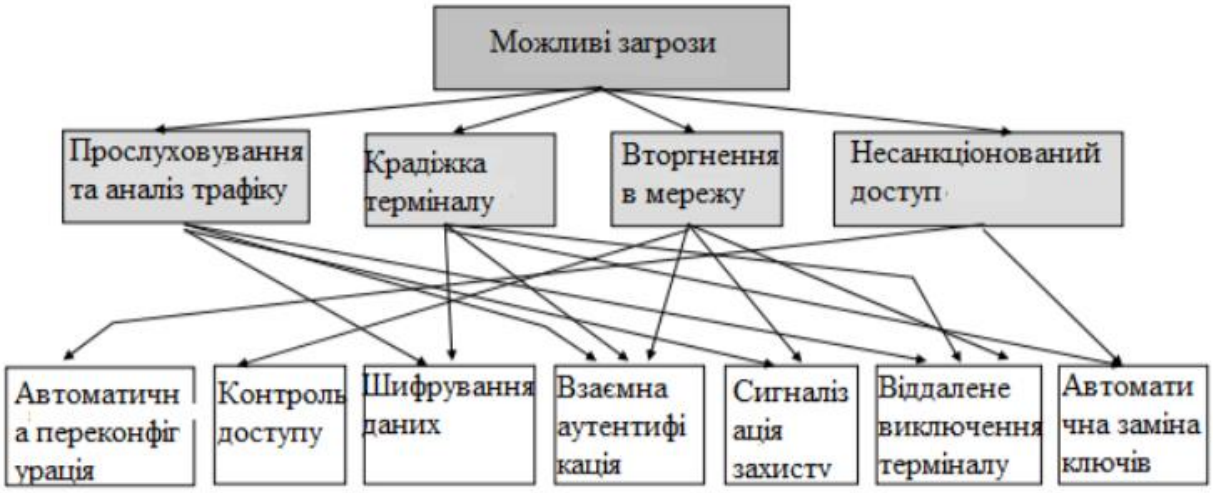

Рисунок 3.2 – Модель механізмів протидії загрозам ІБ безпровідній мережі

3.2 Розробка профілю захисту для мереж стандарту 802.11

3.2.1 Специфіка створення профілю захисту для мереж стандарту 802.11

ISO/IEC 27001 визначає критерії, які направлені на захист інформації від НСД, модифікації або втрати можливі її використання. На сьогодні "Загальні критерії" (Common Criteria) - найповніший і сучасний оціночний стандарт. Насправді, цей стандарт, визначає інструменти оцінки безпеки ІС і порядок їх використання; він не містить визначених класів безпеки. Такі класи можна будувати, опираючись на задані вимоги. Загальні критерії (ЗК) оцінки ІБ ІС мають два види вимог безпеки:

– функціональні (відповідник активному аспекту захисту), які ставляться до функцій безпеки і до реалізованих ними сервісами;

– вимоги довіри (відповідник пасивному аспекту).

Здійснюється формулювання вимог безпеки, проводиться перевірка їх виконання для певного об'єкту оцінювання – апаратно-програмного продукту або ІС. Загальні критерії сприяють формуванню двох базових видів використовуваних на практиці нормативних документів - це профіль захисту (ПрЗ) і завдання по безпеці.

ISO/IEC 27001 містить критерії, які повинні використовуватися експертами при формуванні суджень про відповідність об’єкта оцінки вимогами щодо їх

безпеки. Документ описує безліч спільних дій, які повинен виконати експерт, і функції безпеки, відповідно до яких виконуються ці дії. Відзначимо, що загальні критерії не визначають процедури, якої треба дотримуватися при проведенні цих дій. Для того щоб досягти більшої порівнянності результатів оцінки між собою, оцінки повинні виконуватися в рамках узгодженої системи оцінки, яка враховує стандарти, стежить за якістю оцінок і керує правилами, яким повинні відповідати засоби оцінки і оцінювачі.

Використання загальної методології оцінок сприяє відтворюваності і об'єктивності результатів, але саме по собі не є достатнім. Багато з критеріїв оцінки вимагають застосування експертного висновку та додаткових знань і навичок, за якими важче досягти узгодженості. Щоб підвищити узгодженість отриманих даних по оцінці, остаточні результати оцінки можна піддати процесу сертифікації. Процес сертифікації є незалежною перевіркою результатів оцінки, що веде до вироблення кінцевого сертифіката або підтвердження. Сертифікат зазвичай публічно доступний. Загальні критерії являють собою вимоги безпеки під певні категорії функціональних вимог і вимог гарантії. Функціональні вимоги безпеки (ФБВ) накладаються на ті функції об’єкту оцінки, які існують спеціально для підтримки безпеки продукту інформаційних технологій і визначають бажану поведінку в галузі безпеки.

У зв'язку з цією потребою виділилося і сформувалося поняття профілів захисту, як основного інструменту функціональної стандартизації. Профіль - це сукупність кількох (або підмножина одного) базових стандартів з чітко визначеними і гармонізованими підмножинами обов'язкових і факультативних можливостей, призначених для реалізації заданої функції або групи функцій. ПрЗ інформації повинен забезпечувати реалізацію політики ІБ, що розробляється відповідно до необхідної категорією безпеки і критеріями безпеки. Специфіка створення профілю захисту для безпровідних мереж базується на специфіці їх побудови, особливості конфігурації і технології обробки і передачі інформації.

За рахунок відкритого середовища передачі даних в бездротових мережах повинні бути посилені вимоги безпеки, що висуваються до об’єкту оцінки на етапах аутентифікації, авторизації, контролю доступу і шифрування переданої

інформації.

Найчастіше положення профілю захисту для безпровідних мереж багато в чому перетинаються з традиційним змістом подібних документів (табл. 3.2). Так, наприклад, вимоги щодо фізичного захисту точок доступу цілком перекриваються питаннями фізичної безпеки активного мережного обладнання.

Таблиця 3.2 – Основні вимоги безпеки до безпровідних мереж

Вимоги до безпеки	Специфіка безпровідних мереж
Контроль підключень до мережі	Рівень ризику, пов'язаного з підключенням несанкціонованої точки доступу або клієнта бездротової мережі, можна знизити шляхом відключення невикористовуваних портів комутаторів, фільтрації по MAC-адресам (Port-security), аутентифікації 802.1x, систем виявлення атак і сканерів безпеки, контролюючих появу нових мережевих об'єктів
Фізична безпека	Контроль потужності випромінюваного сигналу дозволяє обмежити ймовірність підключення до мережі бездротових пристроїв.
Мінімізації привілеїв користувача	Якщо користувач працює на комп'ютері з мінімально необхідними правами, то знижується ймовірність самовільної зміни налаштувань бездротових інтерфейсів
Контроль політики безпеки	Засоби аналізу захищеності, такі як сканери вразливостей, дозволяють виявляти появу в мережі нових пристроїв і визначити їх тип, а також відстежувати відхилення параметрів клієнтів від заданого профілю
Інвентаризація ресурсів	Наявність актуального оновлюваного списку мережевих ресурсів полегшує виявлення нових мережевих об'єктів
Виявлення атак	Застосування систем виявлення атак як традиційних, так і бездротових дає можливість своєчасно визначати спроби НСД
Безпека середовища	У зв'язку з відкритої природою каналів передачі даних безпровідних мереж накладається ряд обмежень на передану інформацію в залежності від її цінності і на допустиму дальність її поширення.
Аутентифікація	Повинні бути визначені вимоги до зберігання даних аутентифікації, їх зміні, складності, безпеки при передачі по мережі. Можуть бути явно визначені використовувані методи EAP, методи захисту загального ключа сервера RADIUS.
Віддалений доступ до мережі	У більшості випадків користувачів бездротової мережі логічно відносити до користувачів систем віддаленого доступу. Це обумовлено аналогічними загрозами і як наслідок - контрзаходами, характерними для даних компонентів ІС

Продовження табл. 3.2

Розподіл мереж	У зв'язку зі специфікою бездротових мереж бажано виділяти точки бездротового доступу в окремий мережевий сегмент за допомогою брандмауера, особливо коли мова стосується гостьового доступу
Використання криптографічних методів	Повинні бути визначені використовувані протоколи і алгоритми шифрування трафіку в бездротової мережі (WEP або AES).

3.2.2 Графоаналітична модель структури сімейства профілів захисту

Для побудови графоаналітичної моделі структури сімейства профілів захисту розробимо сам ПрЗ в наочному вигляді. У загальному вигляді структура профілю захисту представлена на рисунку 3.3.

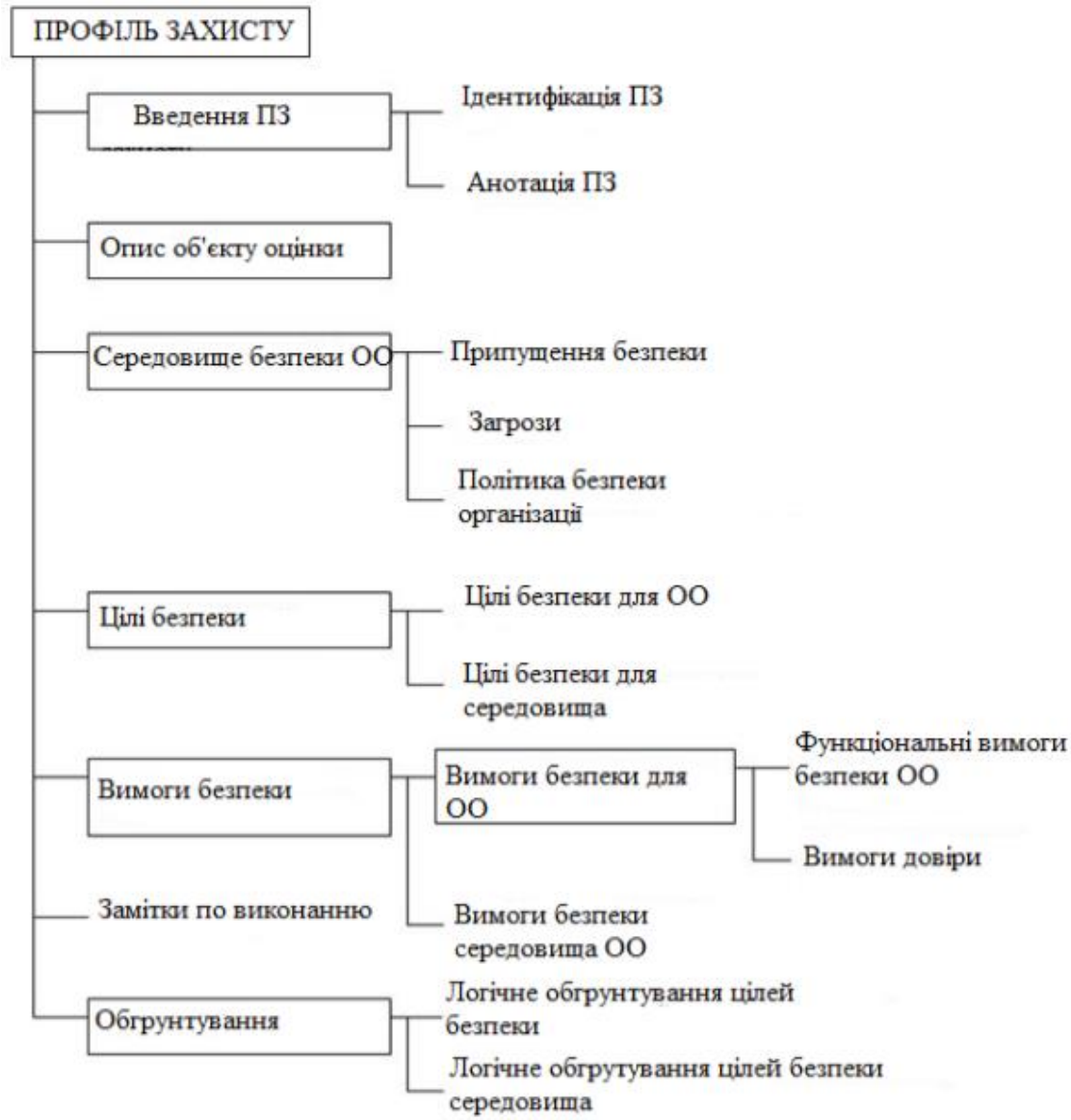

Рисунок 3.3 – Загальна структура профілю захисту

Об'єднавши описані вище поняття профілю захисту, побудуємо схему формування профілю захисту на основі виробленого для сімейства базового функціонального пакету (рис. 3.4)

Рисунок 3.4 – Схема формування профілю захисту

Виходячи з наведеної вище структури типового ПрЗ і вдаючись до теорії графів, побудуємо в загальному вигляді модель даної структури (рис. 3.5).

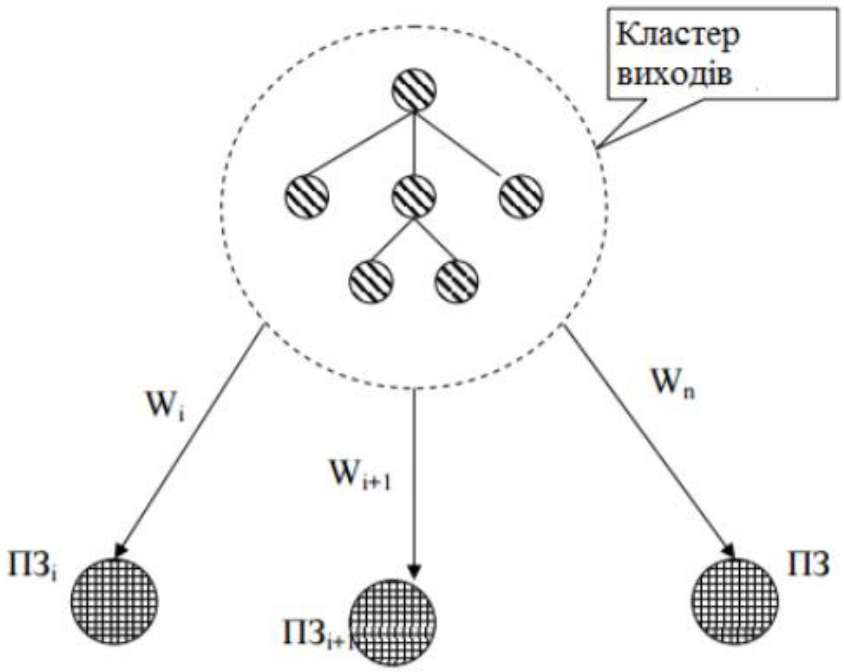

Рисунок 3.5 – Модель структури сімейства профілів захисту

Кластер результатів являє собою вершину графа. У нашому випадку вершиною графа є ФБВ ПрЗ, що складається з безлічі базових ФВБ:

$$ФВБ = \{Wб\} = \{Уб, ЦБб\}, \quad (3.1)$$

де {Wб} – множина, яка представляє базовий набір ФВБ; {Уб, ЦБб } – множии базових загроз для об’єкту оцінки.

Залежно від середовища безпеки об’єкту оцінки на базовий функціональний пакет накладається ряд додаткових ФВБ, виходячи з яких і будується ПрЗ для певного класу захищеності об’єкту оцінки:

$$ВБ = \{Wd\} = \{Уd, ЦБd\}, \quad (3.2)$$

Таким чином, підсумовуючи все вищесказане, отримуємо, що ПрЗ для певного класу захищеності ОО являє собою сукупність двох множин: множини базових ФВБ, що представляють собою БФП сімейства ПрЗ, і безлічі додаткових ФВБ, що додаються до нього:

$$Зі= БФП + \{Wd\} = \{Wб\} + \{Wd\} = \{Уб,ЦБб\} \vee \{Уd, ЦБd\}, \quad (3.3)$$

Таким чином, ми отримали сукупність компонентів ПрЗ виходячи з принципу формування сімейства ПрЗ. Для побудови графоаналітичної моделі структури ПрЗ введемо наступне його визначення: сукупність агентів захисту, розташованих у вузлах комутації, і з'єднань захисту, організаційно реалізованих в окремих виділених віртуальних каналах. Позначимо ПрЗ як наступну множину - сукупність чотирьох сервісних служб захисту - аутентифікації, конфіденційності, достовірності та контролю доступу, які і реалізуються агентами захисту (рис. 3.6):

$$ПрЗ = \{GA, GK, GД, GЦ\}, \quad (3.4)$$

де GA- граф аутентифікації, GК- граф конфіденційності, GД- граф достовірності, GЦ- граф контролю доступу

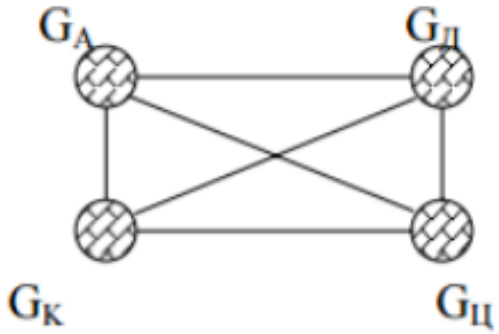

Рисунок 3.6 – Модель структури ПрЗ при однаковій вазі агентів захисту

Всі сервісні служби за замовчуванням мають рівнозначну вага при побудові ПрЗ, але в залежності від специфіки ОО і його середовища безпеки одні можуть переважати над іншими (рис. 3.7).

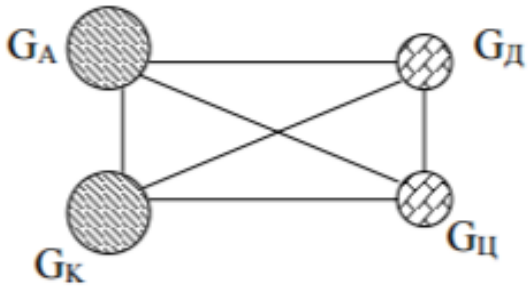

Рисунок 3.7 – Модель структури ПрЗ при різній вазі агентів захисту

Таким чином, при зміні хоча б одного з параметрів змінюється відповідно і сам ПрЗ, але його основа залишається незмінною. Для того, щоб оцінити захищеність бездротової мережі, а згодом проаналізувати отримані результати, нам необхідно виробити ряд критеріїв, відповідно до яких буде можливо провести оцінку мережі.

3.2.3 Критерії оцінки захищеності безпровідної мережі

Для реалізації ІБ безпровідної мережі використовуються засоби (механізми) захисту інформації. Для отримання критеріїв оцінки захищеності бездротової мережі пропонується метод, мета якого полягає в оцінці безпеки безпровідної мережі на основі використовуваних в ній засобів захисту інформації. Причому розглядаються тільки ті методи, які описані безпосередньо в стандартах 802.11 [13], тобто ми виключаємо механізми захисту, спрямовані на запобігання конкретних видів атак і включаються в систему захисту бездротової мережі додатково, наприклад, для запобігання атак на кшталт «хробака» (wormhole-атак), для боротьби з якими використовується або специфічне обладнання (наприклад, спрямовані антени) або розробляються спеціальні протоколи маршрутизації (LiteWorp або TIK). Для розробки системи критеріїв оцінки захищеності безпровідної мережі проведемо аналіз сімейства стандартів 802.11 в розрізі реалізованих в них механізмів захисту.

Як уже згадувалося вище, особливістю реалізації безпровідних мереж є відкритість каналів передачі інформації, так як фізично вони практично незахищені. Виходячи з цього, велика увага приділяється захисту інформації, що передається цими каналами.

На сьогоднішній день найкращим методом захисту даних є їх шифрування. Таким чином, можна сформувати першу групу критеріїв, які будуть оцінювати захищеність мережі з точки зору, реалізованих в ній криптографічних функцій. Але недостатньо просто обмежитися шифруванням трафіку. Алгоритм WEP, який використовувався на початковому етапі еволюції 802.11 має достатню кількість вразливостей [ ], і посилення його криптографічного стійкості за рахунок збільшення довжини ключа або вектора ініціалізації свідомо не може привести до належного рівня безпеки мережі. Отримавши НСД до каналу передачі даних безпровідної мережі, зловмисник може зчитати передану інформацію і надалі використовувати її в своїх цілях. Для запобігання НСД до переданому вже зашифрованого трафіку необхідно контролювати можливість доступу до самої мережі і її каналах зв'язку. Для цих цілей використовується ідентифікація користувачів і обладнання, яке підключається до мережі, їх

аутентифікація і авторизація.

Таким чином, можна виділити дві групи критеріїв, відповідно до яких і буде проведено дослідження засобів захисту, реалізованих в сімействі стандартів 802.11: криптографічні критерії; критерії аутентифікації.

В безпровідних мережах шифрування трафіку здійснюється за допомогою використання двох криптографічних алгоритмів. Спочатку в якості стандарту для бездротових мереж був прийнятий алгоритм WEP. Але після того, як було виявлено достатнє число його вразливостей, він був замінений на алгоритм AES. Відповідно першим критерієм при оцінці захищеності мережі є використовуваний в ній криптографічний алгоритм. Зміна алгоритму шифрування даних в стандарті 802.11 було досить тривалим процесом.

Оскільки використовуваний алгоритм вже не міг забезпечити належного рівня безпеки переданих даних, а новий ще не був схвалений в якості стандарту, було запропоновано збільшити довжину послідовності ключа. Це призвело до поліпшення криптостійкості шифру. З введенням в стандарт нового алгоритму AES можливість варіювати довжину ключа не зникла, що дозволило ранжувати рівень безпеки мережі в залежності від середовища її розгортання, використовуваного при її побудові обладнання та інших чинників.

Таким чином, другим критерієм при оцінці захищеності є довжина використовуваного при шифруванні ключа. Ті ж причини, які вплинули на застосування при шифруванні ключів різної довжини, привели і до використання динамічних ключів. Спочатку ключ був статистичним. Для реалізації такої властивості ІБ як цілісність в БМ використовуються спеціальні технології перевірки цілісності повідомлень. Вони представляють наступний критерій в групі криптографічних критеріїв. Належність технологій перевірки цілісності повідомлень саме до цієї групи критеріїв визначається криптографічного основою при побудові контрольних пакетів цілісності даних. Для підтримки останньої властивості ІБ, доступності, в бездротових мережах застосовуються засоби захисту спрямовані на контроль доступу до неї. Для їх структуризації виробимо ряд критеріїв аутентифікації.

Одним з найважливіших засобів захисту в даній сфері є протокол,

відповідно до якого і здійснюється розмежування доступу. Використовуваний протокол аутентифікації якраз і представляє перший і основний критерій в цій групі. Розвиток сімейства стандартів 802.11 як з точки зору криптографії, так і з точки зору аутентифікації відбувалося паралельно. Для поліпшення безпеки та посилення захисту мережі вводяться нові алгоритми. Найчастіше вони вже були реалізовані і широко використовуються в провідних мережах, але для їх адаптації до завдань бездротових з'єднань потрібно значно більше часу.

Найбільш захищеними прийнято вважати такі види мереж, як провідні, так і бездротові, в яких поряд з криптографічним захистом переданих даних реалізований також і криптографічний захист даних користувачів. Для безпровідних мереж подібна можливість була виражена за допомогою застосування, а згодом і закріплення в стандарті 802.11i, цифрових сертифікатів. Їх наявність або відсутність при побудові мережі значно впливає на її кінцеву захищеність. Таким чином, використання цифрових сертифікатів при доступі до безпровідних мереж варто включити в критерії аутентифікації в якості останнього критерію.

Підсумовуючи вищесказане було виділено ряд критеріїв для проведення аналізу, а згодом і оцінки захищеності бездротової мережі. Було отримано дві основні групи критеріїв, відповідно до яких і відбувається оцінка мережі: криптографічні критерії; критерії аутентифікації. Кожна група включає в себе ряд компонентів, зокрема криптографічні критерії: криптографічні алгоритми; довжина використовуваного ключа; використання динамічних або статичних ключів; технології перевірки цілісності повідомлень. Критерії аутентифікації: протокол; наявність сервера аутентифікації; використання цифрових сертифікатів. Завдяки отриманню цих груп критеріїв було проведено дослідження всіх можливих параметрів та механізмів безпеки бездротових мереж.

3.3 Дослідження логічних зв’язків в структурі механізмів захисту

Для ранжування механізмів захисту безпровідної мережі по виробленим

рівнями довіри необхідно проаналізувати сімейство стандартів 802.11 за критеріями оцінки захищеності, отриманим під другому розділі. В результаті аналізу передбачається отримати повний структурований набір механізмів захисту, які описуються стандартах для безпровідних мереж.

Спочатку дослідимо механізми захисту, покликані забезпечити мережу з точки зору захисту переданих даних. Для цих цілей проаналізуємо сімейство стандартів за допомогою криптографічних критеріїв. Основоположним механізмом в цій сфері є криптографічний алгоритм, який використовується для шифрування переданого трафіку.

На початку становлення безпровідних технологій, усі цілі задовольняв алгоритм WEP, який використовується спільно з 40-бітовим роздільним ключем. Пізніше для посилення його криптостійкості стали використовувати вже 128-бітний ключ, в той час як сам алгоритм залишився колишнім.

В стандарті 802.11i вводиться новий алгоритм AES, який володіє значно більшою криптостійкістю в порівнянні з попередником. Але посилення захисних властивостей алгоритму призводить до значного збільшення ресурсоємності обладнання для розгортання безпровідних мереж. Саме тому на перших етапах впровадження алгоритму AES також застосовується 128-бітовий ключ. Але в стандарті відразу ж закладається можливість подальшого розширення, і алгоритм AES можна використовувати як зі 192- бітовим ключем, так і зі 256-бітовим.. Коли безпровідні мережі тільки почали з'являтися на ринку мережевих технологій, статичний ключ цілком задовольняв поставленим цілям безпеки. Але пропорційно зростанню популярності бездротового зв'язку збільшуються і вимоги кінцевих користувачів до рівня безпеки, який можуть забезпечити подібні з'єднання. На рівні з збільшенням довжини ключа застосовується методика його періодичної зміни, ключ стає динамічним.

Для перевірки цілісності переданих повідомлень в стандартах сімейства 802.11 описуються два протоколи: MIC і CCMP.

Таким чином, було отримано повний набір механізмів захисту безпровідної мережі у відповідності до криптографічних критеріїв.

Логічну структуру криптографічних механізмів наведено на рисунку 3.8.

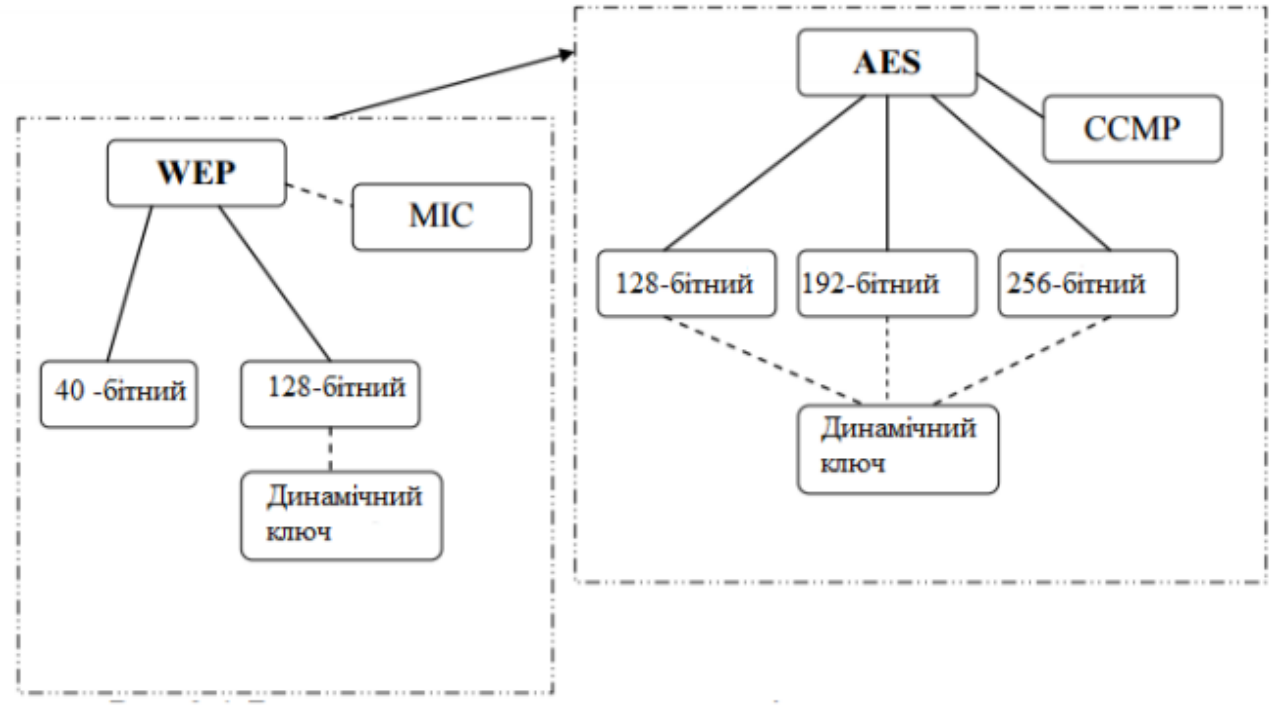

Рисунок 3.8 – Логічна структура криптографічних механізмів захисту безпровідної мережі

Узагальнивши дані по всіх можливих реалізаціях криптографічних механізмів захисту в безпровідних мережах, отримуємо наступне (див. табл.3.4).

Таблиця 3.4 – Співвідношення криптографічних механізмів захисту при використанні алгоритмів WEP та AES

Ключ	Цілісність	AES-128	AES-192	AES-256	WEP-40	WEP-128
Статичний	Є перевірка цілісності	+	+	+		+
	Немає перевірки цілісності	+	+	+	+	+
Динамічний	Є перевірка цілісності	+	+	+		+
	Немає перевірки цілісності	+	+	+		+

Для WEP отримуємо 5 можливих варіантів.

Для AES отримуємо 12 можливих варіантів.

Тепер будемо досліджувати механізми захисту, спрямовані на контроль доступу до безпровідної мережі. При аналізі сімейства стандартів 802.11 скористаємося отриманими критеріями аутентифікації. Якщо з точки зору криптографічного захисту даних алгоритм шифрування є основним критерієм, то

з точки зору захисту доступу до мережевих ресурсів основним критерієм для оцінки є протокол аутентифікації, реалізований в об’єкті оцінки. У даній сфері теж досить-таки яскраво простежується поступальна динаміка посилення захисних властивостей протоколу з розвитком бездротових технологій.

На ранніх етапах використовувалися примітивні схеми аутентифікації, як: аутентифікація з відкритим або загальним ключем. Перша, як вже згадувалося вище, по суті, не є як таким алгоритмом аутентифікації, а друга - лише незначно посилює першу за рахунок шифрування переданої службової інформації. Повноцінні протоколи аутентифікації з'являються пізніше, після того, як було знайдено і обгрунтовано невідповідність можливостей WEP постійно розростаючому колі завдань безпровідної мережі.

Розробляється сімейство протоколів EAP. Його різноманіття пояснюється тим, що виробники бездротового обладнання впроваджували свою версію протоколу в залежності від свого бачення майбутнього розвитку технологій. На сьогоднішній день використовується п'ять основних протоколів даного сімейства, кожен з яких підсилює властивості попереднього: EAP-MD5, LEAP, EAP-TLS, PEAP, EAP-TTLS. Але захист бездротового зв'язку не обмежується лише схемою аутентифікації користувача в мережі. Для досягнення більш високих показників в цій області вводяться додаткові механізми захисту. Починаючи з реалізації протоколу LEAP, в структуру рішення по забезпечення захисту від НСД вводять сервер аутентифікації, який забезпечує додаткові можливості розмежування прав користувача при роботі в мережі.

Також в якості додаткових механізмів захисту можна розглядати і використання цифрових сертифікатів (починаючи з реалізації протоколу EAPTLS) для верифікації наданої користувачем інформації. Варто відзначити, що при реалізації протоколу EAP-TLS використання цифрових сертифікатів є обов'язковим умовою, в той час як в наступних протоколах сімейства EAP - лише додатковою опцією. За аналогією з криптографічними засобами захисту інформації складемо зведену таблицю всіх можливих наборів механізмів захисту, спрямованих на контроль доступу до мережі (табл. 3.5).

Таблиця 3.5 – Співвідношення криптографічних механізмів захисту при використанні алгоритму WEP

Протокол аутентифікації	Сервер аутентифікації		Цифрові сертифікати
	Відсутня	Взаємна аутентифікація	
З відкритим ключем	–		–
З закритим ключем	–		–
EAP-MD5		–	–
LEAP		+ / –	–
EAP-TLS		+ / –	+
PEAP		+ / –	+ / –
EAP-TTLS		+ / –	+ / –

Підрахунок дає 15 можливих варіантів реалізації.

Таким чином, в частині криптографічної оцінки захищеності мережі ми маємо 17 можливих сукупних реалізацій механізмів захисту інформації, в той час як в частині аутентифікації - 15.

3.4 Технології захисту передачі даних та доступу до мережі Wi-Fi

Використання технології WEP. Процес шифрування WEP виконується у два етапи. Спочатку підраховується контрольна сума (Integrity Checksum Value - ICV) із застосуванням алгоритму Cyclic Redundancy Check (CRC-32), що додається в кінець незашифрованого повідомлення та служить для перевірки його цілісності прийнятою стороною. На другому етапі здійснюється безпосередньо шифрування. Ключ для WEP-шифрування - загальний секретний ключ, що повинні знати пристрої на обох сторонах бездротового каналу передачі даних. Цей секретний 40-бітний ключ разом з випадковим 24-бітним вектором ініціалізації є вхідною послідовністю для генератора ПВЧ, що базується на шифрі Вернама для генерації рядка випадкових символів, називаної ключовим потоком (key stream). Дана операція виконується з метою запобігання методів злому, заснованих на статистичних властивостях відкритого тексту.

Вектор ініціалізації використовується, щоб забезпечити для кожного

повідомлення свій унікальний ключ. Зашифроване повідомлення утвориться в результаті виконання операції XOR над незашифрованим повідомленням з ICV і ключовим потоком. Щоб одержувач міг прочитати його, у переданий пакет у відкритому виді додається вектор ініціалізації. Коли інформація приймається на іншій стороні, виробляється зворотні процеси ($p=c \cdot b$). Значення b одержувач обчислює, застосувавши код Вернама до вхідної послідовності, що складає із ключа К (якого він знає заздалегідь) і вектор ініціалізації, що пришли цим же повідомленням у відкритому виді. Для кожного чергового пакету процес повторюється з новим обраним значенням вектором ініціалізації.

До числа відомих властивостей алгоритму RC4 відноситься те, що при використанні того самого значення ключа й вектора ініціалізації ми завжди будемо одержувати однакове значення b, отже, застосування операції XOR до двох текстів, зашифрованим RC4 за допомогою того ж значення b, являє собою не що інше, як операцію XOR до двох початкових текстів. Таким чином, ми можемо одержати незашифрований текст, що є результатом операції XOR між двома іншими оригінальними текстами. Процедура їхнього добування не становить великої праці. Наявність оригінального тексту й IV дозволяє обчислити ключ, що надалі дасть можливість читати всі повідомлення даної бездротової мережі.

Після нескладного аналізу можна легко розрахувати, коли повториться b. Тому що ключ К постійний, а кількість варіантів IV становить 224=16 777 216, то при достатнім завантаженні крапки доступу, середньому розмірі пакета в бездротовій мережі, рівний 1500 байт (12 000 біт), і середньої швидкості передачі даних, наприклад 5 Mbps (при максимальній 11 Mbps), ми одержимо, що крапкою доступу буде передаватися 416 повідомлень у секунду, або ж 1 497 600 повідомлень у годину, т. е. повторення відбудеться через 11 год 12 хв (224/1 497 600=11,2 год).

Дана проблема зветься "колізія векторів". Існує велика кількість способів, що дозволяють прискорити цей процес. Крім того, можуть застосовуватися атаки "з відомим простим текстом", коли одному з користувачів мережі посилає повідомлення із заздалегідь відомим змістом і прослуховується зашифрований

трафік. У цьому випадку, маючи три складові із чотирьох (незашифрований текст, вектор ініціалізації й зашифрований текст), можна обчислити ключ.

У згадуваній вище роботі "Intercepting Mobile Communications: The Insecurity of 802.11" була описана безліч типів атак, включаючи досить складні, що використають маніпуляції з повідомленнями і їхньою підміною, засновані на ненадійному методі перевірки цілісності повідомлень (CRC-32) і аутентифікації клієнтів. З ICV, використовуваним в WEP-алгоритмі, справи йдуть аналогічно. Значення CRC-32 підраховується на основі поля даного повідомлення. Це гарний метод для визначення помилок, що виникають при передачі інформації, але він не забезпечує цілісність даних, тобто не гарантує, що вони не були підмінені в процесі передачі. Контрольна сума CRC-32 має лінійну властивість:
CRC(A XOR B)=CRC(A)XOR CRC(B), що надає порушникові можливість легко модифікувати зашифрований пакет без знання WEP-ключа та перерахувати для нього нове значення ICV.

У 2001 році з'явилася специфікація WEP2, що збільшила довжину ключа до 104 біт, не вирішила проблеми, тому що довжина вектора ініціалізації й спосіб перевірки цілісності даних залишилися колишніми.

Використання технологій WPA / WPA2 та 802.1x та їх порівняння. Протокол IEEE 802.1x, що є стандартом із серпня 2001 р., забезпечує контроль доступу на рівні портів. Основна його ідея полягає в тім, що розблокування мережного порту й забезпечення доступу клієнта до мережі відбувається тільки після успішної аутентифікації, що виконується на другому рівні моделі OSI. 802.1x може використатися разом із протоколами більше високих рівнів для генерації й керування ключами шифрування.

802.1x використає протокол EAP (Extensible Authentication Protocol), що споконвічно розроблявся для роботи поверх PPP (Point-to-Point Protocol) для передачі повідомлень між трьома учасниками аутентифікації у ЛОМ-середовищі. Цей вид інкапсуляції відомий як EAP over LANs, або EAPOL. EAP не можна назвати методом аутентифікації. Він визначає основну протокольну структуру для вибору специфічного методу аутентифікації. При використанні

EAP аутентифікатору не потрібно "розуміти" деталі різних методів

аутентифікації. У цьому випадку він виступає тільки як проміжна ланка, що переупаковує EAP-пакети при їхньому проходженні між саплікантом (supplicant - об'єкт на кінці сегмента "точка--точка", якому необхідна аутентифікація: це може бути клієнтське ПО на комп'ютері, PDA або іншому бездротовому пристрої) і сервером аутентифікації. Така технологія надає розроблювачам можливість вибору між різними видами аутентифікації, що є безсумнівною перевагою. Хоча для протоколу EAP на сьогоднішній день є вже більше десяти різних методів аутентифікації, найбільш широке поширення одержали три:

- Message Digest 5 (MD5) -і процедура однобічної аутентифікації сапліканта сервером аутентифікації, заснована на застосуванні хеш-суми MD5 імені користувача й пароля як підтвердження для сервера RADIUS. Даний метод не підтримує ні керування ключами, ні створення динамічних ключів. Тим самим виключається його застосування в стандарті 802.11і й WPA.

- Transport Layer Security (TLS) - процедура аутентифікації, що припускає використання цифрових сертифікатів X.509 у рамках інфраструктури відкритих ключів (Public Key Infrastructure - PKI). EAP-TLS підтримує динамічне створення ключів і взаємну аутентифікацію між саплікантом і сервером аутентифікації. Недоліком даного методу є необхідність підтримки інфраструктури відкритих ключів.

- Tunneled TLS (TTLS) -і EAP, розроблений компаніями Funk Software і Certicom і розширювальної можливості EAP-TLS. EAP-TTLS використає безпечне з'єднання, установлене в результаті TLS-квотування для обміну додатковою інформацією між саплікантом і сервером аутентифікації.

IEEE 802.11x визначає три основних компоненти в мережному оточенні:

- Саплікант.

- Сервер аутентифікації (authentication server) - об'єкт, що забезпечує служби аутентифікації. У стандарті чітко не визначено, що повинне виступати як сервер аутентифікації, але, як правило, їм є сервер RADIUS (Remote Access Dial In User Service).

- Аутентифікатор (authenticator) - об'єкт на кінці сегмента "точка - точка" локальної обчислювальної мережі, що сприяє аутентифікації об'єктів. Це

пристрій-посередник, розташований між сервером аутентифікації і саплікантом. Звичайно його роль виконує бездротова точка доступу.

Аутентифікація в 802.1x включає кілька кроків. Конкретна схема обміну EAP-кадрами залежить від обраного способу аутентифікації. В одному з найпростіших варіантів (OTP - One Time Password) даний процес виглядає в спосіб показаний на рис.3.9:

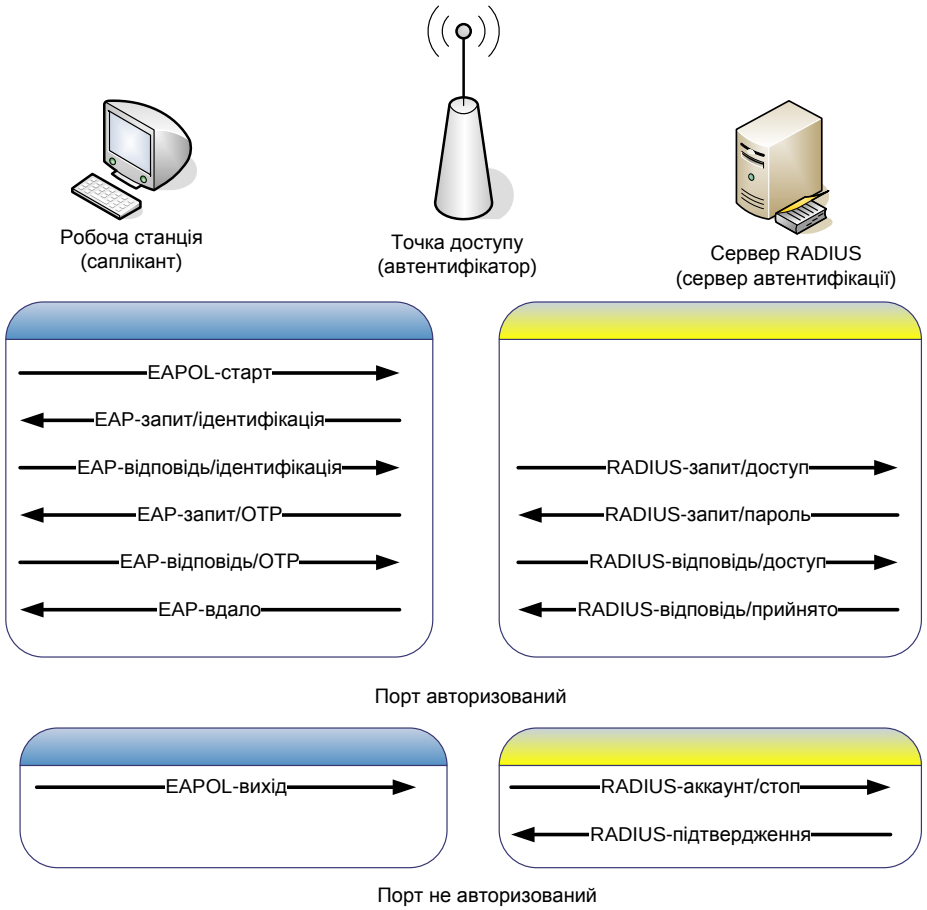

Рисунок 3.9 – Схема аутентифікації користувача стандарту 802.11x

1. Саплікант ініціює з'єднання з аутентификатором.

2. Аутентифікатор вимагає ідентифікаційну інформацію про саплікант.

3. Саплікант відсилає ідентифікаційну інформацію аутентификатору, що відправляє її серверу аутентифікації.

4. Сервер аутентифікації запитує в аутентификатора інформацію, що підтверджує дійсність сапліканта. Аутентифікатор пересилає запит сапліканту.

5. Саплікант передає інформацію, що підтверджує його дійсність, аутентификатору. Аутентифікатор відправляє її серверу аутентифікації.

6. Сервер аутентифікації перевіряє інформацію про дійсність сапліканта й у випадку успішної аутентифікації посилає спеціальне повідомлення аутентификатору, що відкриває порт для доступу сапліканту й відправляє йому повідомлення про завершення процесу аутентифікації.

Temporal Key Integrity Protocol (TKIP) - другий протокол, передбачений специфікацією WPA. TKIP призначений для рішення основних проблем WEP в області шифрування даних. Для сумісності з існуючим апаратним забезпеченням TKIP використає той же алгоритм шифрування, що й WEP - RC4. TKIP має на увазі кілька способів підвищення захищеності бездротових мереж: динамічні ключі, змінений метод генерації ключів, надійніший механізм перевірки цілісності повідомлень, збільшений по довжині вектор ініціалізації.

На відміну від WEP, де для контролю цілісності переданих даних використовувався CRC-32, TKIP застосовує так званий Message Integrity Code (MIC), що забезпечує криптографічну контрольну суму від декількох полів (адреса джерела, адреса призначення та поля даних). Тому що класичні MIC-алгоритми для існуючого бездротового устаткування були дуже "важкими" і вимагали більших обчислювальних витрат, спеціально для використання в бездротових мережах був розроблений алгоритм Michael. Для шифрування він застосовує 64-бітний ключ і виконує дії над 32-бітними блоками даних. MIC включається в зашифровану частину фрейму між полем даних і полем IV.

При аутентифікації за допомогою протоколу IEEE 802.1x на основі заздалегідь визначеної інформації, відомої сапліканту й серверу аутентифікації (наприклад, сертифікат, ім'я користувача, пароль і т.д. - залежить від способу аутентифікації), генерується майстер-ключ (Master Key - MK), за допомогою якого вони роблять взаємну аутентифікацію. Далі на підставі MK саплікант і сервер аутентифікації генерують парний MK (Pairwise Master Key - PMK), а потім сервер аутентифікації передає (не копіює) його аутентифікатору. Одержання аутентификатором PMK є останнім етапом у процесі EAP-аутентифікації, після чого сервер аутентифікації посилає аутентификатору пакет

"відповідь/прийнята" (RADIUS/Accept), а аутентифікатор сапліканту -"успішно" (EAP/Success). PMK не використається для операції безпосереднього шифрування й дешифрування даних, він застосовується для генерації цілої групи ключів.

Після одержання саплікантом й аутентифікатором PMK вони роблять взаємну аутентифікацію й генерацію парного тимчасового ключа (Pairwise Transient Key - PTK). Генерація PTK відбувається такі етапи:

У першому повідомленні аутентифікатор посилає сапліканту випадкові дані. Саплікант поєднує випадкові дані аутентифікатора зі своїми власними випадковими даними і застосовує ці дані для генерації PTK. Далі саплікант підраховує значення Message Integrity Check (MIC) від тіла другого повідомлення і перших 128 біт ключа PTK.

У другому повідомленні саплікант посилає випадкові дані та MIC аутентифікатору, що також генерує PTK і потім використає його для перевірки значення MIC, отриманого в другому повідомленні. Якщо помилок не виявлено, аутентифікатор відправляє сапліканту повідомлення про застосування PTK. У четвертому повідомленні саплікант підтверджує аутентифікатору використання даного ключа.

PTK є складовим. Біти з 0 по 127 являють собою ключ підтвердження ключа (Key Confirmation Key - KCK), застосовуваного для шифрування нового сесійного ключа (PMK) при його наступній зміні. Біти з 128 по 255 приділяються для ключа шифрування ключа (Key Encryption Key - KEK), що використається для поширення групового тимчасового ключа (Group Transient Key - GTK). Біти з 256-го й вище можуть мати специфічну структуру, що залежить від методу шифрування, і являють собою тимчасовий ключ (Temporal Key - TK), застосовуваний для шифрування даних.

GTK - це ключ, призначений для шифрування групового і широкомовного трафіку. Він генерується із групового МК (Group Master Key - GMK), що, у свою чергу, є похідним МК. Поширення GTK відбувається у два етапи, на відміну від чотирьох у випадку з PTK, тому що його доставка виконується через безпечне з'єднання після того, як передані всі парні ключі, і аутентифікація в цьому

випадку не потрібно. При відключенні одного із клієнтів від мережі здійснюються генерація нового ключа GTK і його поширення клієнтам, що залишилися.

TK також може бути складовим, і його частина або він повністю разом з MAC-адресою джерела (Transmitter Address - TA) і вектором ініціалізації (IV) є вхідними даними для двофазової функції мікшування, що генерує пакетні ключі (Per-packet Key -і PK) довжиною 128 біт як показано на Рис.3.10.

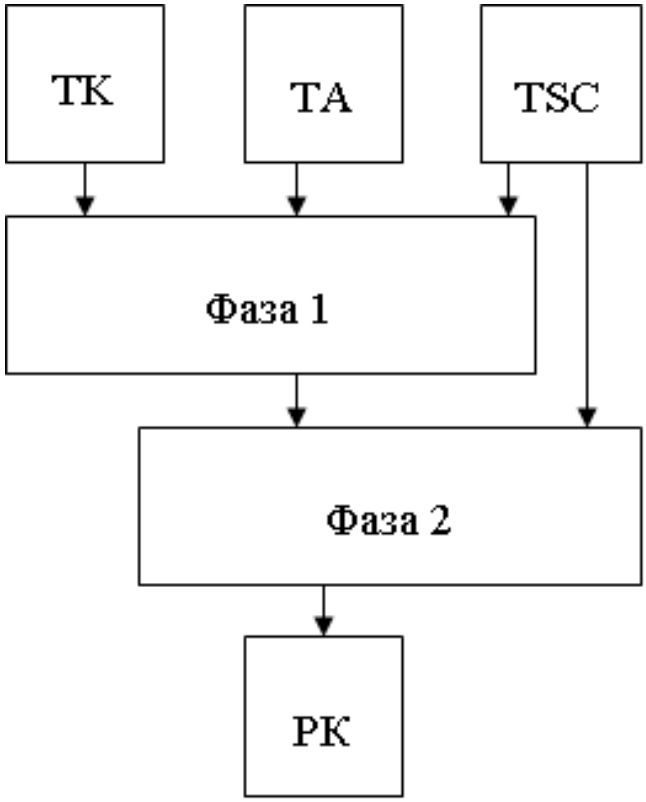

Рисунок 3.10 – Процес формування пакетного ключа.

Введення у функцію мікшування такого параметра, як TA, дозволяє уникнути атак з використанням підставних об'єктів. Для домашнього застосування й невеликих офісів, де, як правило, відсутній сервер аутентифікації, специфікація WPA передбачає режим використання загального ключа (Pre-Shared Key -і PSK). У цьому випадку PMK вводиться вручну на саплікант і аутентифікаторі. В іншому процедура генерації ключів залишається незмінною.

WPA2 побудований на основі попередньої версії WPA, що також використовує елементи 802.11i.

Основні подібності та відмінності протоколів наведено в таблиці 3.6.

Таблиця 3.6 – Порівняння протоколів доступу до мережі Wi-Fi

Протокол	Open System	Shared Key	WPA-PSK	WPA-EAP	WPA2-PSK	WPA2-EAP
Алгоритм шифрування	RC4	RC4	RC4	RC4	AES (CTR)	AES (CTR)
Аутентифікація	Відсутня	Preshared Key	Preshared Key	IEEE 802.1x	Preshared Key	IEEE 802.1x
Довжина ключа, біт	64 або 128	64 або 128	128 (шифрув.), 64 (аутент.)	128 (шифрув.), 64 (аутент.)	128	128
Повторюваність ключа	24-бітовий IV	24-бітовий IV	48-бітовий TSC	48-бітовий TSC	48-бітовий PN	48-бітовий PN
Цілісність даних	CRC-32	CRC-32	Michael	Michael	AES (CBC-MAC)	AES (CBC-MAC)
Цілісність заголовка	Відсутня	Відсутня	Michael	Michael	AES (CBC-MAC)	AES (CBC-MAC)
Керування ключами	Статичні для всієї мережі			На основі EAP	Статич. для всієї мережі	На основі EAP

3.5. Висновки до розділу

В цьому розділі практично досліджено модель проведення аудиту захищеності безпровідних мереж, запропоновано профіль захисту для мереж стандарту 802.11, описано логічні зв’язки в структурі механізмів захисту. Досліджено використання технологій захисту передачі даних та доступу до мережі Wi-Fi.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Встановлення та налаштування сервера контролю безпечного доступу ACS

Після встановлення Cisco Secure Access Control Server версії 4.1, виконати вхід на нього можна за допомогою будь-якого браузера (Internet Explorer 5 та вище, Opera, Mozilla та ін.), в рядку адреси потрібно ввести http://ip_address_ACS:2002 , де ip_address_ACS - IP-адреса серверу на який було встановлено CS ACS 4.1. Вигляд вікна входу на сервер ACS 4.1 показаний на рис. 4.1.

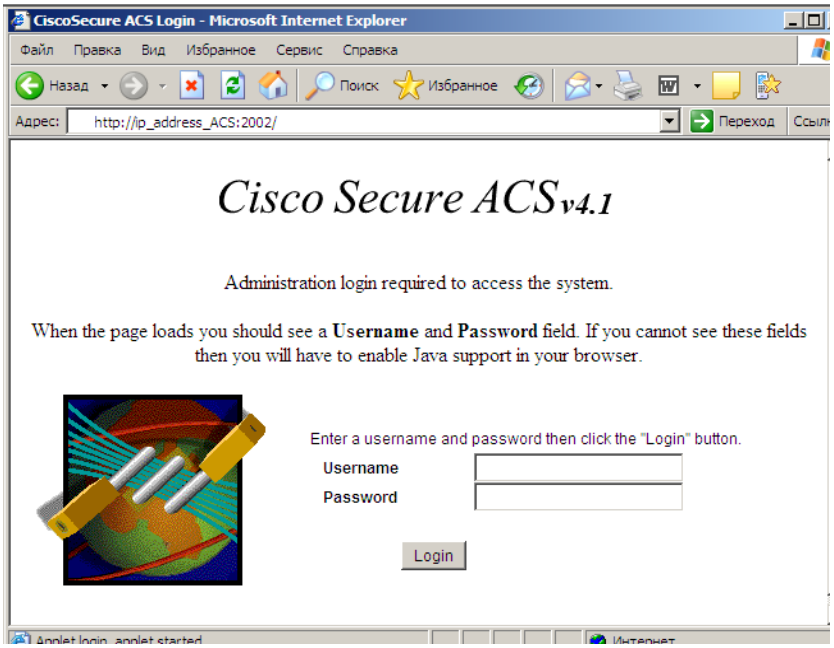

Рисунок 4.1 – Вигляд вікна входу на сервер ACS 4.1

Після вдалої аутентифікації на сервері, сервер автоматично переадресує на сторінку управлянні сервером через веб-інтерфейс, при цьому буде автоматично змінено номер порту, по якому працює сервер.

Через веб-інтерфейс серверу можна отримати доступ до таких пунктів меню:

User Setup – в цьому пункті меню створюються користувачі, настроюються їх права доступу на мережне обладнання, рівні превілегій з якими користувачі

можуть авторизуватись на обладнанні. Також є можливість використовувати базу даних користувачів взяту з Active Directory.

Приклад створення користувача показаний на рис.4.2.

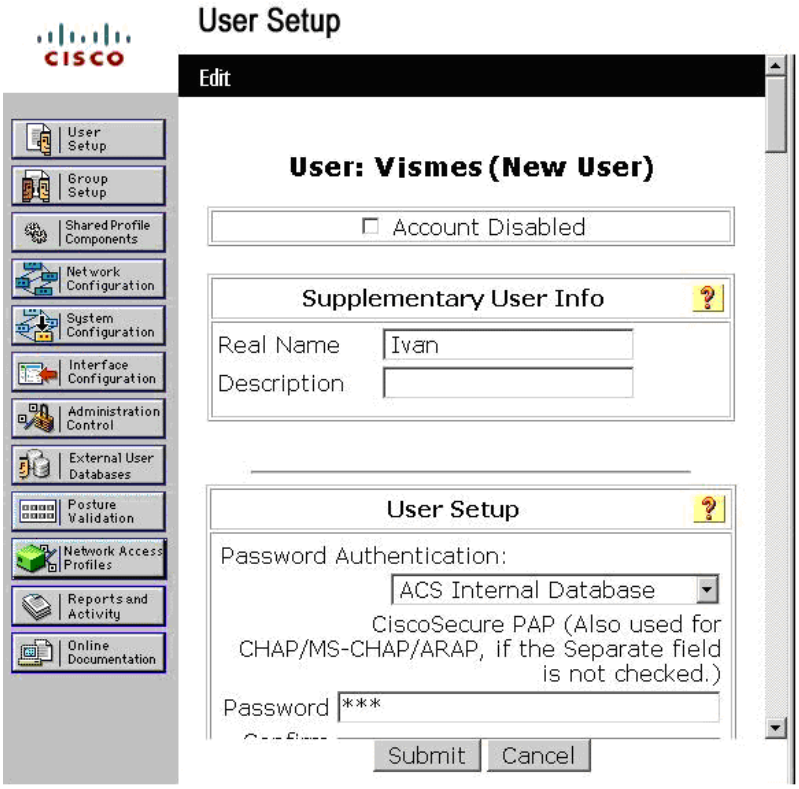

Рисунок 4.2 – Створення користувача в системі ACS

Group Setup – тут створюються та редагуються групи, наприклад в одну групу можна віднести користувачів які мають виконувати схожі функції, або належать одній організації. Параметри з даного меню розповсюджуються на всю групу.

Shared Profile Components – в даному меню конфігуруються параметри авторизації для користувачів, якщо зміни в конфігурацію вносити не варто, то цей пункт можна не використовувати. Взагалі в цьому меню створюються списки доступу, що застосовуються до користувачів в т.ч. доступ на такі пристрої як PIX, ASA – фаєрволи.

Network Configuration – саме в цьому меню задаються параметри для пристроїв на яких буде проходити аутентифікація, обов’язковими полями є ім’я пристрою – в системі ACS пристрій буде відомий під іменем заданим в даному

полі; IP-адрес – один або декілька адрес пристрою; ключ – секретний ключ, що має співпадати з ключем який буде вказано при конфігурації Wi-Fi пристрою для обміну сеансовими ключами та шифрування подальшого трафіку, та вибір серверу з переліку TACACS+ чи RADIUS. Вигляд вікна створення запису для Wi-Fi пристрою в системі ACS представлений на рис.4.3.

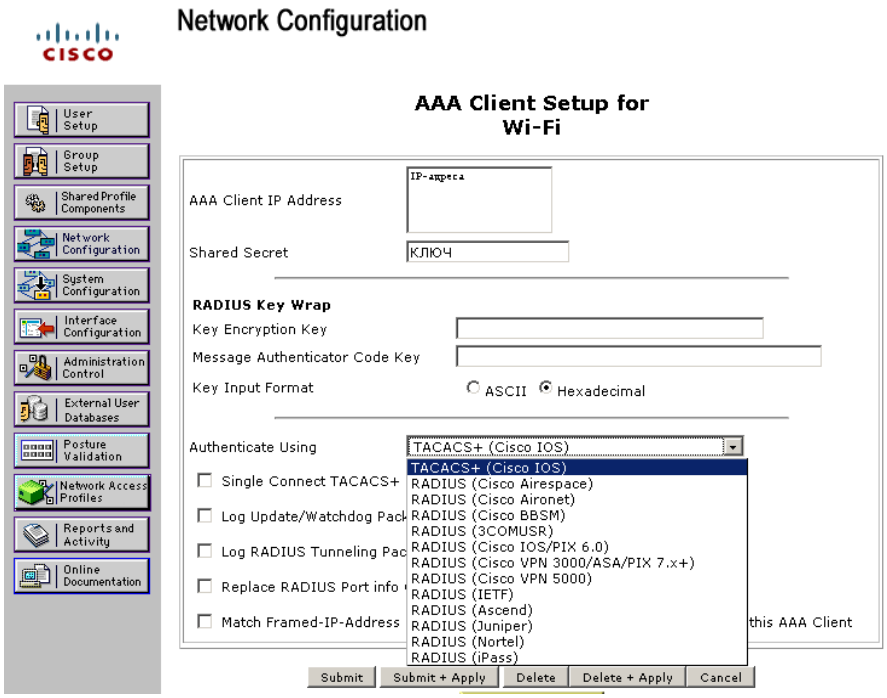

Рисунок 4.3 – Створення запису для Wi-Fi пристрою.

Reports and Activity – в даному меню знаходиться велика кількість журналів зокрема: Аудит TACACS+ (як початок та кінець роботи з Wi-Fi пристроєм, так і введені команди); аудит RADIUS – початок та кінець сесії користувача; користувачі, що пройшли аутентифікацію, та невдалі спроби входу, в усіх випадках зазначається IP-адреса з якої виконувався вхід, імя користувача який виконував вхід та група до якої належить користувач, IP-адреса пристрою на який виконувався вхід, та ім’я пристрою в системі.

При спробі аутентифікуватися на Wi-Fi пристрою з IP-адресою 10.0.110.2 та випадково двічі неправильно ввести пароль відповідні записи будуть зроблені в файлах аудиту ACS, процес аутентифікації та аудиту зображено на рис. 4.4 та 4.5.

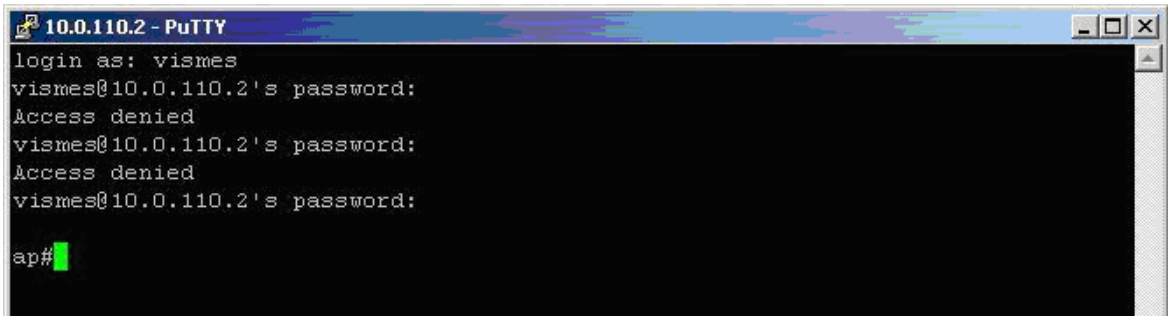

Рисунок 4.4 – Вхід на точку доступу за допомогою утиліти telnet

Рисунок 4.5 – Перегляд записів аудиту, та виявлення невдалих спроб входу

Приклад введення декількох команд на точці доступу (див. рис.4.6), та моніторинг їх через програмний продукт ACS (див. рис.4.7).

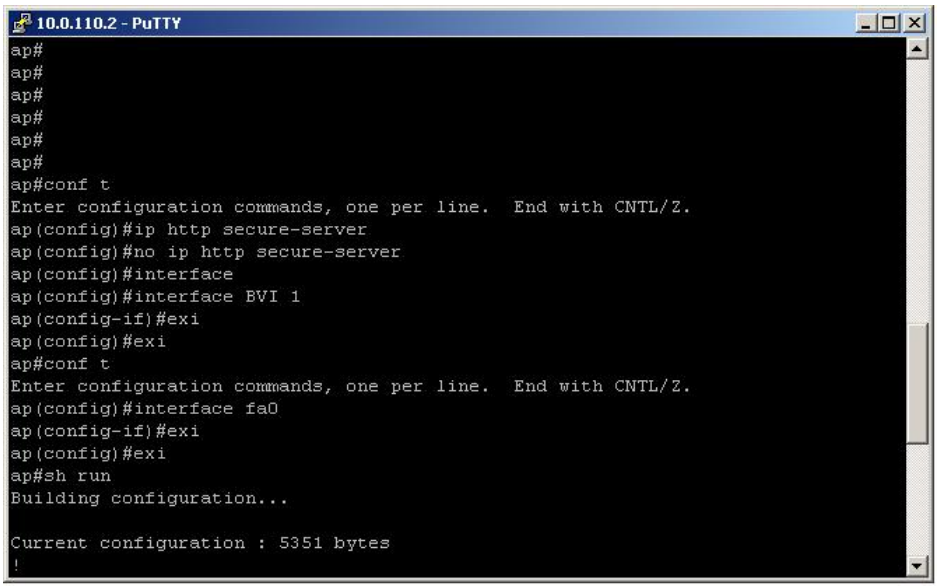

Рисунок 4.6 – Конфігурування точки доступу через командний інтерфейс

Date ↓	Time	User-Name	Group-Name	cmd	priv-lvl
11/23/2019	16:19:25	vismes	Administrators	ip http secure-server <cr>	15
11/23/2019	16:19:24	vismes	Administrators	no ip http secure-server <cr>	15
11/23/2019	16:19:10	vismes	Administrators	interface BVI 1 <cr>	15
11/23/2019	16:19:08	vismes	Administrators	configure terminal <cr>	15
11/23/2019	16:17:13	vismes	Administrators	interface FastEthernet 0 <cr>	15
11/23/2019	16:17:03	vismes	Administrators	show running-config <cr>	15

Рисунок 4.7 – Перегляд введених команд користувачем, за допомогою веб-інтерфейсу програмного продукту ACS

4.2 Конфігурування точки доступу Wi-Fi для аутентифікації через ACS

Після підключення точки доступу до дротової мережі чи мережі Wi-Fi, вона стає доступною для конфігурації декількома методами, насамперед через web-інтерфейс – найбільш легкий та популярний метод конфігурації зрозумілий більшості користувачів. Також конфігурування точки доступу можливе через командний інтерфейс, який надає більше можливостей та вимагає базових знань операційної системи Cisco IOS від адміністраторів. Тобто для конфігурування можна використовувати протоколи : http, https, telnet та ssh.

Можливий варіант коли необхідно виконати процедуру повернення паролю, чи коли потрібно змінити адресу інтерфейсу з якого був виконаний вхід можна використовувати консольний інтерфейс, для цього необхідний фізичний доступ до Wi-Fi-точки та консольний кабель.

Після виконання настроювань з боку серверу захисту ACS, Wi-Fi-точка для роботи з сервером TACACS+ конфігурується наступним чином:

За допомогою командного інтерфейсу Wi-Fi-пристрою, після аутентифікації потрібно перейти в режим глобальної конфігурацію, використавши команду `configure terminal`.

Наступною командою дозволяємо використовувати аутентифікацію,

авторизацію та аудит з віддаленою базою захисту: *aaa new-model*

Створений запис означає що аутентифікація буде проходити по списку ACS за допомогою серверу TACACS+, в разі недоступності серверу, аутентифікація буде виконана на основі локальної бази даних.

aaa authentication login ACS group tacacs+ local

Наступна команда означає що аутентифікація для привілейованого режиму(режим без обмежень) проходить на основі бази даних серверу TACACS+, у випадках коли сервер не доступний, користувачу буде запропоновано ввести пароль на привілейований режим, що зберігається в локальній базі даних.

aaa authentication enable default group tacacs+ enable

Наступний запис означає, що авторизація користувачів буде проходити на сервері TACACS+, якщо сервер не доступний то локально, якщо локальної бази розмежування прав доступу немає, користувач авторизується так як він вже аутентифікований.

aaa authorization exec default group tacacs+ local if-authenticated

Наступні дві команди відповідають за аудит який відбувається на сервері TACACS+, тобто кожен початок та кінець роботи користувача та всі введенні ним команди.

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

Також необхідно визначити IP-адресу на якій знаходиться сервер TACACS+, робиться це за допомогою команди: *tacacs-server host IP-адреса_серверу*.

Після вказування адреси серверу необхідно вказати ключ, такий же як на сервері ACS за допомогою команди: *tacacs-server key ключ*

Після введення вищевказаних команд, необхідно «прив’язати» список ACS, що був створений раніше до ліній vty, для цього потрібно ввести наступну команди:

line vty номер_лінії

login authentication ACS

Номер лінії може бути від нуля до п’ятнадцяти, що значить максимально п'ятнадцять користувачів можуть одночасно конфігурувати Wi-Fi-точку.

Також налаштувати авторизацію, аутентифікацію та аудит можна використовуючи веб-інтерфейс. Після вдалої аутентифікації через веб-браузер на Wi-Fi-точці, необхідно в меню вибрати пункт SECURITY та в ньому підпункт Server Manager.

На вкладниці Corporate Servers відображаються сервери захисту RADIUS та TACACS+, де також є можливість створити новий сервер захисту, задавши його адресу та ключ доступу. За бажанням можна змінити порт для аудиту чи аутентифікації . Також налаштувати аутентифікацію, авторизацію та аудит для адміністраторів точки-доступу, та аутентифікацію користувачів Wi-Fi мережі шляхом вибору у необхідному стовпчику адресу серверу з списку серверів, також є можливість вибору резервних (до трьох) серверів у випадку не доступності основного. Вигляд процесу конфігурування точки доступу через веб-інтерфейс представлений на рис. 4.8.

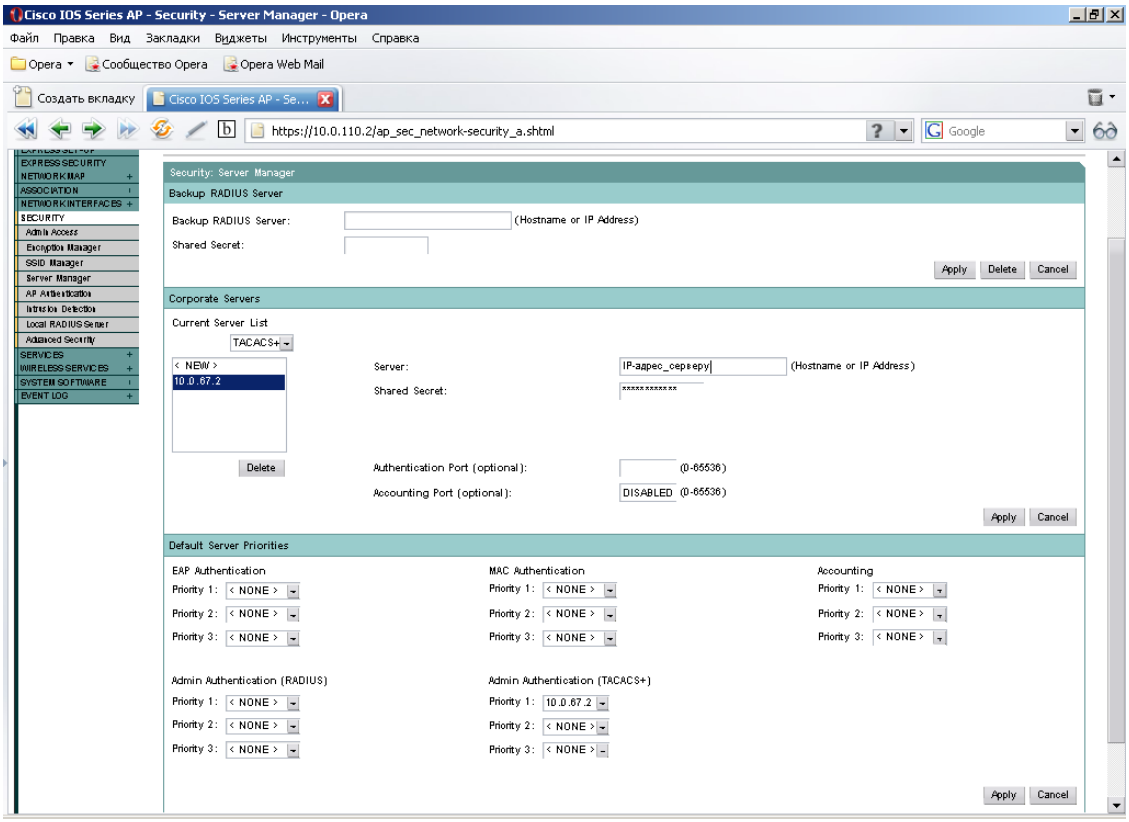

Рисунок 4.8 – Конфігурування Wi-Fi-точки доступу для аутентифікації через сервер ACS

4.3 Висновки до розділу

В даному розділі дипломної роботи описано процеси встановлення та налаштовування сервера контролю безпечного доступу ACS, а також конфігурування точки доступу Wi-Fi для аутентифікації через описаний сервер.

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою дипломної роботи є реалізація комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі (на основі раніше досліджених технологій та методів захисту).

Головною метою розділу є обґрунтування економічної ефективності впровадженої даної розробки.

Щоб виконати оцінку економічної ефективності необхідно розрахувати трудомісткість реалізації проекту, витрати на оплату праці найманим працівникам, витрати апаратного і програмного забезпечення, амортизаційні відрахування, витрати енергоресурсів та інші витрати які є основними пунктами виконання обчислень, а також показники економічної ефективності розробки проекту.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Реалізація проекту комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі складається з низки послідовних та взаємопов’язаних етапів.

Кожен із етапів реалізації проекту характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Реалізація проекту комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі складається із підготовчого етапу, етапу технічної пропозиції, створення технічного завдання, проектування системи, практичної реалізації, тестування, верифікації та заключного етапу.

Норми часу на виконання науково-дослідницької роботи розраховуватимуться на основі середнього часу виконання стадії в годинах, що наведені в таблиці 5.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовча стадія	Проектний менеджер	10
		Інженер-програміст	
2	Технічна пропозиція	Проектний менеджер	10
		Інженер-програміст	
3	Створення технічного завдання	Проектний менеджер	20
		Інженер-програміст	
4	Проектування системи	Інженер-програміст	20
5	Практична реалізація	Інженер-програміст	135
6	Тестування системи	Тестувальник	20
7	Верифікація системи	Тестувальник	20
		Інженер-програміст	
		Проектний менеджер	
8	Створення документації	Інженер-програміст	20
9	Заключна стадія	Проектний менеджер	10
Разом			265

В підсумку на реалізацію комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі необхідно 265 людино-годин, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу, ставки в годину чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці. Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами. Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Наймані працівники для розробки комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі працюють згідно контракту, який в якому вказано їхню погодинну ставку. Тобто розрахунок заробітної плати працівників відбуватиметься на базі тарифної ставки та кількості відпрацьованих годин.

У штаті найманих працівників для розробки залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу реалізації комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі:

– Проектний менеджер – 150 грн./год.

– Інженер-програміст – 130 грн./год.

– Тестувальник – 100 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \bullet К_г , \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою (5.1);

$$З_{осн.} = 150 \cdot 35 + 130 \cdot 200 + 100 \cdot 30 = 34250 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати й визначається за формулою (5.2).

Коефіцієнт додаткових виплат працівникам становить 0,1.

$$Здод. = Зосн. \cdot Кдопл., \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам

$$З_{дод} = 34250 \cdot 0,1 = 3425 \text{ грн.}$$

Звідси загальні витрати на оплату праці (фонд заробітної плати) визначаються за формулою:

$$Во.п. = Зосн. + Здод. \quad (5.3)$$

$$В_{о.п.} = 34250 + 3425 = 37675 \text{ грн.}$$

З цієї суми утримуються обов'язкові відрахування на заробітну плату:

– Єдиний соціальний внесок (ЄСВ), що становить 22%;

– Військовий збір (ВЗ), що становить 1,5%;

Сума відрахувань становить 23,5% від фонду оплати праці та визначається за формулою:

$$В_{с.з.} = Ф_{оп} \bullet 0,235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$B_{с.з.} = 37675 \cdot 0,235 = 8853,62$$

Усі витрати обчислюються детально наведені в таблиці 5.2 та обчислюються за формулою (5.5):

$$Взп = ФЗП + ФОП \quad (5.5)$$

$$В_{зп} = 34250 + 8853,62 = 43103,62 \text{ грн.}$$

Таблиця 5.2 – Розрахунки витрат на оплату праці

з/п	**Категорія працівників**	**Основна заробітна плата, грн.**			**Додаткова заробітна плата, грн.**	**Нарахув. на ФОП, грн.**	**Всього витрати на плату праці, грн. (6=3+4+5)**
		Тарифна ставка, грн.	**Кількість відпрацьов аних год.**	**Фактично нарах. з/пл., грн.**			
А	Б	1	2	3	4	5	6
1.	Проектний менеджер	150	35	5250	525	-	-
2.	Інженер-програміст	130	200	26000	2600	-	-
3.	Тестувальник	100	30	3000	300	-	-
Разом		380	265	34250	3425	8853,62	43103,62

Опираючись на розрахунки витрат на оплату та таблицю результатів 5.2 видно, що всього витрати на плату праці становлять 43103,62 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати є невід’ємною частиною розробки комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою:

$$M_{вi} = q_i \bullet p_i \,, \qquad (5.6)$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою:

$$З_{м.в.} = \sum M_{вi} \,. \qquad (5.7)$$

Результати проведених розрахунків наведено у таблиці 5.3.

Таблиця 5.3 – Результати розрахунків матеріальних витрат.

№ п/п	**Найменування матеріальних ресурсів**	**Од. виміру**	**Фактично витрачено матеріалів**	**Ціна одиниці, грн.**	**Загальна сума витрат, грн.**
1	CD диски	шт.	2	7,45	14,90
2	Папір для друку	листів	500	0,15	75,00
3	Чорнила для принтера	шт.	1	80,00	80,00
Всього					169,90

Згідно проведених розрахунків, матеріальні витрати становлять 169,90 грн.

5.4 Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту.

Затрати на електроенергію одиниці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S, \qquad (5.8)$$

де W – необхідна потужність, кВт; T – кількість годин на реалізацію розробки; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації кінцевого продукту – 400 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 265 годин.

Визначимо витрати на електроенергію згідно формули:

$$З_в = 0{,}4 \cdot 265 \cdot 2{,}42 = 256{,}52 \text{ грн.}$$

Згідно формули затрати на електроенергію становлять 256,52 грн.

5.5 Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність. Для вирішення проблеми із відновленням даних фондів використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів.

Для визначення амортизаційних відрахувань використовується формула:

$$A = \frac{Б_В \cdot H_A}{100\%} \tag{5.9}$$

де A – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; H_A – норма амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для даної розробки засобом розробки є комп'ютер. Його сума становить 18500 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18500 \cdot 5\% / 100\% = 925 \text{ грн.}$$

Згідно проведених обчислень амортизаційні відрахування становлять 925 грн.

5.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (5.10)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати становлять згідно формули (5.10):

$$H_в = 37675 \cdot 0{,}2 = 7535 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 7535 грн.

5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків наведено у таблиці 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	**Сума, грн.**	**В % до загальної суми**
Витрати на оплату праці	43103,6	70,8
Відрахування на соціальні заходи	8853,6	14,6
Матеріальні витрати	169,9	0,3
Витрати на електроенергію	256,52	0,4
Амортизаційні відрахування	925	1,5
Накладні витрати	7535	12,4
Собівартість	60843,66	100

Собівартість ($C_в$) програмного продукту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + А + Н_в \text{ .} \quad (5.11)$$

Отже, собівартість програмного продукту дорівнює:

Св = 43103,6+ 8853,6+ 169,90 + 256,52+ 925+ 7535= 60843,66 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 60843,66 грн.

5.8 Розрахунок ціни програмного продукту

Ціну науково-дослідної роботи можна визначити можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + Р_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ) \text{ ,} \quad (5.12)$$

де $Р_{рен.}$ – рівень рентабельності (30 %); $К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем); $В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість (20%).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та $В_{н.і.}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \qquad (5.13)$$

Звідси ціна на роботу складе:

$$Ц = 60843{,}66 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 94916{,}11 \text{ грн.}$$

Загальний розрахунок ціни програмного продукту становить 94916,11 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = \frac{П}{C_B}, \qquad (5.14)$$

де $П$ – прибуток; C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - С_в \,. \tag{5.15}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 94916{,}11 - 60843{,}66 = 34072{,}45 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П}{С_В}. \tag{5.16}$$

Тоді,

$$E_р = 34072{,}45 / 60843{,}66 = 0{,}56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = \frac{1}{E_р}\ , \tag{5.17}$$

Термін окупності дорівнює:

$$T_р = 1 / 0{,}5 = 1{,}78 \text{ р.}$$

Згідно формул плановий прибуток від розробки становить 34072,45 грн., економічна ефективність дорівнює 0,56, а термін окупності становить 1,78 роки що вважається доцільним та економічно вигідним.

5.10 Висновки до п’ятого розділу

В організаційно-економічній частині дипломної роботи освітнього рівня «магістр» було розраховано основні техніко-економічні показники реалізації комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі (див. таблиця 5.5).

Орієнтоване значення економічної ефективності становить 0,56, що є достатньо високим значенням.

Період окупності повинен варіюватися від 1 до 3 років, тоді розвиток вважається доцільним та економічно вигідним. Термін окупності даної роботи становить 1,78 років.

Таблиця 5.5 – Техніко-економічні показники науково-дослідної роботи

№ п/п	**Показник**	**Значення**
1	Собівартість, грн.	60843,66
2	Плановий прибуток, грн.	34072,45
3	Ціна, грн.	94916,11
4	Економічна ефективність	0,56
5	Термін окупності, рік	1,78

На основі проведених обрахунків можна зробити висновок, що реалізація комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі є доцільною у зв’язку з невеликим терміном окупності та великим обсягом планового прибутку.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

Метою дипломної роботи магістра є реалізація комплексного підходу для забезпечення надійного механізму захисту інформації від НСД в безпровідній Wi-Fi мережі (на основі раніше досліджених технологій та методів захисту). Оскільки, проведення робіт з розробки та використання системи передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки виконавцем дипломної роботи.

Для ефективної і безпечної роботи колективу працівників з розробки програмного забезпечення комп'ютерних систем, в тому числі і фахівців з оцінювання зрілості вимог, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [17].

Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин». Згідно Правил приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-13- 98), з димовими пожежними

сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 № 151 зареєстрованих у Міністерстві юстиції України 29.04.2004 за № 554/9153 (НАПБ Б.03.001-2004), і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2004.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-13-98, НАПБ А.01.001-2004 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним.

Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі.

Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При експлуатації програмної системи підтримки процесу розробки вимог, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-1.28-10.

Організація робочого місця фахівця із запровадження або оцінювання рівня зрілості вимог програмного забезпечення повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ГОСТ 12.2.032-78 "ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования".

Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з побудови та оцінювання моделей і рівнів зрілості вимог програмного забезпечення при проектуванні комп’ютерних систем.

6.2 Вплив радіації на працездатність населення

Вплив радіації на організм людини називають опроміненням. Під час цього процесу енергія радіації передається клітинам, руйнуючи їх. Опромінення може викликати всілякі захворювання: інфекційні ускладнення, порушення обміну речовин, злоякісні пухлини і лейко, безпліддя і багато іншого. Коли радіоактивне випромінювання проходить через тіло людини або ж коли в організм потрапляють заражені речовини, то енергія хвиль і частинок передається нашим тканинам, а від них клітинам. Радіонукліди накопичуються в організмі поступово [18].

Як відомо, вплив радіації на організм людини або тварини може бути двох видів: зсередини або зовні. Здоров'я не додає ні один з них. Крім того, науці відомо, що внутрішній вплив радіаційних речовин небезпечніше зовнішнього. Найчастіше радіаційні речовини потрапляють в наш організм разом із зараженою водою і їжею. Вплив радіації на організм майже завжди негативний. Хоча доведено, що ультрафіолетова радіація підвищує працездатність організму, оскільки такі промені не тільки мають терапевтичне значення, але при відсутності природного сонця, особливо восени та взимку, є незамінним

профілактичним засобом відносно різних інфекцій. Багато районів з підвищеним радіаційним фоном є визнаними курортами (наприклад, Кавказькі Мінеральні Води, Карлові Вари і т.п.) В Україні в лікувальних закладах достатньо широко використовується корисне опромінення альфа-частинками в радонових ваннах як лікування.

Проте, в основному, радіація за своєю природою шкідлива для життя людини. Спочатку людина втрачає фізичну працездатність, а потім – розумову. Малі дози опромінення можуть призвести до тимчасової втрати працездатності, середні та великі – до онкологічних захворювань і, як наслідок, смерті. Науковий комітет по дії атомної радіації при ООН спробував висловити генетичні наслідки опромінення через такі параметри, як скорочення тривалості життя і періоду працездатності. Ці параметри, звичайно, не можуть дати адекватного уявлення про страждання жертв спадкових недуг або таких речах, як відчай батьків хворої дитини, але до них і неможливо підходити з кількісними мірками. Цілком віддаючи собі звіт в тому, що ці оцінки не більш ніж перша груба прикидка, ООН приводить в своїй доповіді наступні цифри: хронічне опромінення населення з потужністю дози 1 Гр на покоління скорочує період працездатності на 50 000 років, а тривалість життя – також на 50 000 років на кожен мільйон живих немовлят серед дітей першого опроміненого покоління; ті ж параметри при постійному опроміненні багатьох поколінь виходять на стаціонарний рівень: скорочення періоду працездатності складе 340 000 років, а скорочення тривалості життя – 286 000 років на кожен мільйон живих немовлят.

Проникаюча радіація, поширюючись у середовищі, іонізує його, а при проходженні через живу тканину іонізує атоми і молекули, що входять до складу клітин. Це призводить до порушення нормального обміну речовин, зміни характеру життєдіяльності клітин, окремих органів і систем організму, як наслідок - виникає променева хвороба. Аналіз і узагальнення основних результатів наукових досліджень показали, що медичні наслідки Чорнобильської аварії суттєво відрізнялися від прогнозованих ефектів, зокрема значно знижувалася працездатність населення аж до отримання інвалідності та настання смертельних випадків. Всі особи, що зазнали загального хронічного

опромінювання в діапазоні потужності поглинених доз 10-4 — 5 * 10-4 Гр/добу (0,01—0,05 рад/добу) чи еквівалентних доз 0,05 — 0,15 Зв/рік (5 — 15 бер/рік), залишаються здоровими і працездатними.

Відомо, що ступінь променевих (радіаційних) уражень залежить від отриманої дози випромінювання та часу, впродовж якого людина підпадає під його дію. Якщо доза не перевищує 50Р, то виключена навіть втрата працездатності, не кажучи вже про променеву хворобу. Доза в 200-300Р, отримана за короткий час, може викликати тяжкі радіаційні ураження. Здоровий організм людини здатний за цей час виробляти нові клітин на заміну загиблих. Навіть найменші дози викликають необоротні генетичні зміни, які передаються з покоління в покоління, призводять до розвитку синдрому Дауна, епілепсії, появі інших дефектів розумового і фізичного розвитку. Особливо страшно те, що радіаційному зараженню піддаються і продукти харчування, і предмети побуту. Останнім часом почастішали випадки вилучення контрафактної та низькоякісної продукції, що є потужним джерелом іонізуючого випромінювання.

Найпростіший і ефективний спосіб захистити себе від негативного впливу смертоносних променів - триматися подалі від їхнього джерела. Якщо знати все про радіацію і вміти правильно користуватися приладами для її вимірювання, то можна практично повністю уникнути її негативного впливу. Незважаючи на високу небезпеку, яку несе в собі практично будь-яке джерело радіації, методи захисту від опромінення все ж існують.

Всі способи захисту від радіаційного впливу можна розділити на три види: час, відстань і спеціальні екрани. Хоча необхідно знати, що на сьогодні ідеального засобу захисту від радіації не існує. Найкращий спосіб захисту від радіації - взагалі не мати контакту з зараженими предметами і не перебувати в місцях з підвищеним радіаційним фоном.

6.3 Планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації

Найбільш повне та організоване виконання заходів цивільного захисту (ЦЗ) на об’єкті досягається завчасною розробкою плану заходів, які необхідно проводити при загрозі або виникненні надзвичайної ситуації (НС).

План дій органів управління і сил ЦЗ (міністерств, відомств, областей, районів, міст, підприємств, установ і організацій) із запобігання і ліквідації НС розробляється на підставі законодавчих, директивних і нормативних документів і призначений для координації і діяльності центральних і місцевих органів виконавчої влади, керівництва, а також оперативності їх реагування на загрозу і виникнення НС, відвернення або зниження можливої загибелі людей, мінімізація матеріальних збитків і втрат та організацію задоволення першочергових потреб населення, яке постраждало [17]. План визначає порядок дій і відповідальність керівництва відповідних органів управління підприємств, установ і організацій, а також основні заходи щодо організації і проведення робіт із запобігання і ліквідації НС техногенного і природного характеру, узгодження термінів їх виконання, фінансові, матеріальні та інші ресурси, які необхідні для цих заходів і робіт. У план дій включаються заходи щодо захисту робітників і службовців, підтримування виробничої діяльності та інші з урахуванням обстановки після виникнення НС, передбачаються необхідна кількість сил і засобів для ліквідації наслідків НС. Основними вихідними даними при розробці плану дій на об’єкті є рішення та вказівки вищого штабу ЦЗ, розпоряджень начальника ЦЗ об’єкта, документів, що характеризують об’єкт (комунально-енергетичні мережі, стан будівель і споруд, вододжерела та ін.). План дій розробляється на підставі наказу начальника ЦЗ об’єкта. До розробки документів плану залучається керівний склад і спеціалісти об’єкта. Начальник штабу ЦЗ складає графік розробки окремих документів (розділів) і контролює його виконання.

План дій розробляється у двох (при необхідності і більше) примірниках. Підписується план дій начальником штабу ЦЗ об’єкта, погоджується з територіальними управліннями (відділами) з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи і затверджується начальником ЦЗ об’єкта. Після затвердження зміст плану дій доводиться до виконавців. План дій органів управління і сил ЦЗ із запобігання та

ліквідації НС – це програма здійснення запобіжних та захисних заходів. Він дозволяє цілеспрямовано та організовано вирішувати завдання ЦЗ в умовах НС мирного та воєнного часу. При визначенні цих заходів враховується важливість та особливості виробничої діяльності об’єкта, основні завдання органів управління та сил ЦЗ щодо запобігання і ліквідації НС.

План дій органів управління та сил ЦЗ на мирний час складається із п’яти розділів текстової частини і додатків до них. Текстова частина плану включає такі розділи: 1. Висновки із оцінки обстановки на території об’єкта. 2. Приведення в готовність та організація роботи органів управління в НС. 3. Сили ЦО об’єкта, що залучаються до виконання аварійно-рятувальних, пошукових та відновлювальних робіт. 4. Організація забезпечення заходів та дій ЦЗ. 5. Організація управління, оповіщення і зв’язку. Окремо розробляється “План дій органів управління та сил ЦЗ об’єкта при переведенні з мирного на воєнний стан” за ступенями готовності воєнного часу та раптовому нападі супротивника. Крім цього, на об’єкті господарської діяльності розробляються плани служб ЦЗ, щодо забезпечення заходів і дій органів управління і сил ЦЗ при загрозі і виникненні НС та при переведенні органів управління і сил з мирного на воєнний стан.

6. 4 Висновки до розділу

В цьому розділі описані важливі питання охорони праці, вплив радіації на працездатність населення та планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації.

7 ЕКОЛОГІЯ

7.1 Методологічні основи обробки екологічної інформації на базі комп’ютерних технологій

Це комплексне питання містить наступні складові [19]:

— зведення і первинне оброблення статистичних даних (статистичне зведення — це первинне наукове оброблення даних спостереження для характеристики суцільного явища узагальнюючими показниками. Етапи: статистичне групування; підсумовування даних; табличне і графічне оформлення одержаних даних. За допомогою статистичного зведення розв'язують такі завдання: групування даних, розроблення системи показників для характеристики груп і всієї статистичної сукупності, обчислення групових і загальних показників, зведення результатів обчислення у статистичних таблицях. У результаті обробки та систематизації статистичних матеріалів отримуємо ряди цифрових показників, які характеризують окремі сторони явищ, що вивчаються, в просторі або зміну цих явищ у часі. Тому побудова статистичних рядів є основою будь-якого первинного оброблення статистичної інформації);

– статистична оцінка екологічного стану НПС і закономірностей його розподілу (властивістю статистичної сукупності є коливання, мінливість значень будь-якої ознаки, тобто варіація. Вона зумовлена дією безлічі взаємопов’язаних причин, серед яких є основні і другорядні. Основні причини формують центр розподілу, другорядні - варіацію ознак, сукупна їх дія - форму розподілу. Аналіз варіаційного ряду розподілу полягає у виявленні закономірностей зміни частот залежно від зміни кількісної ознаки, яка покладена в основу групування. При аналізі варіаційних рядів найуживанішими є такі групи показників: центра розподілу, розміру варіації, форми розподілу);

– статистичне групування в екології (мета - поділ сукупностей на однорідні типові групи за існуючими для них кількісними ознаками з метою всебічної характеристики їхнього стану, розвитку і взаємодії. Метод статистичних

групувань робить статистику могутнім знаряддям соціального пізнання і використовується для вирішення трьох взаємопов'язаних завдань: виділення різних соціально-економічних типів явищ (процесів) та всебічна їх характеристика; дослідження структури масової сукупності; вивчення взаємодії між окремими ознаками сукупності. Суть цього методу полягає у тому, що складне масове явище розглядається не як єдине нероздільне ціле, а в ньому виділяються окремі групи одиниць із статистичними показниками, які дають кількісну характеристику якісно своєрідній частині одиниць усієї сукупності);

– дисперсійний аналіз в екології (для кількісної оцінки взаємозв'язків і їхньої суттєвості при незначній кількості спостережень застосовується дисперсійний аналіз. Головне призначення дисперсійного аналізу — статистично виявити вплив різних факторів на мінливість ознаки, що вивчається. В результаті дисперсійного аналізу одержуються дані, що характеризують загальне розсіювання, або дисперсію ознаки, обумовлену дією всіх факторів; часткову або факторну дисперсію, викликану впливом організованих і врахованих дослідником факторів; та залишкову дисперсію, пов’язану з невідомими експериментатору, випадковими, неорганізованими факторами. за його допомогою розв'язуються такі завдання: кількісне вимірювання сили впливу факторних ознак та їх сполучень на результативну; визначення вірогідності впливу та його довірчих меж; аналіз окремих середніх та статистична оцінка їх різниці);

– кореляційний аналіз зв’язків в екології (поглибленням дослідження й кількісною оцінкою характеру та механізму взаємодії факторних і результативних ознак є метод аналізу регресії та кореляції, тобто кореляційний аналіз. При кореляційній залежності будь-якому значенню однієї змінної величини може відповідати декілька чи навіть безліч різноманітних, тобто варіюючих значень іншої змінної величини. Розрахунки на основі кореляційних моделей підвищують ступінь точності аналізу, часто виявляють недоліки попереднього аналізу. Перевага цього методу полягає також і в тому, що він дає можливість розв'язувати задачі, які не можна вирішити за допомогою інших методів економічного аналізу. У дослідженнях важливо вивчати не стільки міру

кореляції, скільки форму її й характер зміни однієї ознаки залежно від зміни іншої. Ці задачі розв'язуються методами регресійного аналізу. Використання методу кореляції і регресії дозволяє вирішити такі основні завдання: встановити характер і тісноту зв'язку між досліджуваними явищами; визначити і кількісно виміряти ступінь впливу окремих факторів і їх комплексу на рівень досліджуваного явища; на підставі фактичних даних моделі залежності екологічних показників від різних факторів розраховувати кількісні зміни аналізованого явища при прогнозуванні показників і давати об'єктивну оцінку діяльності підприємств);

– статистичний аналіз тенденцій і закономірностей динаміки в екології (екологічні процеси - явище не статичне, а динамічне, оскільки упродовж певного часу - місяць за місяцем, рік за роком змінюється стан забруднень природних сфер, рівень викидів забруднюючих речовин в навколишнє середовище, об’єм промислових і побутових відходів на звалищах тощо. Дослідження процесів зміни і розвитку явищ у часі відбувається на основі побудови і аналізу рядів динаміки. Для динамічного ряду характерні перелік хронологічних дат або інтервалів часу і конкретні значення відповідних статистичних показників, які називають рівнями ряду. Тому кожен ряд динаміки має елементи двох типів - рівні (цифри, з яких складається ряд) і періоди (дати, яким відповідають рівні ряду);

– індексний метод в екології (статистична практика при вивченні екологічних явищ широко використовує індекси. Знання методології побудови індексів значно розширює аналітичні можливості дослідника, збагачує результативну інформацію досліджень. За допомогою індексів можна характеризувати зміну в часі і просторі найрізноманітніших показників: обсяги викидів в атмосферу, скидів шкідливих речовин у водне середовище, інтенсивність забруднень і т. д. За допомогою індексного методу вирішуються такі завдання: характеризують загальну зміну складного економічного явища чи окремих його елементів (складових); виділяють вплив одного з факторів через елімінування впливу інших; відокремлюють впливу зміни структури явища на зміну індексованої величини).

7.2 Радіоактивне забруднення довкілля та його моніторинг

Радіоактивне забруднення характеризується збільшенням природного радіоактивного фону в результаті використання людиною природних і штучних радіоактивних речовин, які переносяться повітряними потоками і водними течіями, тваринами, птахами, рибами. У результаті випадання радіоактивних речовин забруднюються такі компоненти природного середовища, як атмосферне повітря, ґрунтовий покрив, водні маси, рослини, тварини тощо. Радіоактивне забруднення природних екосистем відбувається аерозольним, контактним або біологічним шляхом. Радіонукліди включаються у кругообіг речовин і потрапляють в організм людини з харчовими продуктами по ланцюгах живлення.

Середні величини природного фону становлять 10 - 20 мікрорентген за годину, хоча в деяких місцях планети, там, де на поверхню виходять радіоактивні кристалічні породи, природний фон може сягати 200 - 400 мкР/ год і навіть 1200 мкР/ год. Значна частина території нашої країни також розміщена на виходах Українського кристалічного щита, тому природний радіаційний фон тут теж підвищений. Загальний фон радіоактивного випромінювання на території України складає 70 – 100 мбер/рік.

Радіоактивному забрудненню підпадають такі компоненти;

– природніх екосистем: ґрунтовий покрив, рослини і тварини, водне середовище;

– агроекосистем (радіоактивне забруднення, поступово, всмоктується ґрунтовим розчином, з якого через коріння надходить до рослин і нагромаджується в їхній біомасі. Врешті-решт радіонукліди виявляються у продуктах харчування рослинного походження, а також у молоці, м’ясі, що спричинено споживанням домашньою худобою забруднених кормів);

– урбоекосистем (радіаційна небезпека у великих урбоекосистемах значною мірою спричинена радіоактивністю, яка потрапляє у водні джерела. Передусім це зумовлено тим, що людина використовує значну кількість води.

Також радіоактивні матеріали потрапляють в урбоекосистеми з транспортом);

– техноекосистем (гірничовидобувні об’єкти з підвищеною радіоактивністю, зокрема відвали, кар’єри, відстійники, хвостосховища тощо.)

Радіоекологічний моніторинг – комплексна інформаційно-технічна система спостережень, досліджень, оцінювання й прогнозування радіаційного стану біосфери, територій поблизу АЕС і потерпілих від радіаційних аварій.

Головними завданнями радіоекологічного моніторингу є:

– спостереження та контроль за станом забрудненої радіонуклідами зони, її окремих особливо шкідливих ділянок та пропонування заходів щодо зниження шкідливості;

– моніторинг стану об’єктів природного середовища за параметрами, які характеризують радіоекологічну ситуацію у зоні забруднення та за її межами;

– виявлення тенденцій до змін природного середовища, спричинених функціонуванням екологічно небезпечних об’єктів, а також при реалізації заходів, що проводяться на забруднених територіях;

– з’ясування тенденцій до змін стану здоров’я населення, яке проживає на забруднених радіонуклідами територіях;

– інформаційне забезпечення прогнозу радіоекологічної ситуації в забрудненій зоні та країні загалом.

Радіологічний моніторинг реалізують у трьох напрямах: базовий (стандартний), кризовий (оперативний), науковий (фоновий).

В Україні після катастрофи на ЧАЕС здійснюють радіоекологічний моніторинг основних складових довкілля на різних територіальних рівнях за характерними лише для нашої держави показниками. Так, в зоні забруднення (крім об’єкта “Укриття” та 30-кілометрової зони відчуження) здійснюється радіоекологічний моніторинг:

– ландшафтно-геологічного середовища з метою отримання базової інформації для оцінювання та прогнозування загальної радіоекологічної ситуації на забруднених радіонуклідами територіях і її впливу на екологічну ситуацію в Україні;

– поверхневих і підземних водних систем;

– природоохоронних заходів та споруд;

– локальних довгочасних джерел реального і потенційного забруднення (об’єкт “Укриття”, ставок-охолоджувач, пункти захоронення радіоактивних відходів, пункти тимчасової локалізації радіоактивних відходів);

– біоценозів;

– медичний і санітарно-гігієнічний.

Комплексний радіоекологічний моніторинг ґрунтується на інформації, отриманій внаслідок здійснення базових видів радіаційного моніторингу.

Основними складовими радіоекологічного моніторингу є

– ядерно-радіаційний моніторинг (контроль за станом ядерно-радіаційних об’єктів і напрацювання заходів щодо зниження ступеня їх шкідливості, оцінювання і прогнозування радіаційної обстановки на об’єктах природного середовища – в Україні здійснює система ГАММА);

– радіогеохімічний моніторинг (є основним джерелом отримання регулярної і системно-організованої інформації про просторовий розподіл радіоактивних, зокрема техногенних, елементів або їх ізотопів і закономірності їх мобілізації, транзиту, локалізації та фіксації);

– моніторинг поверхневих водних систем (потрапляння великої кількості радіоактивних опадів у водозбори рік Прип’ять, Десна, Дніпро, які є основними водними артеріями водосховищ Дніпровського каскад);

– радіогідрогеологічний моніторинг (у 30-кілометровій зоні проводяться режимні спостереження на гідрогеологічних постах, дренажних та осушувальних системах, на певних ділянках ґрунту, свердловинах).

7.3. Висновки до розділу

В цьому розділі описано методологічні основи обробки екологічної інформації на базі комп’ютерних технологій та радіоактивне забруднення довкілля та його моніторинг.

ВИСНОВКИ

В дипломній роботі розглянуто основні методи та технології захисту інформації в Wi-Fi мережах стандарту 802.11.

Бездротові мережі стандарту IEEE 802.11 тривалий час використовуються як в приватній, так і в корпоративній сферах. Серйозною проблемою є забезпечення надійного захисту передачі даних в мережі.

За результатами проведеного дослідження, враховуючи особливості технології безпровідної передачі даних по радіоканалах, можна стверджувати, що ефективна система захисту інформації у WI-FI мережі повинна складатися із комплексу апаратних та програмних компонентів. Головними з них вважаються механізми, які гарантують, що дані дійсно надходять із передбачуваного джерела, а їхній несанкціонований перегляд і зміна неможливі.

Основні результати, отримані в роботі:

– досліджено та проаналізовано основні можливості служб та протоколів забезпечення захисту бездротових мереж;

– запропоновано механізм проведення комплексного аудиту захищеності безпровідних мереж;

– на основі критеріїв оцінки захищеності безпровідної мережі побудовано модель профілю захисту для Wi-Fi мереж;

– проведено тестування серверів автентифікації на предмет забезпечення захищеності безпровідних мереж стандарту 802.11;

– протестовано етапи автентифікації на Wi-Fi пристроях з аудитом подій на сервері контролю безпечного доступу ACS.

Описаних та досліджених в роботі технологій, механізмів, методів та засобів захисту є достатньо для забезпечення комплексного підходу до безпеки бездротових мереж, та можливості організації безпечного віддаленого доступу для спеціалістів інших компаній.

БІБІЛОГРАФІЯ

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам // Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. – М.: Наука, 2012. - 552 с.

2. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: Вильямс, 2004. — 304 с.

3. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей – М., Вильямс., 2002. – 432 с.

4. Мартинюк І.Є. Про один підхід до захисту інформації у wi-fi мережах стандарту 802.11 / І.Є. Мартинюк – Матеріали VII науково-технічної конференції «Інформаційні моделі, системи та технології» – Тернопіль, ТНТУ, 11-12 грудня 2019 р.– с. 68.

5. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець, Р.І. Банах // Інформаційна безпека. – Східноукраїнський Національний університет імені Володимира Даля.) – 2013. – № 4(12). – С. 16-22

6. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11 / Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Тарас Петренко // Захист інформації, том 17, №4 – 2015 . – С. 285-291.

7. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей // Составитель М. Кадер – М.: Cisco Press, 2012. – 456 с.

8. Решения Cisco для обеспечения информационной безопасности (издание 4) // Составитель А. Лукацкий. – М.: Cisco Press, 2010. – 623 с.

9. Администрирование информационно-вычислительных сетей // Н.Т.Кустов. – Томск: Пресса, 2011. – 724 с.

10. Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 2017. [Електронний ресурс]. – Режим доступу: www.cisco.com. (дата звернення 07.10.2019).

11. http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1200/vxworks/configuration/guide/ap120scg/bkscgch4.html [Електронний ресурс] – Дата звернення: 15.10.2019.

12. Уэнстром М. Организация защиты сетей Cisco - М., Вильямс, 2005. – 768 с.

13. Владимир Антонович Ткаченко. Технологии стандарта 802.11x [Електронний ресурс]. – Режим доступу: http://www.lessons-tva.info/articles/net/003.html (дата звернення 10.11.2019).

14. Дмитрий Бугрименко. Проблемы безопасности в беспроводных ЛВС IEEE 802.11 и решения Cisco Wireless Security Suite [Електронний ресурс]. – Режим доступу: https://www.cisco.com/web/RU/downloads/WLANSecurity1.2a.pdf (дата звернення 11.11.2019).

15. В. Ф. Шаньгін. Захист інформації в комп'ютерних системах і мережах / В. Ф. Шаньгін – Київ : МК Прес, 2012. - 592 с.

16. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO // Сучасний захист інформації. 2016. №2. – С. 60–68.

17. Зеркалов Д.В. Охорона праці в галузі: Загальні вимоги [Електронний ресурс] . Навчальний посібник. – К.: «Основа». 2011. – 551 с.

18. Основи екології та охорона навколишнього природного середовища : Навч. посібник для студ. вузів / Я. І. Бедрій. – Київ : Центр учбової літ. (ЦУЛ), 2002. – 247 с.

19. Тарасова В.В. Екологічна статистика. – К.: «Центр учбової літератури», 2008. - 391с.