КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
(факультет)

інформаційних технологій
(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

на тему: «Розробка інформаційної системи побудови кабельних та бездротових мереж»

Горкуценко Віктор
(прізвище, ім’я та по батькові студента повністю)

Київ 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
_____
(факультет)

інформаційних технологій
_____
(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В..
_____
„___” _____2023 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

на тему: «Розробка інформаційної системи побудови кабельних та бездротових мереж»

Виконав: Студент спеціальності
122 «Комп`ютерні науки .
(шифр і назва напряму підготовки, спеціальності)

Горкуценко В. .
(прізвище та ініціали)

Керівник __д.т.н., проф. Терентьєв О.О. ___
(прізвище та ініціали)

Рецензент __к.т.н., доц. Шабала Є.Є. .

Київ, 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: __автоматизації і інформаційних технологій .
Кафедра:__ __інформаційних технологій .
Освітній рівень: «бакалавр» за ОП .
Спеціальність:_122 «Комп`ютерні науки» .

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
д.т.н., професор Цюцюра С.В.
_____
„___” _____2023 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

Горкуценко Віктор
1. Тема роботи: Розробка інформаційної системи побудови кабельних та .
бездротових мереж .
затверджена наказом ректора КНУБА № _____ від «__» _листопад__2022 р.
2. Керівник роботи: Терентьєв Олександр Олександрович, д.т.н, професор .
кафедри інформаційних технологій проектування і прикладної математики .
3. Строк подання студентом роботи до захисту: __червень 2023 року .
4. Зміст пояснювальної записки за розділами:
Р.1. Аналіз предметної області та постановка задачі .
Р.2. Технології проектування структури кабельних та бездротових мереж .
Р.3. Розробка інформаційного забезпечення системи .
Р.4. Розробка програмного забезпечення системи .
Р.5. Тестовий приклад програми .
Р.6. Ергономіка інформаційних технологій .
5. Інформаційні слайди:
С.1. Класифікація бездротових мереж .

С.2. Радіус дії персональних глобальних бездротових мереж .
С.3. Структура захищеної локальної бездротової мережі .
С.4. Методи захисту комп'ютерних мереж від проникнення .
С.5. Програмне забезпечення системи. Тестовий приклад програми .

6. Календарний план виконання атестаційної випускної роботи бакалавра

Види робіт та їх зміст	Дата виконання
Р. 1. Аналіз предметної області та постановка задачі	Травень 2023 р.
Р. 2. Технології проектування мереж	Травень 2023 р.
Р. 3. Розробка інформаційного забезпечення системи	Травень 2023 р.
Р. 4. Розробка програмного забезпечення системи	Травень 2023 р.
Р. 5. Тестовий приклад програми	Травень 2023 р.
Р. 6. Ергономіка інформаційних технологій	Травень 2023 р.
Остаточне оформлення роботи	Червень 2023 р.
Попередній захист роботи на кафедрі	Червень 2023 р.

7. Консультанти розділів атестаційної випускної роботи бакалавра

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Ергономіка інформаційних технологій	д.т.н. проф. Терентьєв О.О.		
Прийом програмного продукту	к.т.н. доц. Шабала Є.Є.		

8. Дата видачі завдання: 11 листопада 2023 року

Керівник _____ Терентьєв О.О.
(підпис) (прізвище та ініціали)

Бакалавр _____ Горкуценко В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Горкуценко В. «Розробка інформаційної системи побудови кабельних та бездротових мереж».

Атестаційна випускова робота бакалавра за спеціальністю: 122 «Комп'ютерні науки». – Київський національний університет будівництва та архітектури. – Київ, 2023.

Атестаційна робота присвячена технології створення та налаштування бездротової локальної мережі. Метод дослідження – теоретичний аналіз протоколів дротових та бездротових локальних мереж, вивчення механізмів передачі даних Wi-Fi мережах, можливості її захисту та аналіз програмних продуктів для реалізації даного типу мереж.

Ключові слова: моделі, методи, моделювання систем, Wi-Fi.

SUMMARY

Horkutsenko V. "Development of an information system for the construction of cable and wireless networks."

Attestation final work of the bachelor in the specialty: 122 "Computer science". - Kyiv National University of Construction and Architecture. - Kyiv, 2023.

Attestation work is devoted to the technology of creation and adjustment of wireless LAN. The research method is a theoretical analysis of wired and wireless LAN protocols, the study of Wi-Fi data transmission mechanisms, the possibilities of its protection, and the analysis of software products for the implementation of this type of network.

Keywords: models, methods, systems simulation, Wi-Fi.

ЗМІСТ

ВСТУП

Способи мережного доступу з кожним роком стають все популярніше, їх кількість невпинно зростає. І постає звичайно питання про безпеку. Адже саме безпека доступу користувачів та механізм захисту – є одними з нагальних проблем сьогодення.

За останні десятиліття локальні дротові та бездротові мережі передачі інформації стали одним із основних напрямків розвитку телекомунікаційної індустрії. Вони проникли у всі сфери людської діяльності, включаючи економіку, науку, культуру, освіту, промисловість та ін.

Метою дипломного проекту є дослідження технологій створення дротових та бездротових мереж.

Основне завдання будь-якої мережі – передача інформації. Підключитися до мережі Wi-Fi можна за допомогою ноутбуків і кишенькових комп'ютерів, оснащених спеціальним устаткуванням. На сьогоднішній день практично всі сучасні портативні та кишенькові комп'ютери є Wi-Fi-сумісними. Однак і власники не нових мобільних ПК також можуть легко використати цю зручну технологію, установивши в PCMCIA-слоти своїх комп'ютерів спеціальні Wi-Fi-картки, або підключивши зовнішній Wi-Fi-пристрій через USB-порт.

Для досягнення поставленої мети необхідно проаналізувати особливості цих типів мереж та їх функціональні можливості. А також звернути увагу на безпеку та захист дротових та бездротових мереж, адже це є невід’ємною частиною при їх створенні та експлуатації.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Технології локальних мереж

Локальна комп’ютерна мережа (англ. Local Area Network(LAN)) являє собою об’єднання певного числа комп’ютерів (іноді досить великого) на відносно невеликій території. В порівнянні з глобальною мережею(WAN), локальна мережа зазвичай має більшу швидкість обміну даними, менше географічне покриття та відсутність необхідності використовувати запозиченої телекомунікаційної лінії зв’язку

Мережева технологія – це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують, достатній для побудови локальної обчислювальної мережі. Мережеві технології називають базовими технологіями або мережевою архітектурою локальних мереж. Мережева технологія або архітектура визначає топологію і метод доступу до середовища передавання даних, кабельну систему або середовище передавання даних, формат мережевих кадрів, тип кодування сигналів, швидкість передавання в локальній мережі. У сучасних локальних обчислювальних мережах значного поширення набули такі технології або мережеві архітектури, як: Ethernet, Token Ring, Arcnet, FDDI, SNA, Internet, Wi-Fi.

Технологія Ethernet була розроблена групою американських учених у 70-х роках XX ст. (рис. 1.1).

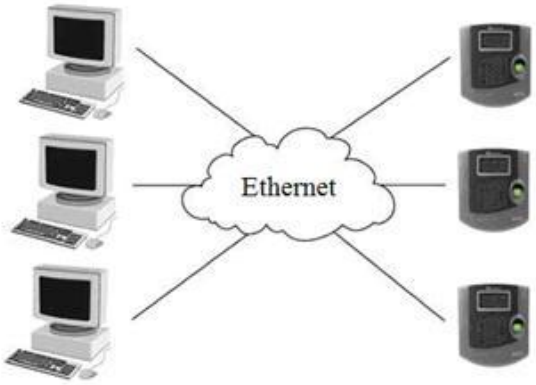

Рисунок 1.1 Мережа Ethernet

Мережі Ethernet призначені для з’єднання робочих станцій до локальної мережі зі швидкістю передавання до 1 Гбіт/с. Для каналів зв’язку використовуються коаксіальний кабель, кручена пара та оптоволоконний кабель. Якщо застосовується кручена пара, мережа конфігурується як «зірка», якщо коаксіальний кабель – як «шина». Існує кілька систем: 10Base2 – тонкий Ethernet, ThinNet, 10Base5 – товстий Ethernet, ThickNet, 10BaseT – Ethernet на основі крученої пари, 10BaseF – оптоволоконний Ethernet, 100BaseT – Fast Ethernet, швидкий Ethernet, Gigabit Ethernet, Радіо-Ethernet, які відрізняються: довжиною сегмента; кількістю робочих станцій, які можна підключити до сегмента засобом підключення до кабелю.

Для підключення станцій до кабелів використовуються трансівер та адаптер. Трансівер забезпечує прийом та посилення електричних сигналів, які надходять з кабелю, та передає їх у зворотному напрямку до коаксіального кабелю та мережевого адаптера. Довжина кабелю між адаптером та трансівером може досягати 50 м. Довжина сегмента залежно від типу системи коливається у межах 185 – 500 м; кількість робочих станцій, які можна підключити до одного сегмента, – 30 – 100.

Використання спеціальних пристроїв-повторювачів (вони виконують повторення та посилення прийнятого сигналу, який «затухає» під час передавання на великі відстані) дозволяє з’єднати до п’яти сегментів мережі. Таким чином, максимальна довжина мережі Ethernet 10BASE2 складає 1 км, а мережі Ethernet 10BASE5 – 2,5 км.

Система 10BASE-T для передавання інформації використовує кручені пари напівпровідників, які з’єднують робочі станції через концентратор. За допомогою коаксіального кабелю можна з’єднати кілька концентраторів.

Мережа Ethernet 10BASE-F – це мережа з оптоволоконними кабелями зі швидкістю передавання даних 10 Мбіт/с, зіркоподібною топологією та максимальною довжиною сегмента до 2100 м.

Технологія Arcnet може будуватися як «зірка» та як «шина» (рис. 1.2). За способом організації передавання даних ця технологія належить до мереж із маркерним методом доступу. Це означає, що доступ виконується за допомогою кадру маркера певного формату, який передається безперервно. Передавання маркера відбувається від однієї станції до іншої в порядку зменшення їхніх логічних адрес. Станція з мінімальною адресою передає кадр маркера станції з найбільшою адресою.

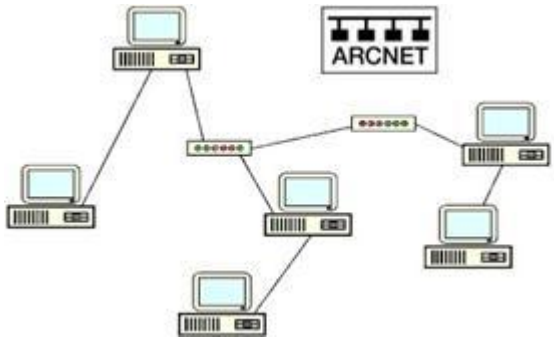

Рисунок 1.2 Мережа Arcnet

Управління мережею виконує станція, яка має маркер у даний момент часу. Вона виконує: генерацію (реконфігурацію) логічного кільця; контроль за передачею маркера; змінення параметрів системи управління; прийом та оброблення запитів на підключення пасивних станцій (станцій, що не підключені до логічного кільця).

Технологія Token Ring розроблена фірмою IBM і являє собою суміш топологій (рис. 1.3). Token Ring працює за топологією «зірка» зі спеціальним пристроєм IBM, який має назву «станції багато користувацького доступу» як центральний хаб. Але для зв’язку з ним кожний комп’ютер має два кабелі (типу «кручена пара»), одним з яких він посилає дані, а іншим – отримує. За способом організації передавання даних Token Ring належить до кільцевих мереж із маркерним методом доступу. Кадри даних, як і кадр маркера,

передаються кільцем незалежно від розташування станцій. Відправник «звільняє» маркер та передає його далі кільцем лише після отримання кадру з доповненою інформацією про результати прийняття від отримувача. Швидкість передавання даних – 16 - 1000 Мбіт/с.

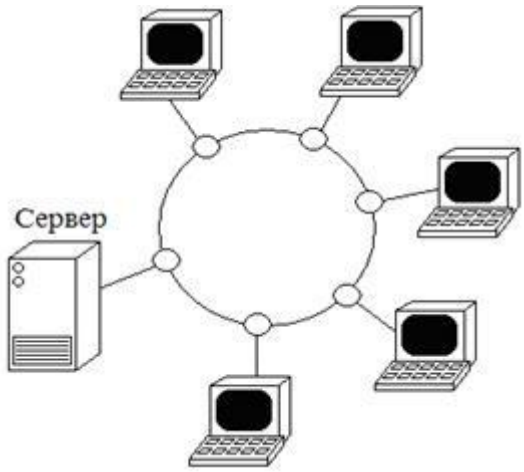

Рисунок 1.3 Мережа Token Ring

Передача маркера

Token Ring і IEEE 802.5 є головними прикладами мереж з передачею маркера. Мережі з передачею маркера переміщують вздовж мережі невеликий блок даних, званий маркером. Володіння цим маркером гарантує право передачі. Якщо вузол, який приймає маркер, не має інформації для відправки, він просто переправляє маркер до наступної кінцевої станції. Кожна станція може утримувати маркер протягом певного максимального часу (за замовчуванням – 10 мс).

Дана технологія пропонує варіант вирішення проблеми колізій, що виникає при роботі локальної мережі. У технології Ethernet, такі колізії виникають при одночасній передачі інформації кількома робочими станціями, які перебувають в межах одного сегмента, тобто використовують загальний фізичний канал даних.

Якщо у станції, що володіє маркером, є інформації для передачі, вона захоплює маркер, змінює у нього один біт (в результаті чого маркер перетворюється в послідовність «початок блоку даних»), доповнює інформацією, яку він хоче передати і відсилає цю інформацію до наступної станції кільцевої мережі. Коли інформаційний блок циркулює по кільцю, маркер в мережі відсутня (якщо тільки кільце не забезпечує «раннього звільнення маркера» – early token release), тому інші станції, які бажають передати інформацію, змушені чекати. Отже, в мережах Token Ring не може бути колізій. Якщо забезпечується раннє вивільнення маркера, то новий маркер може бути випущений після завершення передачі блоку даних.

Інформаційний блок циркулює по кільцю, поки не досягне передбачуваної станції призначення, яка копіює інформацію для подальшої обробки. Інформаційний блок продовжує циркулювати по кільцю, він остаточно видаляється після досягнення станції, що відіслали цей блок. Станція відправлення може перевірити повернувся блок, щоб переконатися, що він був переглянутий і потім скопійовано станцією призначення.

Сфера застосування

На відміну від мереж CSMA / CD (наприклад, Ethernet) мережі з передачею маркера є детерміністичних мережами. Це означає, що можна обчислити максимальний час, який пройде, перш ніж будь-яка кінцева станція зможе передавати. Ця характеристика, а також деякі характеристики надійності, роблять мережу Token Ring ідеальною для застосувань, де затримка повинна бути передбачена і важлива стійкість функціонування мережі. Прикладами таких застосувань є середа автоматизованих станцій на заводах. Застосовується як більш дешева технологія, набула поширення скрізь, де є відповідальні програми, для яких важлива не стільки швидкість, скільки надійна доставка інформації. В даний час Ethernet по надійності не поступається Token Ring і істотно вище за продуктивністю

Технологія Fiber Distributed Data Interface, FDDI (укр. розподілений волоконний інтерфейс даних) будується на основі стандарту на оптоволоконний інтерфейс розподілених даних. Швидкість передавання даних 100-200 Мбіт/с (рис. 1.4).

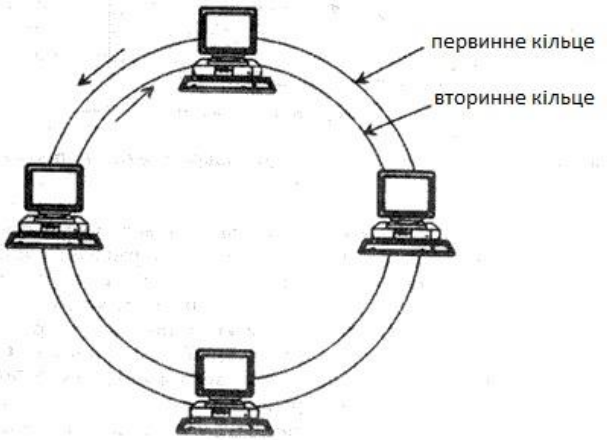

Рисунок 1.4 Стандарт FDDI

Забезпечує зв’язок між мережами різних типів, може використовуватись в MAN, але має обмеження на довжину кільця (не більше 100 км). Виступає в ролі магістральної мережі, до якої можуть підключатись інші менш продуктивні мережі. Має суттєву відмінність від традиційної технології з передачею маркера. Так, певний комп’ютер може захопити маркер на певний проміжок часу і звільнити його одразу після завершення передачі. Тому в даних мережах можлива циркуляція декількох кадрів одночасно. Вибір оптоволокна як середовища передачі визначив такі переваги нової мережі, як висока перешкодозахищеність, максимальна таємність передачі інформації й прекрасна гальванічна розв’язка абонентів. Висока швидкість передачі, що у випадку оптоволоконого кабелю досягається набагато простіше, дозволяє вирішувати багато завдань, недоступних менш швидкісним мережам, наприклад, передачу зображень у реальному масштабі часу. Крім того, оптоволоконий кабель легко вирішує проблему передачі даних на відстань

декількох кілометрів без ретрансляції, що дозволяє будувати більші за розмірами мережі, що охоплюють навіть цілі міста й мають при цьому всі переваги локальних мереж (зокрема, низький рівень помилок). Все це визначило популярність мережі FDDI, хоча вона поширена ще не так широко, як Ethernet й Token-Ring. Також для FDDI часто застосовують топологію подвійного кільця. Трафік в такій мережі складається із двох потоків, протилежних за напрямком, по двох кільцях. У разі виходу з ладу одного з них, мережа автоматично переконфігуровується. Одне кільце вважається основним, ним передається інформація в звичайному стані; друге — додатковим, ним дані передаються у разі обриву на першому кільці.

Мережі SNA (системна мережева архітектура) ґрунтуються на ідеології фірми IBM щодо побудови комп'ютерних мереж на базі систем телеоброблення даних. Згідно з системною мережевою архітектурою комп'ютерна мережа організовується за регіональним принципом. Через мережеві процесори регіонів за допомогою каналів зв'язку функціонує єдина мережа.

Для з'єднання мереж SNA з іншими мережами може бути використана еталонна модель відкритих систем (OSI).

Internet – це розгалужена мережа, що з'єднує комп'ютери, розташовані по всьому світу. Internet була створена на основі ARPANET – мережі, що з'єднувала навчальні заклади та військові організації. У результаті розвитку комп'ютерних мереж виникла попотрібно в їх з'єднанні. Із цією метою було розроблено протокол передавання інформації TCP/IP.

Технологія Wi-Fi – це можливість, не розгортаючи кабельної системи, дістати доступ до будь-яких сервісів Internet, де б не знаходився користувач, він завжди можете бути в мережі (рис. 1.5).

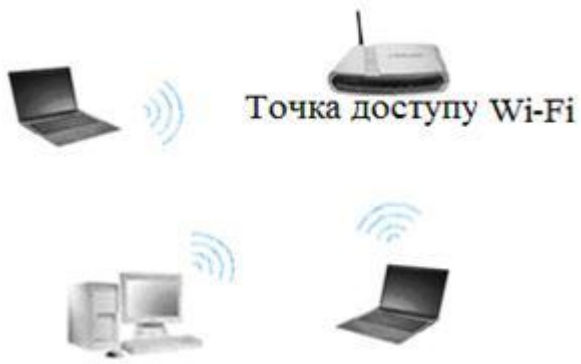

Рисунок 1.5 – Мережа Wi-Fi

Технологія Wi-Fi – це безпроводовий аналог стандарту Ethernet, на основі якого сьогодні побудована велика частина офісних комп'ютерних мереж. Він був зареєстрований в 1999 році і став справжнім відкриттям для менеджерів, торгових агентів, співробітників складів, основним робочим інструментом яких є ноутбук або інший мобільний комп'ютер.

Wi-Fi – скорочення від англійського Wireless Fidelity, що означає стандарт бездротового (радіо) зв'язку, який об'єднує кілька протоколів та має офіційне найменування IEEE 802.11. Подібно традиційним провідним технологіям, Wi-Fi забезпечує доступ до серверів, що зберігають бази даних або програмні додатки, дозволяє увійти до Internet, роздруковувати файли і т. п. Але при цьому комп'ютер, з якого зчитується інформація, не потрібно підключати до комп'ютерної розетки. Досить розмістити його в радіусі 300 м від так званої точки доступу (access point) – Wi-Fi-пристрою, що виконує приблизно ті ж функції, що звичайна офісна АТС. У цьому випадку інформація буде передаватися за допомогою радіохвиль в частотному діапазоні 2,4-2,483 ГГц.

Таким чином, Wi-Fi-технологія дозволяє вирішити три важливих задання: спростити спілкування з мобільним комп'ютером; забезпечити комфортні умови для роботи діловим партнерам, які прийшли до офісу зі своїм ноутбуком; створити локальну мережу в приміщеннях, де прокладка кабелю є неможливою або надмірно дорогою.

Класифікація бездротових мереж

В даний час існує велика кількість різноманітних бездротових технологій, що вимагає введення класифікації. Один із способів класифікації бездротових мереж грунтується на радіусі дії мережі, при цьому виділяються чотири основних типи (див. Рисунок 1.6):

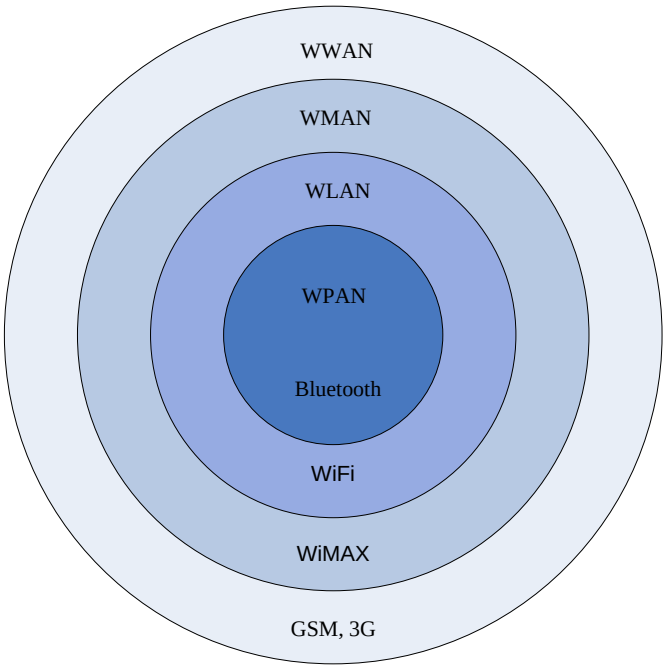

Рисунок 1.6 Класифікація бездротових мереж по площі охоплення

WPAN (Wireless Personal Area Network) - використовуються для передачі інформації від стільникових телефонів, портативних комп'ютерів і інших побутових приладів, мають малий радіус дії (близько 10 м). До цієї категорії можна віднести технологію Bluetooth;

WLAN (Wireless Local Area Network) - використовуються для обслуговування невеликих територій, мають середній радіус охоплення (близько 100 м). Сюди відносяться стандарти 802.11;

WMAN (Wireless Metropolitan Area Network) - в основному застосовуються операторами зв'язку для створення інфраструктури доступу кінцевих користувачів, так званої «останньої милі», характеризується

середнім радіусом дії (1-10 км). До цієї категорії відноситься стандарт 802.16 (WiMax)

WWAN (Wireless Wide Area Network) - використовуються в стільниковому зв'язку (GSM, CDMA, UMTS) і характеризуються великим радіусом дії (до 40 км);

В залежності від способу комутації, мережі поділяються на два класи:

Мережу з комутацією пакетів;

Мережу з комутацією каналів.

Залежно середовища через яке передається сигнал, можна визначити такі класи бездротових мереж:

Мережі на радіомодемах;

Інфрачервоні системи;

Системи з використанням низькоорбітальних супутників;

Системи лазерного зв'язку.

Розрізняють безпровідні систем також по способу організації мережі:

Двоточковий звязок. У телекомунікаційних первинних мережах така схема вже довгий час застосовується для створення так званих радіорелейних ліній зв'язку. Таку лінію утворюють кілька веж, на яких встановлені параболічні спрямовані антени.

Схема бездротового каналу з одним передавачем і кількома приймачами характерна для такої організації доступу, при якій численні термінали користувачів з'єднуються з базовою станцією (Base Station, BS) або точкою доступу (Acess Point, AP).

Зв'язок декількох передавачів і декількох приймачів У випадку схеми з кількома передавачами і кількома приймачами бездротова лінія зв'язку представляє собою загальне електромагнітне середовище, що розділяється вузлами. Кожен вузол може використовувати це середовище для взаємодії з будь-яким іншим вузлом без звернення до базової станції.

1.2 Бездротова персональна мережа WPAN

Стандарт Bluetooth розроблений групою Bluetooth SIG (Bluetooth Special Interest Group), яка була організована з ініціативи компанії Ericsson. Стандарт Bluetooth також адаптований робочою групою IEEE 802.15.1 відповідно до загальної структурою стандартів IEEE 802.

У технології Bluetooth використовується концепція пікомережі. Ця назва підкреслює невелику зону покриття, від 10 до 100 м, в залежності від потужності випромінювання передавального пристрою. У пікомережу може входити до 255 пристроїв, але тільки 8 з них можуть в кожен момент часу бути активними і обмінюватися даними. Один з пристроїв у пікомережі є головним, інші – підлеглими.

Головний пристрій відповідає за доступ до середовища пікомережі, яка представляє собою спектр частоти, що не потребує ліцензування діапазону 2,4 ГГц. Дані при цьому передаються зі швидкістю до 3 Мбіт / с, але через витрат на заголовки пакетів і зміну частот корисна швидкість передачі даних у середовищі не перевищує 2,1 Мбіт / с. Пропускна здатність ність середовища ділиться головним пристроєм між сімома підлеглими пристроями на основі техніки TDM.

Приєднання до пікомережі відбувається динамічно. Головний пристрій пікомережі, викотовуючи процедуру опитування, збирає інформацію про пристрої, які потрапляють в зону видимості його пікомереж. Після виявлення нового пристрою головний пристрій проводить з ним переговори. Якщо бажання підлеглого пристрою приєднатися до пікомережі збігається з рішенням головного пристрою (підлеглий пристрій пройшлов перевірку автентичності і виявився в списку дозволених пристроїв), то новий підлеглий пристрій приєднується до мережі.

Мережа Bluetooth використовує техніку розширення спектру FHSS. Колізії, хоча і з дуже невеликою ймовірністю, все ж таки можуть відбуватися,

коли два або більше пристрої з різних пікомереж виберуть для роботи один і той самий частотний канал.

Для надійної передачі даних в технології Bluetooth може виконуватися пряма коррекция помилок (FEC), а одержання кадру підтверджується за допомогою квитанцій.

У мережах Bluetooth для передачі інформації двох типів використовуються різні методи .

Для чутливого до затримок трафіку (наприклад, голос) мережа підтримує синхронний канал, орієнтований на з'єднання (Synchronous connection-Oriented link, SCO). Цей канал працює на швидкості 64 Кбіт / с. Для каналу SCO пропускна здатність резервується на весь час з'єднання.

Для еластичного трафіку (наприклад, комп'ютерних даних) використовується працюючий зі змінною швидкістю асинхронний канал, не орієнтований на з'єднання (Asynchronous connection-Less link, ACL). Для каналу ACL пропускна здатність виділяется за запитом підлеглого пристрою або за потребою головного пристрою.

При приведенні стандартів Bluetooth у відповідність з архітектурою стандартів IEEE 802 робоча група 802.15.1 обмежилася тільки так званими протоколами ядра Bluetooth, які відповідають функцій фізичного рівня та рівня MAC (Рисунок 1.6).

Фізичний рівень описує частоти та потужності сигналів, що використовуються для передачі інформації.

Рівень базового діапазону частот відповідає за організацію каналів передачі даних у радіосередовищі. У його обов'язки входять вибір послідовності псевдовипадковою перебудови частоти, синхронізація пристроїв у пікомережі, формування і передача кадрів за встановленими каналами SCO і ACL. Кадр Bluetooth має змінну довжину, поле даних може містити від 0 до 2744 біт (343 байт). Для передачі голосу використовуються кадри фіксованого розміру з полем даних 240 біт (30 байт).

Диспетчер каналів відповідає за аутентифікацію пристроїв і шифрування трафіку, а також управляє статусом пристроїв, тобто може зробити підлеглий пристрій головним, і навпаки.

1.3 Бездротові локальні мережі WLAN

Самий найпоширеніший стандарт локальних бездротових мереж – 802.11 або WiFi (від англ. Wireless Fidelity) – торгова марка, що належить Wi-Fi Alliance. Загальновживана назва для стандарту бездротового (радіо) зв'язку передачі даних, який об'єднує декілька протоколів та ґрунтується на сімействі стандартів IEEE 802.11:

IEEE802.11a — стандарт бездротових локальних мереж, Працює в діапазоні 5 ГГц. Максимальна швидкість обміну даними складає 54 Мбіт/с.

IEEE802.11b — працює в діапазоні 2,4 Ггц. У всьому діапазоні існує три непересічні канали, тобто на одній території, не впливаючи один на одного, можуть працювати три різні бездротові мережі. У стандарті передбачено два типи модуляції — DSSS і FHSS. Максимальна швидкість роботи складає 11 Мбіт/с.

IEEE802.11g — найпоширеніший стандарт бездротових локальних мереж, заснований на бездротовій передачі даних в діапазоні 2,4 Ггц. Діапазон також розділений на три непересічні канали. Для збільшення швидкості обміну даними застосований метод модуляції з ортогональним частотним мультиплексуванням (OFDM, Ortogonal Frequency Division Multiplexing), а також метод двійкового пакетного згорткового кодування PBCC (Packet Binary connvolutional Coding).

IEEE802.11e (QoS, Quality of service) — додатковий стандарт, що дозволяє забезпечити гарантовану якість обміну даними шляхом перестановки пріоритетів різних пакетів; необхідний для роботи таких потокових сервісів як VoIP або IP-TV.

IEEE802.11i — стандарт, що знімає недоліки в області безпеки попередніх стандартів. 802.11i вирішує проблеми захисту даних канального рівня і дозволяє створювати безпечні бездротові мережі практично будь-якого масштабу.

IEEE802.11n — стандарт бездротових локальних мереж останнього покоління, заснований на бездротовій передачі даних в діапазоні 2,4 Ггц.

Стандарт 802.11n значно перевищує за швидкістю обміну даними попередні стандарти 802.11b і 802.11g, забезпечуючи швидкість на рівні 50 Мбайт; зворотньо сумісний з 802.11b і 802.11g (рис. 1.7).

Рисунок 1.7 Радіус дії стандартів b g n

Зазвичай схема Wi-Fi мережі містить не менш однієї точки доступу і не менше одного клієнта. Ядром бездротової мережі WiFi є так звана точка доступу (Access Point), яка підключається до проводової мережевої інфраструктури та забезпечує передачу радіосигналу. Також можливе підключення двох клієнтів в режимі точка-точка (Ad-hoc), коли точка доступу не використовується, а клієнти з'єднуються за участю мережевих адаптерів «напряму». Максимальна дальність передачі сигналу у такій мережі становить 100 метрів, однак на відкритій місцевості вона може досягати до 300—400 м. Дальність залежить від потужності передавача (яка в окремих моделях обладнання регулюються програмно), наявності та характеристики перешкод, типу антени.

Розглянемо протоколи захисту бездротового трафіку які використовуються в мережах стандарту 802.11.

Технологія WEP (Wired Equivalent Privacy) була розроблена спеціально для шифрування потоку даних, що передаються в локальній мережі. Проте в ній використовується не найстійкіший алгоритм RC4 на статичному ключі. Існує 64 -, 128 -, 256 - і 512-бітове шифрування. Для посилення захисту частину ключа (від 40 біт в 64-бітному шифруванні) є статичною, а інша частина - динамічної, так званий вектор ініціалізації (Initialization Vector або IV), змінюється в процесі роботи мережі. Цей вектор 24-бітний. Основний вразливістю WEP є те, що вектор ініціалізації повторюється через певний проміжок часу (24 біта - близько 16 мільйонів комбінацій). Зломщикові буде потрібно лише зібрати ці повтори і за секунди зламати решту ключа. Після чого він входить в мережу, як звичайний зареєстрований користувач.

WPA (Wi-Fi Protected Access) - стійкіший алгоритм шифрування, ніж WEP. Високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC.

TKIP - протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol) – передбачає присвоєння кожному пристрою змінюваний ключ.

MIC - технологія перевірки цілісності повідомлень (Message Integrity Check) - захищає від перехоплення пакетів і їх перенаправленння. Протокол TKIP використовує автоматично підібрані 128-бітові ключі, які створюються псевдовипадковим способом, і загальна кількість їх варіацій сягає 500 мільярдів. Використовується складна ієрархічна система алгоритму підбору ключів і динамічна їх заміна через кожні 10 KB (10 тис. переданих пакетів) роблять систему максимально захищеною. MIC використовує достатньо складний математичний алгоритм, який дозволяє звіряти відправлені в одній і отримані в іншій точці дані. Якщо виявлені зміни і результат порівняння не сходиться, такі дані вважаються помилковими і відкидабться. Існує два види WPA:

WPA-PSK (Pre-shared key) - для генерації ключів мережі і для входу в мережу використовується ключова фраза. Оптимальний варіант для домашньої або невеликої офісної мережі.

WPA-802.1x - вхід в мережу здійснюється через сервер аутентифікації. Оптимально для мережі великої компанії.

WPA2 багато в чому побудований на основі попередньої версії, WPA. Стандарт передбачає застосування шифрування AES, аутентифікації 802.1x, а також захисних специфікацій RSN і CCMP. WPA2 істотно підвищує захищеність Wi-Fi-мереж в порівнянні з попередніми технологіями. За аналогією з WPA, WPA2 також ділиться на два типи: WPA2-PSK і WPA2-802.1x.

IEEE 802.1x - стандарт, за основу якого взято виправлення недоліків технологій безпеки, що застосовуються в 802.11, зокрема можливість злому WEP, залежність від технологій виробника і т. д. 802.1x передбачає підключення до мережі навіть PDA-пристроїв, що дозволяє більш вигідно використовувати саму ідею бездротового зв'язку. З іншого боку, 802.1x і 802.11 є сумісними стандартами. 802.1x базується на наступних протоколах:

EAP (Extensible Authentication Protocol). Протокол розширеної аутентифікації. Використовується спільно з RADIUS-сервером у великих мережах.

TLS (Transport Layer Security). Протокол, який забезпечує цілісність і шифрування переданих даних між сервером і клієнтом, їх взаємну аутентифікацію, запобігаючи перехоплення і підміну повідомлень.

RADIUS (Remote Authentica-tion Dial-In User Server). Сервер аутентифікації користувачів за логіном і паролем.Также з'явилася нова організація роботи клієнтів мережі. Після того як користувач пройшов етап аутентифікації, йому висилається секретний ключ в зашифрованому вигляді на певний незначний час - термін чинного на даний момент сеансу. По його завершенні генерується новий ключ.

VPN з самого початку його розробки не був розрахований для роботи з Wi-Fi, проте його можна достатньо ефективно застосувати і до Wi-Fi мережі. Для шифрування трафіку в VPN найчастіше застосовується протокол IPSec (близько 70% випадків), рідше - PPTP або L2TP. При цьому можуть використовуватися такі алгоритми, як DES, Triple DES, AES і MD5. VPN підтримується на багатьох платформах (Windows, Linux, Solaris) як програмними, так і апаратними засобами. Варто відзначити високу надійність - поки що ще не зафіксовано випадків злому VPN-мереж. Зазвичай VPN рекомендується застосовувати у великих корпоративних мережах, для домашнього користувача встановлення та налаштування може здатися занадто громіздкою і трудомісткою. При застосуванні технології доведеться пожертвувати близько 35% пропускної здатності каналу.

1.4 Бездротові мережі масштабу міста WMAN

При всьому різноманітті бездротових технологій складно одночасно дотримати три основні вимоги до мережі: висока пропускна здатність, надійність і мобільність. Вирішити таке завдання може наступне покоління бездротових технологій - WiMAX (Worldwide Interoperability for Microwave Access), стандарт IEEE 802.16.

У загальному WiMAX мережі складаються з наступних основних частин — базових і абонентських станцій, а також обладнання, що зв'язує базові станції між собою з постачальником сервісів і з Інтернетом.

Для з'єднання базової станції з абонентською використовується високочастотний діапазон радіохвиль від 1,5 до 11 ГГц. В ідеальних умовах швидкість обміну даними може досягати 70 Мбіт / с, при цьому не вимагається забезпечення прямої видимості між базовою станцією і приймачем. Як вже зазначалось, WiMAX застосовується як для вирішення проблеми «останньої милі», так і для надання доступу в мережу офісним та

районним мережам. Між базовими станціями встановлюються з'єднання (прямої видимості), що використовують діапазон частот від 10 до 66 ГГц, швидкість обміну даними може досягати 120 Мбіт / с. При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних дротових з'єднань. Однак, чим більше число БС підключено до мереж провайдера, тим вища швидкість передачі даних і надійність мережі в цілому.

Стандарт IEEE 802.16 визначає протокол PKM (Privacy and Key Management protocol), протокол конфіденційності і управління ключем. Застосовується захищене з'єднання (Security Association, SA) - одностороннє з'єднання для забезпечення захищеної передачі даних між пристроями мережі. SA бувають двох типів:

Захищений зв'язок для даних (Data Security Association).

Захищений зв'язок для авторизації (Authorization Security Association).

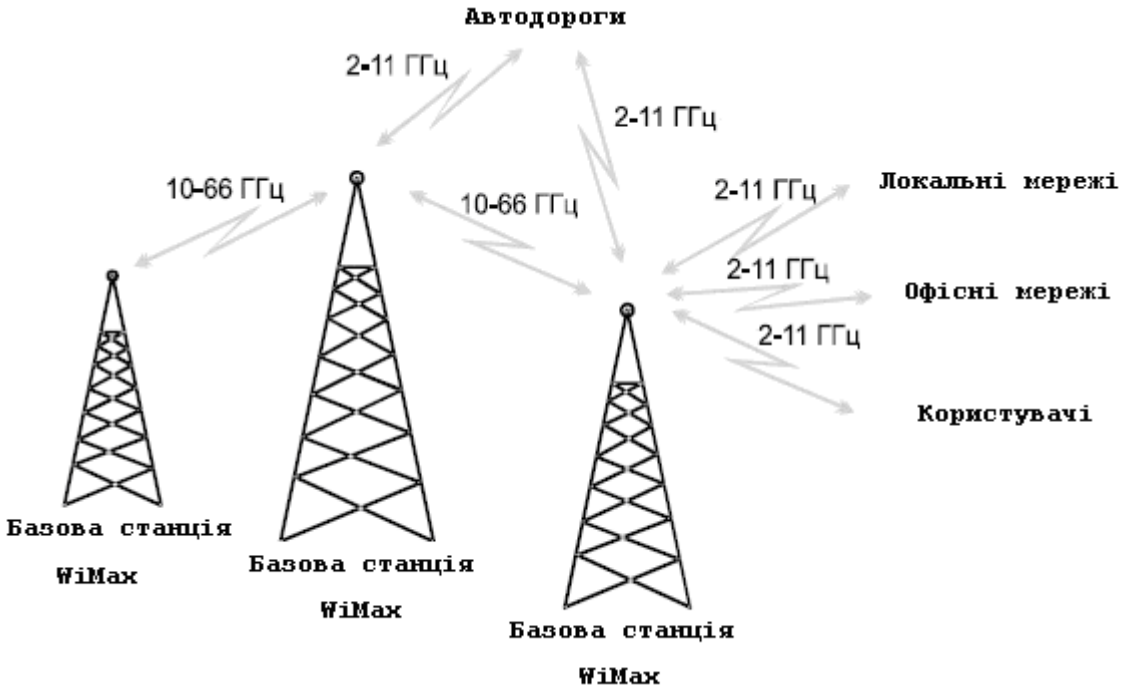

Рисунок 1.8 Схема мережі WiMAX

Захищений зв'язок для даних буває трьох типів:

Первинний (основний) (Primary SA);

Статичний (Static SA);

Динамічний (Dynamic SA).

Первинний захищений зв'язок встановлюється абонентською станцією на час процесу ініціалізації. Базова станція потім надає статичний захищений зв'язок. Що стосується динамічних захищених зв'язків, то вони встановлюються та ліквідуються в міру необхідності для сервісних потоків. Як статичні, так і динамічні захищені зв'язку можуть бути однією для декількох абонентських станцій.

Захищений зв'язок для даних визначається:

16-бітним ідентифікатором зв'язку.

Методом шифрування, застосовуваним для захисту даних при з'єднанні.

Двома ключами шифрування трафіку (Traffic Encryption Key, TEK), поточний і той, який буде використовуватися, коли в поточного TEK закінчиться термін життя.

Двома двухбітними ідентифікаторами, по одному на кожен TEK.

Часом життя TEK. Може мати значення від 30 хвилин до 7 днів. Значення за замовчуванням 12 годин.

Двома 64-бітними векторами ініціалізації, по одному на TEK (необхідні для алгоритму шифрування DES).

Індикатором типу зв'язку (первинна, статична або динамічна).

Захищена зв'язок для авторизації

Захищена зв'язок для авторизації визначається:

Сертифікатом X.509, що ідентифікує абонентську станцію, а також сертифікатом X.509, що ідентифікує виробника абонентської станції.

160-бітовим ключем авторизації (authorization key, AK), який використовується для аутентифікації під час обміну ключами TEK.

4-бітовим ідентифікатором ключа авторизації.

Часом життя ключа авторизації, може приймати значення від 1 дня до 70 днів. Значення за замовчуванням 7 днів.

128-бітовим ключем шифрування ключа (Key encryption key, KEK). Використовується для шифрування та розподілу ключів TEK.

Ключем HMAC для низхідних повідомлень (downlink) при обміні ключами TEK.

Ключем HMAC для висхідних повідомлень (uplink) при обміні ключами TEK.

Аутентифікація може бути односторонньою (мережа перевіряє справжність користувача) або взаємної (мережа перевіряє справжність користувача і користувач перевіряє справжність мережі).

Аутентифікуватись може як пристрій (device authentication), так і користувач (user authentication) або обидва: пристрій і користувач. Для ідентифікації пристрою використовується його MAC адрес. Для ідентифікації користувача застосовується імя користувача та пароль (user name/password) або SIM, USIM.

Global System for Mobile Communications (GSM) - найпопулярніша технологія рухомого зв'язку у світі. За даними деякими даними мережі GSM налічують більш 747.5 млн. абонентів в 184 країнах.

Назва GSM сталося групи (Group Special Mobile), яка була сформована в 1982 році європейської конференцією CEPT (connference of Post and Telecommunications Administrations), для того щоб розробити систему стільникового зв'язку, яка б замінила існуючі системи 1 покоління. Але коли в 1991 розпочала роботу перша мережа GSM абревіатура "GSM" була перейменована в Global System for Mobile Communications.

Мобільна станція, складається з двох принципових частин: обладнання користувача (телефон, GSM модуль в ноутбуці, КПК чи машині) і SIM (Subscriber Identity Module) карти.

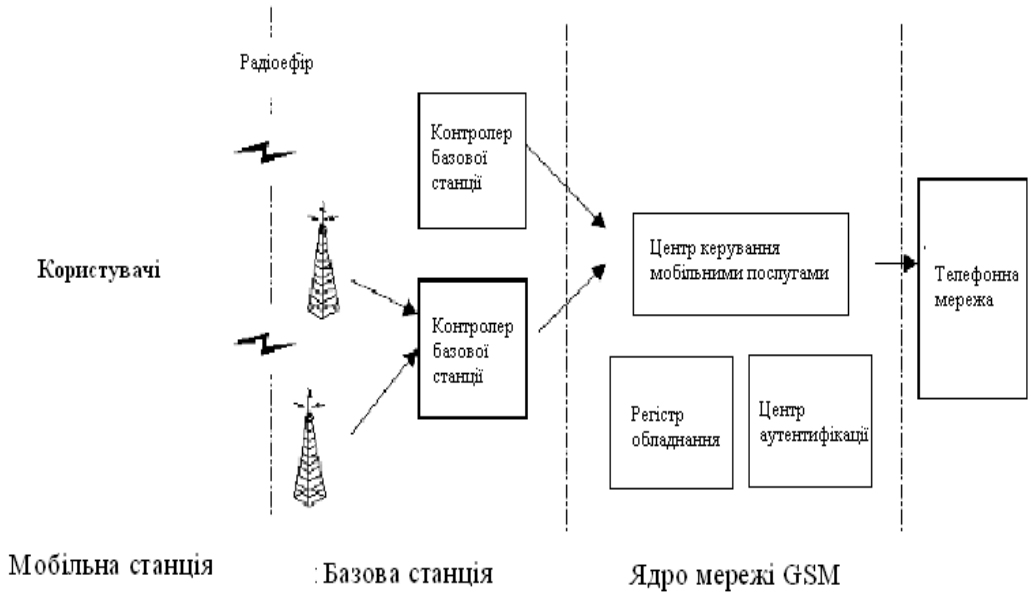

Рисунок 1.9 Структупна схема мережі GSM

Підсистема базових станцій складається з самих базових станцій (Base Transceiver Station ,BTS) і контролер базових станцій (Base Station conntroller, BSC). Базова станція являє собою антену і передавач, який зв'язується з мобільною станцією. Контролер базових станцій керує ресурсами радіоефіру однієї або декількох базових станцій. Він відповідає за радіоканали, розподіл частот, переключення абонентів між станціями. Також контролер базових станцій здійснює перетворення голосового потоку з 64кБіт/с (дротова телефонна мережа) у 13кБіт/с (мобільна мережа).

Ядром мережі є центр управління мобільними послугами (Mobile services Switching Center, MSC)). Він працює як АТС у звичайній дротовій мережі, а також він виконує реєстрацію, аутентифікацію, відстеження абонента, переключення його між стільниками, роумінг. Але основне його завдання це з'єднання зі звичайною проводовою мережею за допомогою сигнальної системи 7 (Signalling System Number 7, SS7) .

Регістр обладнання (Equipment Identity Register, EIR) - це база даних, яка містить список всіх допустимих мобільних пристроїв. Кожен пристрій ідентифікується за допомогою номера IMEI (International Mobile Equipment

Identity) номера. Якщо телефон крадений або призначений для використання в іншій країні, то він буде позначений як сірий і не зможе підключитися до мережі.

Так як у мережах рухомого зв'язку дані передаються по радіоканалу, то можуть бути дуже легко прослухані (що й відбувалося в аналогових мережах першого покоління).

Основні цілі захисту даних в GSM мережах запобігають:

Доступ неавторизованих користувачів до сервісів мережі

Прослуховування розмови третіми особами

Наведемо функції захисту які вбудовані в стандарт GSM:

Аутентифікація абонентів відбувається тільки для зареєстрованих абонентів

Захищена передача даних(шифрування)

Мобільний телефон не працює без SIM карти

Дублювання SIM карти заборонено

У стандарті GSM процедура автентифікації пов’язана з використанням модуля ідентифікації абонента (SIM). Модуль SIM – це знімний модуль, що встановлюється у відповідне гніздо абонентського апарату.

Модуль SIM містить персональний ідентифіка- ційний номер абонента (Personal Identification Number – PIN), міжнародний ідентифікатор абонента мобільного зв’язку (International Mobile Subscriber Identity – IMSI), індивідуальний ключ автентифікації абонента Ki, індивідуальний алгоритм автентифікації абонента A3, алгоритм обчислення ключа шифрування A8.

Для автентифікації використовується зашифрований відгук (signed response) S, що є результатом застосування алгоритму A3 до ключа Ki і квазівипадкового числа R, яке рухома станція отримує від центра автентифікації через центр комутації. Алгоритм A8 використовується для знаходження ключа шифрування повідомлень.

Унікальний ідентифікатор IMSI для поточної роботи замінюється тимчасовим ідентифікатором абонента мобільного зв’язку (Temporary Mobile Subscriber Identity, TMSI), який присвоюється радіотелефону при його першій реєстрації у конкретному регіоні, що визначається ідентифікатором області місцеположення (Location Area Identity, LAI), і анулюється при виході апарату за межі цього регіону.

Ідентифікатор PIN – це код, відомий тільки абонентові, який має служити захистом від несанкціонованого використання SIM-карти, наприклад при її втраті. Після трьох невдалих спроб набору PIN-кода SIM-карта блокується, а блокування може бути знято або набором додаткового коду – персо- нального коду розблокування (Personal unblocking key – PUK), або за командою з центру комутації.

До бездротових глобальних мереж відносяться також мережі мобільного звязку третього покоління (3rd Generation, 3G) —набір послуг, котрий включає до себе як високошвидкісний мобільний доступ до послуг мережі Інтернет, так і технологію радіозв'язку.

Мережі третього покоління працюють на частотах дециметрового діапазону (близько 2 ГГц), швидкість передачі даних становить понад 2 Мбіт/с. Такі мережі надають можливість організувати відеозв'язок, дивитись на мобільному телефоні фільми й телепрограмми та ін. В світі існує два стандарти 3G: UMTS (чи W-CDMA) та CDMA-2000. UMTS більш розповсюджений в основному в Європі, CDMA2000 — в Азії та США.

В основі мережі лежить ядро з комутацією пакетів, яке сполучається з зовнішньою мережею Інтернет. Цей факт робить мережу вразливою для нових типів атак, таких як DOS атаки, віруси, черв'яки і т.д., які поширені в мережі Інтернет.

1.5 Постановка задачі

Метою даної дипломної роботи є створення, налаштування та захист локальної мережі організації. Для досягнення поставленої мети необхідно провести аналіз стандартів локальних мереж на предмет діапазону покриття, швидкості передачі, методів захисту. Крім того необхідно дослідити типи атак на мережі та проаналізувати ефективні способи захисту від них. В даній роботі необхідно спланувати структуру та компоненти локальної мережі. І для ефективного функціонування даної мережі в дипломній роботі необхідно:

- Провести аналіз та використати одне із типів з'єднань з точкою доступу
- Забезпечити захист унікального ідентифікатора
- Відключимо можливість доступу до настройок точки доступу через бездротове з'єднання
- Вибрати спосіб аутентифікації користувачів.
- Використати найбільш стійкий потік шифрування даних.
- Проаналізувати та використати найбільш криптостійкі паролі.
- Вивчити ринок серверів та налаштувати один з серверів для точки доступу.

2. ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ СТРУКТУРИ КАБЕЛЬНИХ ТА БЕЗДРОТОВИХ МЕРЕЖ

2.1 Принципова схема бездротової комп'ютерної мережі та її безпека

Будемо притримуватися зіркоподібної мережі, відомої як типова обчислювальна, в якій в центрі зірки розташована обчислювальна машина (в нашому випадку центр розділений на 3 сервери) , яка обробляє інформацію, що передається перефирійними пристроями, як телефонна система, в якій центральний вузол представляє собою комутатор, який з'єднує різних користувачів мережі. (рис. 2.1)

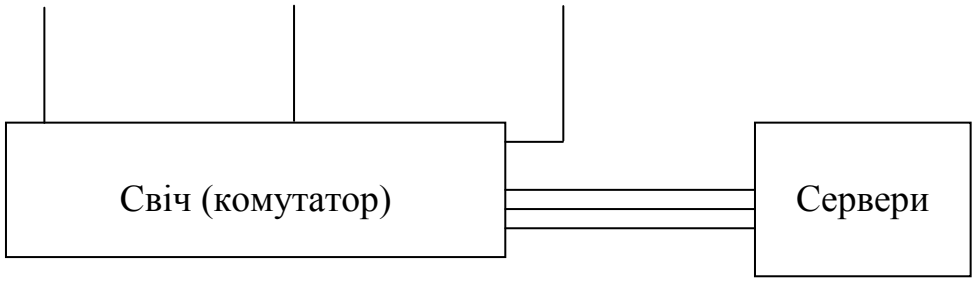

Рисунок 2.1 Типова обчислювальна зіркоподібна мережа

Нам необхідна принципова схема організації бездротової мережі з тим, щоб інтегрувати її в існуючу локальну мережу. Загальний вигляд принципової схеми організації бездротової мережі з використанням Wi-Fi технологій має наступній вигляд. (рис. 2.2).

В даній комп'ютерній мережі ми маємо 3 серверні компьютери на базі операційної системи Windows Server 2008, на яких розташовано наступні програмні сервери: почтовий, WEB, Proxy, FTP та Баз Даних. Крім того, для доступу в глобальну мережу інтернет через модем використовується Kerio FireWall .

Головне завдання, яке ставилось в даній дипломній роботі є технології створення захищеної Wi-Fi мережі. Для досягнення даної мети необхідно

спроектувати мережу таким чином, щоб максимально захистити Wi-Fi мережу від несанкціонованого доступу, втрати інформації та некоректностей роботи мережі. Для цього ми, згідно з принциповою схемою бездротової комп'ютерної мережі, встановлюємо чотири точки доступу та сервер радіус, що з'єднує їх зі свічем за допомогою кабеля UTP 5e.

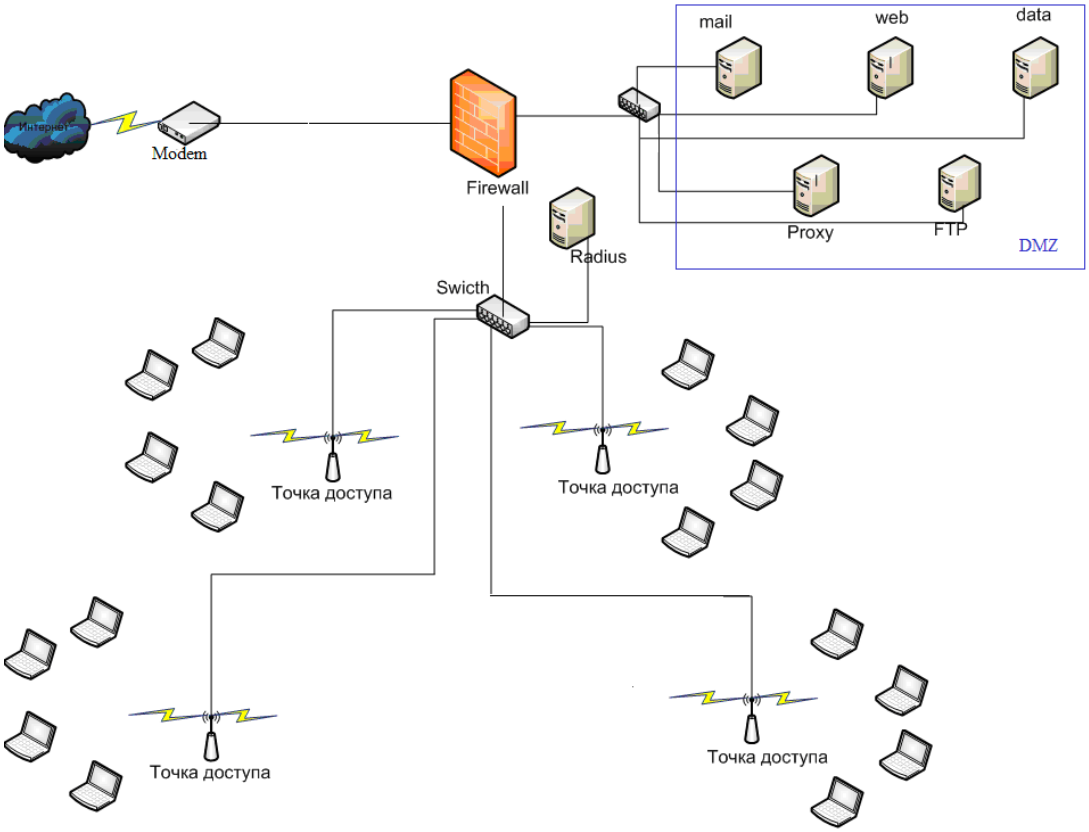

Рисунок 2.2 Принципова схема бездротової комп'ютерної мережі

Безпеці захисту конфіденційної інформації в бездротових мереж варто надавати особливу увагу. Адже бездротова мережа має великий радіус дії, і тому зловмисник може перехоплювати інформацію або ж атакувати мережу, знаходячись на безпечній відстані. В наш час існує безліч різних способів захисту і, за умови правильного налаштування, можна бути упевненим в забезпеченні необхідного рівня безпеки.

До числа основних способів захисту мереж можна віднести наступні:

1. Фільтрація MAC адрес: в цьому випадку адміністратор складає список MAC адрес мережевих карт клієнтів. У разі декількох AP необхідно передбачити, щоб MAC адреса клієнта існувала на всіх, щоб він міг безперешкодно переміщатися між ними. Проте цей метод дуже легко перемогти, так що поодинці його використовувати не рекомендується.

2. SSID (Network ID) – використовування системи мережевих ідентифікаторів. При спробі клієнта підключитися до AP на нього передається семизначний алфавітно-цифровий код; використовуючи мітку SSID можна бути упевненим, що до мережі зможуть під'єднатися тільки клієнти, що знають його.

3. Firewall: доступ до мережі повинен здійснюватися за допомогою IPSec, secure shell або VPN, брандмауер повинен бути налаштований на роботу саме з цими мережевими з'єднаннями

4. AccessPoint – точку доступу треба настроювати на фільтрацію MAC адрес, крімо того, фізично сам пристрій необхідно ізолювати від оточуючих.

Рекомендується також конфігурувати крапку тільки по telnet, відключивши можливість конфігурації через браузер або SNMP.

2.1.1 Налаштування фільтрації MAC-адрес

Один із способів обмеження доступу в безпровідну мережу – визначити пристроям різний рівень привілеїв доступу в мережу. Для цього застосовується фільтрація MAC-адрес.

Фільтрація MAC-адрес дозволяє задати перелік пристроїв, що має дозвіл на з'єднання з безпровідною мережею, за допомогою їх MAC-адрес. При кожній спробі безпровідного клієнта встановити з'єднання або асоціюватися з точкою доступу він повинен передати свою MAC-адресу. Якщо включена функція фільтрації за MAC-адресам, то безпровідний маршрутизатор або точка

доступу виконає пошук MAC-адреса цього пристрою за своїм заздалегідь заданим списком. Дозвіл на з'єднання отримають лише ті пристрої, чиї MAC-адреси були заздалегідь прописані в базі даних маршрутизатора. Якщо MAC-адреса не знайдена в базі даних, пристрою буде відмовлено у встановленні з'єднання або в доступі в безпровідну мережу. (рис. 2.3)

Такий тип забезпечення безпеки має деякі недоліки. Наприклад, він передбачає, що MAC-адреси всіх пристроїв, яким має бути наданий доступ в мережу, включені в базу даних до того, як буде виконана спроба з'єднання. Пристрій, не розпізнаний по базі даних, не зможе виконати з'єднання. При цьому зломщик може створити клон MAC-адреси пристрою, що має доступ в мережу.

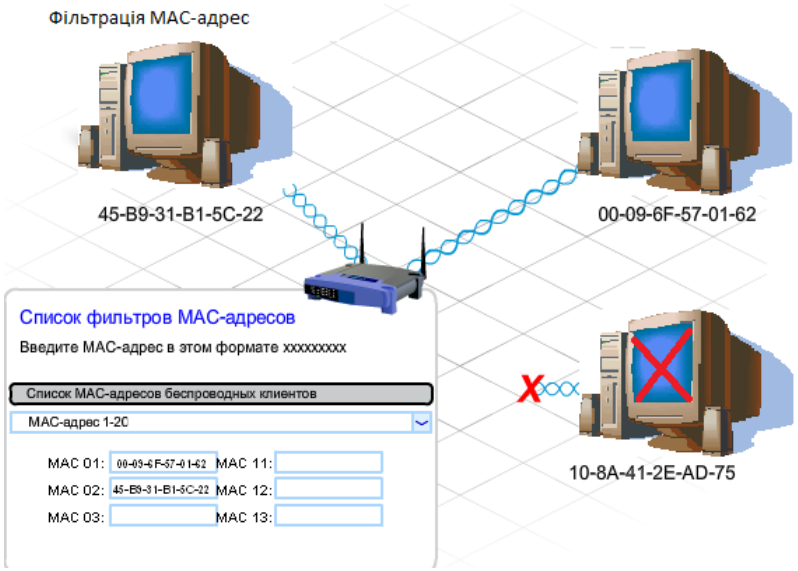

Рисунок 2.3 Фільтрація MAC-адрес

2.1.2 Зміна значення SSID (заданого за замовчуванням)

Всі комп'ютери, підключені до безпровідної мережі, повинні використовувати її SSID. За замовчуванням, безпровідні маршрутизатори і точки доступу розсилають ідентифікатори SSID всім комп'ютерам в межах дії безпровідної мережі. Якщо функція розсилки SSID активована, то будь-який безпровідний клієнт зможе виявити мережу і підключитися до неї, якщо не налагоджені інші функції забезпечення безпеки.

В якості базової міри захисту настійно рекомендується змінити налаштування, задані за замовчуванням. Безпровідні пристрої поставляються із заздалегідь налагодженими SSID, паролями і IP-адресами. Використовуючи налаштування за замовчуванням, зловмисник зможе легко ідентифікувати мережу і дістати доступ.

Навіть якщо відключена розсилка SSID, існує вірогідність проникнення в мережу, якщо зловмисникові став відомий SSID, заданий за замовчуванням. Якщо не змінити інші налаштування за замовчуванням, а саме паролі і IP-адреси, то зломщики можуть проникнути в точку доступу і внести зміни до її конфігурації. Отже, налаштування, задані за замовчуванням, мають бути змінені на безпечніші і унікальні.

2.1.3 Відключення розсилки SSID

За замовчуванням точка доступу повідомляє ідентифікатор мережі всім безпровідним пристроям, що знаходиться в радіусі її дії. При скануванні ефіру безпровідний клієнт може виявити точку доступу і її SSID, після чого підключитися до неї, налаштувавши необхідні параметри. Відповідно, не знаючи SSID-точки доступу, підключитися до неї буде складно хоча за допомогою спеціалізованого програмного забезпечення це можливо.

Функцію розсилки SSID можна відключати. Якщо вона відключена, то відомості про доступність мережі вже не є загальнодоступними. Будь-який комп'ютер, що підключається в мережу, повинен використовувати її SSID. Практично всі точки доступу дозволяють відключити розсилку SSID. Для цього необхідно зайти в налаштування пристрою і змінити значення параметрів.

Запустивши утиліту конфігурації точки доступу, перейдіть на вкладку Wireless (Безпровідна мережа). Щоб заборонити трансляцію ідентифікатора мережі, виберіть із списку SSID Broadcast, що розкривається (Трансляція SSID) значення Disable (Заборонити). (рис. 2.4).

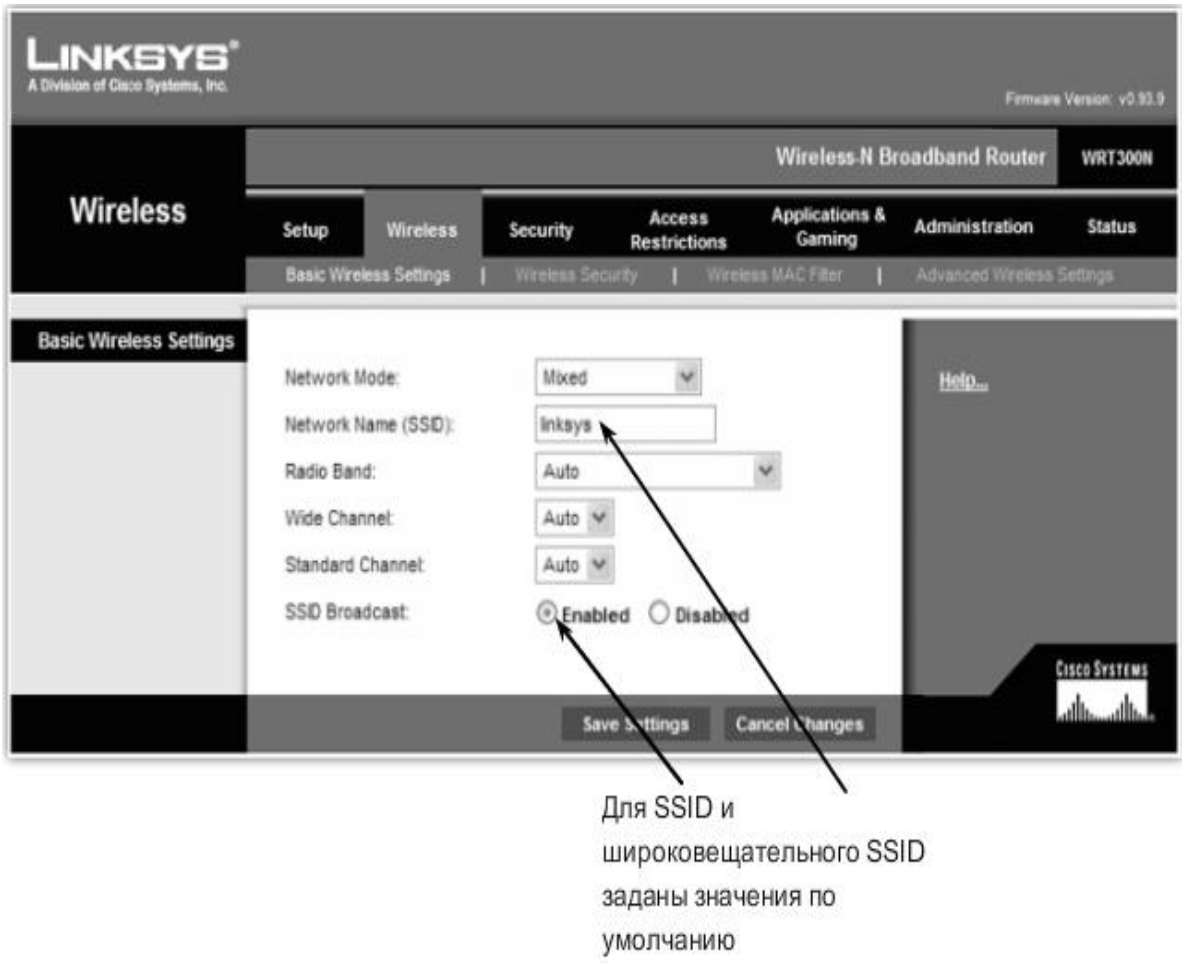

Рисунок 2.4 Значення трансляції SSID за замовчуванням

Ці зміни самі по собі ще не гарантують безпеки вашої мережі. Наприклад, SSID передаються відкритим текстом. Але сьогодні є пристрої для перехоплення безпровідних сигналів і читання повідомлень, складених відкритим текстом. Навіть якщо функція розсилки SSID відключена і значення за замовчуванням змінені, зломщики можуть взнати ім'я безпровідної мережі за допомогою спеціальних пристроїв. Використовуючи цю інформацію, вони зможуть підключитися до мережі. Тому для забезпечення безпеки безпровідної локальної мережі (WLAN) слід використовувати комбінацію з декількох методів захисту.

2.2 Криптографічний механізм WEP

В бездротових мережах застосовуються криптографічні засоби для забезпечення цілісності і конфіденційності інформації. Однак помилки призводять до порушення комунікацій, виникненню загрози криптозахисту і як наслідок, - використанні інформації зловмисниками.

WEP – це криптографічний механізм, створений для безпеки мереж стандарту 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується всіма користувачами. Управляючий доступ до ключів, часта їх зміна і знаходження порушень практично неможливі. Дослідження WEP – шифрування виявило вразливі місця, з яких атакуючий може повністю встановити ключ після захоплення мінімального мереженого трафіку. В Internet є засоби, які дозволяють зловмиснику встановити ключ на протязі кількох годин. Тому на WEP не можна покладатись як на засіб аутентифікаціїі конфіденційності в бездротовій мережі. Використовувати описані криптографічні механізми краще, ніж не використовувати ніяких, але з урахуванням відомої вразливості необхідні інші методи захисту від атак. Усі бездротові комунікаційні мережі підпадають атакам прослуховування в період контакту (встановлення з’єднання, сесії зв’язку і завершення з’єднання). Сама природа бездротового з’єднання не дозволяє його контролювати і тому воно потребує захисту. Управління ключем, як правило викликає додаткові проблеми, коли застосовується при роумінгу і у випадку загального користування відкритою мережею.

Повну анонімність атаки забезпечує бездротовий доступ. Без відповідного обладнання в мережі, що дозволяє виявити місцезнаходження, атакуючий може легко зберегти анонімність і ховатись де завгодно на території дії бездротової мережі. В такому випадку його важко знайти.

В недалекому майбутньому прогнозується погіршення розпізнавання атак в Internet через широке розповсюдження анонімних входів через

небезпечні точки доступу. Вже існують багато сайтів, де публікуються списки таких точок, які можна використати з метою вторгнення. Важливо відмітити, що більшість зловмисників вивчають мережі не для атак на їх внутрішні ресурси, а для отримання безплатного анонімного доступу в Internet, прикриваючись яким вони атакують інші мережі. Якщо оператори зв'язку не приймають мір по захисту від таких нападів, вони повинні нести відповідальність за втрати, причинені іншим мережам при використанні їх доступу до Internet.

2.3 Фізичний захист

Щодо фізичного захисту – сюди належить використання невеликих і переносних пристроїв бездротового доступу до мережі (КПК, ноутбуки), як точки доступу. Крадіжка таких пристроїв в багатьох випадках приводить до того, що зловмисник може потрапити до мережі не використовуючи складних атак, так як основні механізми аутентифікації в стандарті 802.11 розраховані на реєстрацію саме фізичного апаратного пристрою, а не облікового запису користувача. Тому втрата одного мереженого інтерфейсу і несвоєчасне оповіщення адміністратора може призвести до того, що зловмисник отримає доступ до мережі без особливих проблем.

Дамо формулювання визначенням, що стосуються теми мого диплому.

Аутентифікація: визначення джерела інформації, тобто кінцевого користувача чи пристрою (центрального комп'ютера, сервера, комутатора, маршрутизотора тощо).

Конфіденційність даних: забезпечення доступу даних тільки для осіб, які мають право на доступ до цих даних.

Шифрування: метод зміни інформації таким чином, що прочитати її не може ніхто, крім адресату, який повинен її розшифрувати.

Ключ: цифровий код, який може використовуватись для шифрування і розшифрування інформації, а також для її підпису.

Шифр: будь-який метод шифрування даних.

Цифровий підпис: послідовність біт, що додається до повідомлення і забезпечує аутентифікацію і цілісність даних.

2.4 Зниження потужності передавача

Як відомо, кожен безпровідний пристрій передає дані за допомогою приймача і передавача радіохвиль. Від потужності передавача залежить радіус безпровідної мережі, а від чутливості приймача — якість сприйняття сигналу. Оскільки радіохвилі — річ неконтрольована і ніколи не можна передбачити, хто може їх приймати, непоганим варіантом захисту мережі є підбір потужності передавача достатньої для покриття всієї радіомережі. При цьому ви відсікаєте недоброзичливців, які можуть приєднатися до вашої мережі, знаходячись, наприклад, за стінкою сусіднього будинку або в машині на стоянці, розташованій поряд з офісом.

Інша перевага такого підприємства — економія енергії, що важливо для переносних комп'ютерів і пристроїв. Щоб вибрати рівень потужності сигналу, запустите утиліту конфігурації точки доступу і перейдіть в її вікні на вкладку Wireless (Безпровідна мережа). Зверніть увагу на параметр Tx Power (Потужність сигналу), якому можна привласнити наступні значення: Full (Повна потужність), Half (Половина потужності), Quarter (Чверть потужності), Eighth (Восьма частина потужності) або Min (Мінімальна потужність). Відразу встановлювати дуже низьку потужність не варто, оскільки так можна «обрубати» зв'язок з деякими віддаленими комп'ютерами. Зменшувати потужність потрібно поступово. Не слід встановлювати потужність, яка є пороговою для роботи пристрою, оскільки в певних умовах сигнал може ослабіти, що приведе до відключення деяких віддалених комп'ютерів.

2.5 Стек протоколів і їх коротка характеристика

Тема безпеки бездротових мереж як і раніше залишається актуальною, хоча вже достатньо давно існують надійні (на даний момент) методи захисту цих мереж. Мова йде про технології WPA (Wi-Fi Protected Access).

Технологія WPA, призначена тимчасово (в очікуванні переходу до 802.11i) закрити недоліки попередньої технології WEP і складається з кількох компонентів:

- протокол 802.1x – універсальний протокол для аутентифікації, авторизації і обліку (AAA);
- протокол EAP – розширюємий протокол аутентифікації (Extensible Autentification Protocol);
- протокол TKIP – протокол часової цілісності ключів, інший варіант перекладу – протокол цілісності ключів в часі (Temporal Key Integrity Protocol);
- MIC – криптографічна перевірка цілісності пакетів (Message Integrity Code);
- протокол RADIUS.

За шифрування даних у WPA відповідає протокол TKIP, який використовує той же алгоритм шифрування – RC4, що і в WEP, але на відміну від нього використовує динамічні ключі (тобто ключі часто міняються). TKIP використовує криптографічну контрольну суму (MIC) для підтвердження цілісності пакетів.

RADIUS - протокол призначений для роботи в парі з сервером аутентифікації, в якості якого звичайно виступає RADIUS – сервер. В цьому випадку бездротові точки доступу працюють в enterprise – режимі.

Якщо в мережі відсутній RADIUS – сервер, то роль сервера аутентифікації виконує сама точка доступу – так званий режим WPA-PSK (загальний ключ). В цьому режимі в настройках усіх точок доступу попередньо

прописується загальний ключ. Він же прописується і на клієнтських бездротових пристроях. Такий метод захисту достатньо надійний (відносно WEP), але досить незручний з точки зору управління. PSK - ключ необхідно прописувати на всіх бездротових пристроях, користувачі яких його можуть бачити. При необхідності заблокувати доступ до мережі якомусь клієнту потрібно заново прописувати новий PSK на всіх пристроях мережі. Інакше кажучи, режим WPA-PSK підходить для домашньої мережі і, можливо, для невеликого офісу, але не більше.

Технологія WPA використовувалася тимчасово до вводу в дію стандарту 802.11i. Частина виробників до офіційного прийняття цього стандарту ввели у використання технологію WPA2, в якій в тій чи іншій мірі використовуються технології з 802.11i. Використання протоколу CCMP замість TKIP в якості алгоритму шифрування там використовується удосконалений стандарт шифрування AES (Advanced Encryption Standard). А для управління і розподілу ключів як і раніше протокол 802.1x.

Як вже було сказано, протокол 802.1x може виконувати кілька функцій. В моєму випадку нас цікавлять функції аутентифікації користувача і розподілу ключів шифрування. Слід відмітити, що аутентифікація виконується на рівні порта", - тобто доки користувач не буде аутентифікований, йому дозволено відправляти/приймати пакети, що стосуються тільки процесу його аутентифікації (обліку даних) і не більше. І тільки після успішної аутентифікації порт пристрою (будь то точка доступу чи розумний комутатор) буде відкритий і користувач отримає доступ до ресурсів мережі.

Функції аутентифікації покладаються на протокол EAP, який сам по собі є лише каркасом для методів аутентифікації. Вся перевага протоколу в тому, що його досить просто реалізувати на аутентифікаторі (точці доступу), так як їй не потрібно знати ніяких специфічних особливостей різних методів аутентифікації. Аутентифікатор служить передаточним ланцюгом між клієнтом

і сервером аутентифікації. Самих методів аутентифікації існує достатньо багато:

- EAP-SIM, EAP-AKA – використовується в мережах GSM мобільного зв’язку;
- LEAP – пропреоретарний метод від Sisco systems;
- EAP-MD5 – простіший метод, аналогічний CHAP (не стійкий);
- EAP-MSCHAP V2 – метод аутентифікації на основі логін – пароля користувача в MS – мережах;
- EAP-TLS – аутентифікація на основі цифрових сертифікатів;
- EAP-SecureID – метод на основі однократних паролів.

Крім перерахованих слід відмітити наступні два методи, EAP-TTLS і EAP-PEAP. На відміну від попередніх, ці два методи перед безпосередньою аутентифікацією користувача спочатку утворюють TLS – тунель між клієнтом і сервером аутентифікації. А вже всередині цього тунеля здійснюється сама аутентифікація, з використанням як стандартного EAP (MD5, TLS), чи старих не – EAP методів (PAP, CHAP, MS-CHAP, MS-CHAP v2), останні працюють тільки з EAP-TTLS (PEAP використовується тільки сумісно з EAP методами). Попереднє тунелювання підвищує безпеку аутентифікації, захищаючи від атак типу “man-in-middle”, “session hihacking” чи атаки по словнику.

На рисунку 2.5 показана структура EAP кадра. Протокол PPP засвітився там тому, що з самого початку EAP планувався до використання поверх PPP тунелей. Але так як використання цього протоколу тільки для аутентифікації по локальній мережі – зайва збитковість, EAP – повідомлення упаковуються в „EAP over LAN” (EAPOL) пакети, які і використовуються для обміну інформацією між клієнтом і аутентифікатором (точкою доступу).

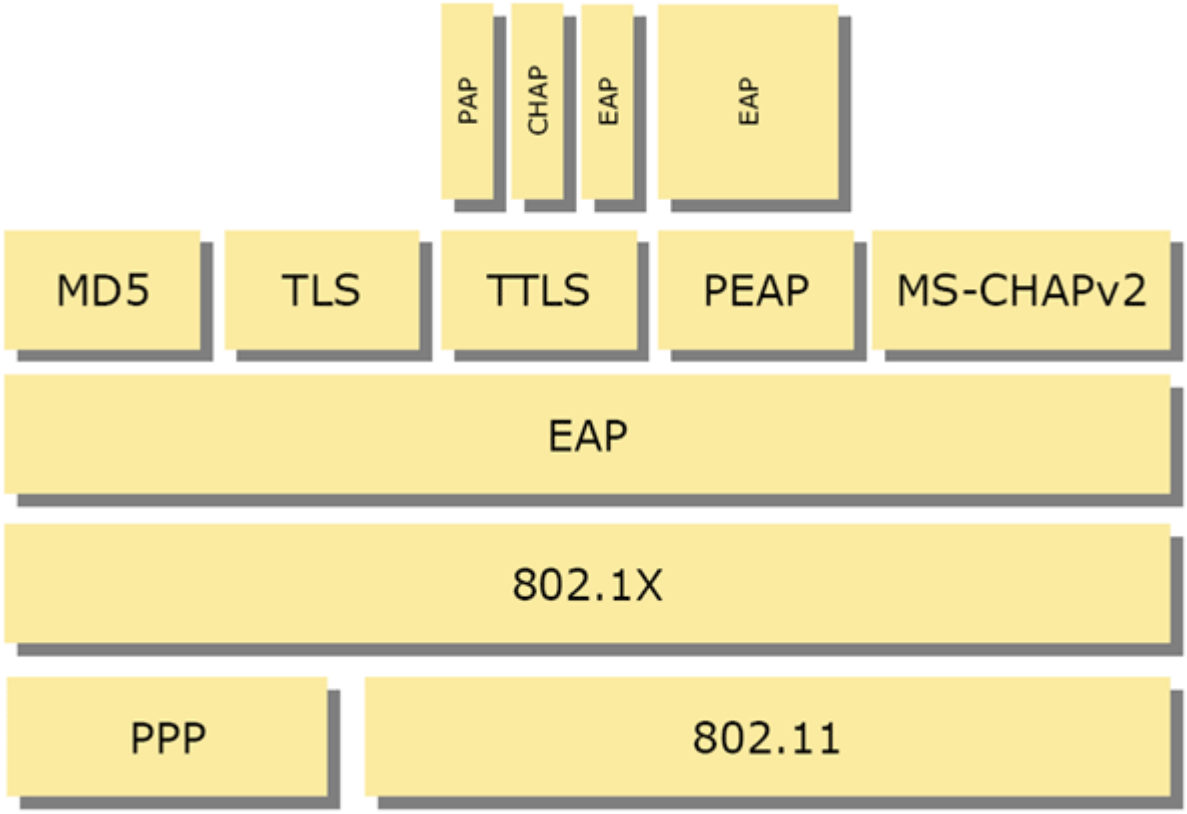

Рисунок 2.5 Структура EAP кадра

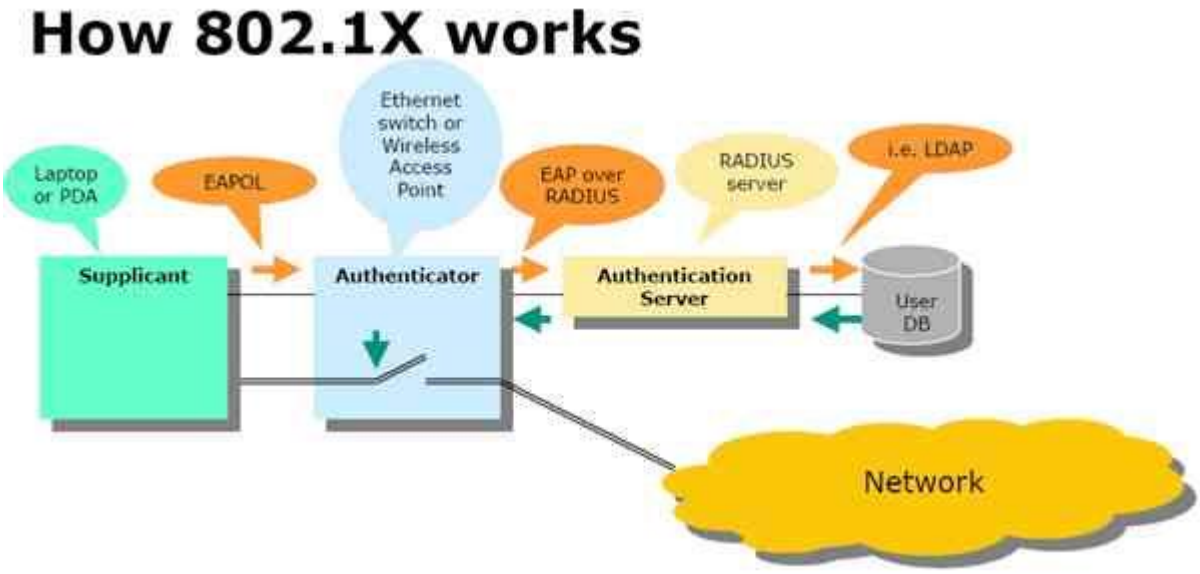

Рисунок 2.6 802.1 в дії

2.6 Варіант застосування аутентифікації в безпроводових комп'ютерних мережах

Схема аутентифікації складається з трьох компонентів:

Supplicant – софт, запущений на клієнтській машині, який намагається підключитись до мережі;

Autentificator – вузол доступу, аутентифікатор (безпроводова точка доступу чи провідний комутатор з підтримкою протоколу 802.1x);

Autentification Server – сервер аутентифікації (звичайно це RADIUS – сервер).

Сам процес аутентифікації складається з наступних стадій:

Клієнт може відправити запит на аутентифікацію (EAP-start message) в напрямку точки доступу.

Точка доступу (аутентифікатор) у відповідь посилає клієнту запит на ідентифікацію клієнта (EAP-request/identity message). Аутентифікатор може відіслати EAP-request самостійно, якщо побачить, що який-небудь з його портів перейшов в активний стан.

Клієнт у відповідь посилає EAP-response packet з необхідними даними, які точка доступу (аутентифікатор) перенаправляє в бік RADIUS – сервера (сервера аутентифікації).

Сервер аутентифікації посилає аутентифікатору challenge-пакет (запит інформації про справжність клієнта). Аутентифікатор пересилає його клієнту.

Далі здійснюється процес взаємної ідентифікації сервера і клієнта. Кількість стадій пересилки пакетів туди-сюди варіює в залежності від метода EAP, але для бездротових мереж підходить лише "strong" аутентифікація зі взаємною аутентифікацією клієнта і сервера (EAP-TLS, EAP-TTLS, EAP-PEAP) і попереднім шифруванням каналу зв"язку.

На наступній стадії, сервер аутентифікації, отримавши від клієнта необхідну інформацію, дозволяє (accept) чи забороняє (reject) тому доступ, з

пересилкою даного повідомлення аутентифікатору. Аутентифікатор відкриває порт для Supplicant-a, якщо зі сторони RADIUS – сервера прийшла позитивна відповідь (accept).

Порт відкривається, аутентифікатор пересилає клієнту повідомлення про успішне завершення процесу і клієнт отримує доступ в мережу.

Після відключення клієнта, порт на точці доступу знову переходить у стан „закрито”.

Описаний процес проілюстровано на рисунку 2.7 (один з найпростіших методів EAP):

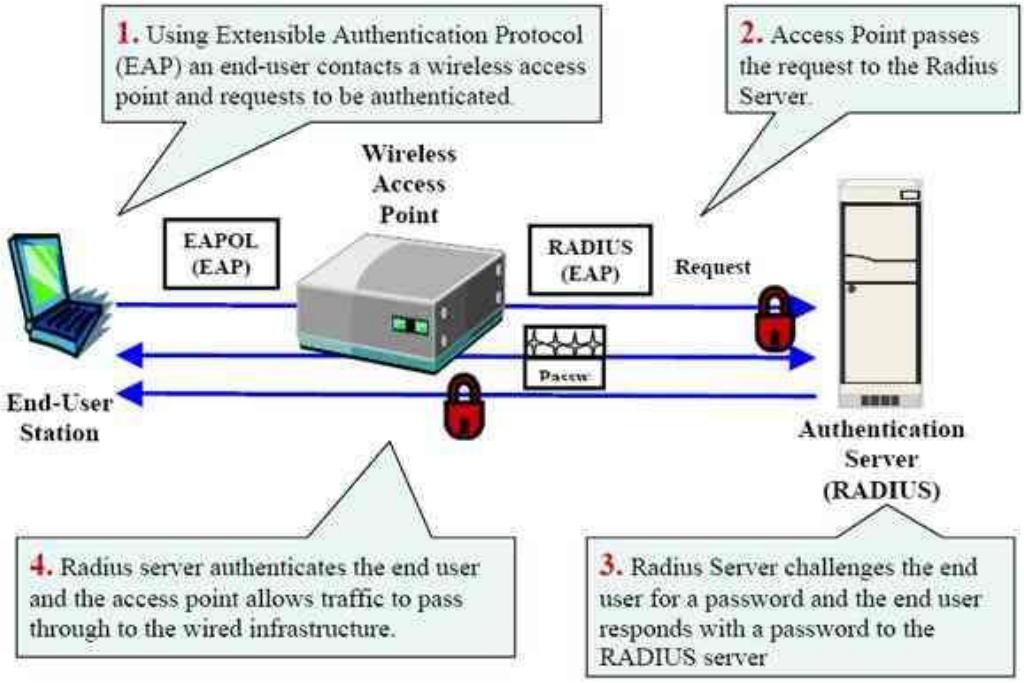

Рисунок 2.7 Процес аутентифікації

Як видно з рисунка, для комунікації між клієнтом (supplicant) і точкою доступу (autentificator) використовуються пакети EAPOL. Протокол RADIUS використовується для обміну інформацією між точкою доступу і RADIUS-сервером. При транзитній пересилці інформації між клієнтом і сервером аутентифікації пакети EAP переупаковуються з одного формата в інший на аутентифікаторі.

Першочергова аутентифікація здійснюється на основі загальних даних, про які знають і клієнт, і сервер аутентифікації (логін-пароль, сертифікат тощо) – на цьому етапі генерується Master Key. Використовуючи Master Key, сервер аутентифікації і клієнт генерують парний майстер-ключ (Pairwise Master Key), який передається аутентифікатору зі сторони сервера аутентифікації. А вже на основі Pairwise Master Key і генеруються всі інші динамічні ключі, яким і закривається передаваємий трафік. Необхідно відмітити, що сам Pairwise Master Key теж динамічно змінюється.

2.7 Цифрові сертифікати, Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) – інфраструктура відкритих ключів. PKI забезпечує створення цифрових сертифікатів (по заздалегідь заданим правилам), управління ними, видача їх суб’єктам і відклик (анулювання). Крім того, PKI забезпечує можливість перевірки валідності сертифікатів. Інфраструктура базується на криптографії з відкритим ключем. А вона, в свою чергу, дає можливість, маючи на руках пари ключів (відкритий і особистий), шифрувати інформацію одним з цих ключів так, щоб розшифрувати її можна було тільки іншим ключем.

Наприклад, зашифрувавши інформацію особистим ключем (який є тільки у власника і нікому не передається), її можна розшифрувати відкритим, загальнодоступним ключем (це називається асиметричним шифруванням). Тим самим засвідчується, що інформація прийшла саме до власника закритого ключа і ні від кого іншого. І навпаки, можна зашифрувати інформацію відкритим ключем власника і відіслати її отримувачу. Навіть якщо хтось по дорозі перехопить повідомлення, він не зможе його прочитати, так як не володіє особистим ключем отримувача.

Для посвідчення особи власника відкритого ключа використовують цифрові сертифікати, що тягнуть за собою всю інфраструктуру PKI.

Сертифікати складають певну інформацію, що дозволяє однозначно засвідчити особу власника (точніше, підтвердження особи власника приходить від третьої сторони).

Кожен суб’єкт PKI (будь-то звичайний користувач, веб-сервер, інший сервер чи мережений пристрій) має особистий сертифікат (чи кілька), в якому міститься інформація, по якій його можна однозначно ідентифікувати і відкритий ключ власника.

Над всім цим стоїть сертифікаційний центр, Certificate Autority (CA), який підписує сертифікати суб’єктів, а також підтверджує валідність виданих сертифікатів тобто посвідчення особи власника. CA довіряють усі суб’єкти PKI, тому кореневий сертифікат (сертифікат CA) має бути у списку довіри всіх суб’єктів PKI.

Проаналізувавши, я можу зробити висновок, що при підключенні до бездротової мережі можна аутентифікувати не тільки користувача, який підключається, але й сам клієнт,який підключається може зі своєї сторони аутентифікувати сервер, до якого він підключається. Достатньо вказати клієнтському софту перевіряти сертифікат сервера (тобто сертифікат, який видається RADIUS-сервером в початковій стадії при підключенні клієнта). Таким чином, можна захистити себе від „чужих” точок доступу, що маскуються під „свої”.

3. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

3.1 Інструментальні засоби для розробки програмного забезпечення

Для реалізацій прикладного програмного забезпечення був використаний CodeGear RAD Studio 2010. Він являється повним рішення для швидкої розробки додатків, що включає все необхідне для створення додатків Windows, .NET, додатків баз даних і веб-додатків. Програми Windows розробляються за допомогою визнаних інтегрованих середовищ розробки Delphi 2010 та C++ Builder 2010. Це найшвидший спосіб створення високопродуктивних програм Windows. Delphi і C++ Builder включають візуальні конструктори і сотні компонентів, що дозволяють легко створювати повнофункціональні інтерфейси користувача і універсальні програми баз даних. Delphi Prism ™ у складі RAD Studio забезпечує можливість розробки для платформ. NET і Mono, а також надає підтримку новітніх технологій. NET Framework 3.5, включаючи ASP.NET, WinForms, WPF і LINQ.

Також мій вибір був зупинений на цьому продукті по тій причині, що цей він працює на Windows 7 без збоїв. Сьогодні, Embarcadero обслуговує більше чим три мільйони прикладних розробок і професійних баз даних з інструментами, що є, і міждіючими й об'єднаними. Фірмові торгові марки DatabaseGear ™ і CodeGear ™ й їхні вироби з'єднують розробку і зв'язування бази даних у новому шляху, що дозволяє їм, збільшити продуктивність і якість, краще адаптуватися протягом більш швидкого часу на ринку, і далі вводять нововведення, усуваючи зауваження менеджера, користувача.

Від індивідуальних продавців програмного забезпечення (ISVS) і розроблювачів до DBAS, продукти також використовують професіонали в області розробок баз даних менеджменту і великі команди підприємства, що працюють в одному зв'язуванні. Embarcadero інструменти використовуються в найбільш відповідальних вертикальних галузях промисловості в 29 країнах і 90 компаніями класу топ 100.

Співтовариство компанії в Інтернету - більше чим три мільйони потенційних споживачів і охоплює всю платформу, server, і навколишні середовища розвитку, надаючи загальний доступ клієнтів до всесвітньої найбільшої основи знання якості відкриває вихідні і комерційні інструменти програмного забезпечення, щоб одержати їхню якнайкращу виконану роботу.

Грамотно і технологично розроблений web-site компанії Embarcadero, свідчить про тім, чому клієнти звертаються за інструментами компанії Embarcadero щодня. Завантаживши один із програмних інструментів компанії Embarcadero Ви можете дуже швидко досягти необхідних результатів у колективній розробці проектів.

Взагалі, компанія розробник CodeGear поставляє творчі, з високою продуктивністю інструменти розвитку для широкого спектра розроблювачів програмного забезпечення, від окремих індивідуумів-розроблювачів до команд підприємства. Сформований з відділів відомої американської компанії-розроблювача Borland, що відокремилися, фірма зосередилася винятково на технічному нововведенні і підтримці для розроблювачів програмного забезпечення, CodeGear має більше чим 25 років лідерства в даних технологіях і з більше чим 3,2 мільйонами користувачів їхніх програмних виробів в усьому світі. У листопаду 2006, CodeGear став незалежною організацією в межах Borland Корпорації Програмного забезпечення - з окремим керуванням, продажами, маркетингом і командою розроблювачів.

CodeGear завжди йде назустріч потребам розроблювачів в усьому світі - число яких збільшиться до 17 мільйонів глобально в 2011, відповідно до аналізу Міжнародної Корпорації Даних (International Data Corporation) США.

CodeGear розробив і запатентував перше комерційне середовище розробки додатків (IDE), що розкриває всебічні здібності команди розроблювачів, для ефективного виробництва програмного забезпечення і комерційних проектів. CodeGear привнесене до ринкового продукту перше

чисте Java IDE, також перший IDE для C++, перший J2EE-компілятор IDE, перше середовище розробки IDE для Linux, і також була першою компанією, що забезпечувала підтримку послуг SOAP в IDE, мові, і бібліотеці під час багаторазового виконання популярних мов програмування.

3.2 Алгоритм роботи інформаційного забезпечення системи

В даній дипломній роботі використовується програмне забезпечення написане на мові C++ і база даних виконана в Access. З'єднання виконано за допомогою ADO компонентів, а саме ADOConnection, ADOQuery, ADODataSet. ADOConnection налаштовується один раз і використовується для всіх інших компонентів. ADOQuery використовується для зв'язку з таблицями в базі даних, через цей компонент працюють запити Select, Insert, Update, Delete. Компонент ADODataSet використано для виведення інформації в таблиці на формах програми.

Відкривши програму, першим, що потрібно занести інформацію про відділи і посади, які будуть використовуватися в подальшому. При успішному внесені переходимо на головну форму, де відбувається занесення всіх працівників, які поступають на роботу. Для коректного внесення даних виведеться повідомлення, якщо хоть одне поле буде пустим, це забезпечує цілісність і захищеність даних.

Також, було реалізовано пошук по ключових словах. Це забезпечує правильність перегляду даних і пришвидшує їх пошук. Це зручно, коли даних дуже багато і пошук займає багато часу.

3.3 Реалізація основних принципів забезпечення безпеки

З'єднання з примірником SQL Server

У випадках, коли користувачеві необхідний доступ до примірника SQL Server, адміністратор повинен надати цьому користувачеві коректну інформацію для перевірки автентичності.

Ця інформація залежить від обраного режиму перевірки автентичності. У даному розділі пояснюється, як створювати імена входу для користувачів операційної системи, які будуть підтримувати режим перевірки автентичності Windows, і імена входу SQL для підтримки режиму перевірки автентичності SQL.

Надаємо доступ користувачам і групам Windows

Можна дозволити користувачам операційної системи встановлювати з'єднання з сервером SQL Server за допомогою створення імені входу для користувача або групи Windows. За замовчуванням, доступ до SQL Server надано тільки членам локальної групи адміністраторів Windows та облікового запису служби, яка запускає служби SQL.

Примітка. Існує можливість видалити права на віддалений доступ до SQL Server зі списку прав членів групи адміністраторів.

Доступ до примірника SQL Server можна надати, створивши ім'я входу або шляхом безпосереднього введення команд SQL, або через інтерфейс SQL Server Management Studio. Наступний код надає доступ до примірника SQL Server користувачеві домену Windows ADWORKS \ jlucas:

CREATE LOGIN [ADVWORKS \ jlucas] FROM WINDOWS;

Примітка. Якщо для створення імені входу використовується SQL Server Management Studio, інструмент виконує аналогічну інструкцію T-SQL. Імена входу Windows за замовчуванням

У процесі установки SQL Server 2005 створюються імена входу Windows, перераховані в табл. 3.1.

Таблиця 3.1. Імена входу Windows за умовчанням

Ім’я входу Windows	Опис
BUILTIN\Administrators	Ім'я входу для локальної групи адміністраторів на комп'ютерах з

	встановленим примірником SQL Server. Для запуску SQL Server це ім'я входу не обов'язково.
<Servername>\SQLServer2005 MSFTEUser$<Servername> $MSSQLSERVER	Ім'я входу для групи користувачів Windows SQLServer2005 MSFTEUser $ <Servername> $ MSSQLSERVER. Члени цієї групи мають необхідні привілеї, які призначаються ним як облікового запису входу в систему асоційованого примірника компонента SQL Server FullText Search. Цей обліковий запис необхідна для запуску компонента SQL Server 2005 Full Text Search.
<Servername>\SQLServer 2005MSSQLUser$<Servername> $MSSQLSERVER	Ім'я входу для групи користувачів Windows SQLServer2005 MSSQLUser $ <Servername> $ MSSQLSERVER. Члени цієї групи мають необхідні привілеї, які призначаються ним як облікового запису входу в систему асоційованого примірника компонента SQL Server. Цей обліковий запис необхідна для запуску SQL Server 2005, оскільки є службовою обліковим записом для SQL Server у тих випадках, коли примірник налаштований на використання локальної службової облікового запису як своєї службової облікового запису.
<Servername>\SQLServer2005	Имя входа для группы пользователей

SQLAgentUser$<Servername>$MSSQLSERVER	SQLServer2005SQLAgentUser$<Servername>$MSSQLSERVER. Члены этой группы имеют необходимые привилегии, которые назначаются им как учетной записи входа в систему ассоциированного экземпляра компонента SQL Server Agent. Эта учетная запись необходима для запуска компонента SQL Server 2005 Agent.

При підключенні до SQL Server 2005 з використанням імені входу Windows, SQL Server покладається на перевірку автентичності операційної системи і перевіряє тільки, чи має користувач Windows відповідне ім'я входу, визначене в цьому примірнику сервера SQL Server, або чи належить це ім'я входу групі Windows з відповідним ім'ям входу в цей екземпляр SQL Server. З'єднання, що використовує ім'я входу Windows, називається довірчим з'єднанням.

Попередження. Не виключена ситуація, при якій користувач або група, зіставлені імені входу Windows, будуть видалені з операційної системи без повідомлення SQL Server. SQL Server 2005 не виконує перевірку для такої ситуації, тому слід періодично перевіряти примірник SQL Server, щоб виявити імена входу, що втратили зв'язок з користувачами. Це легко можна виконати за допомогою системної збереженої процедури sp_validatelogins.

3.4 Надаємо доступ іменам входу SQL Server

У режимі перевірки автентичності Windows і SQL Server також можна створювати імена входу SQL Server і керувати ними. При створенні імені входу SQL Server необхідно поставити для цього імені входу пароль.

Користувачі повинні вказувати пароль при з'єднанні з примірником SQL Server. При створенні імені входу SQL Server можна задати для нього ім'я бази даних і мову за замовчуванням. У тому випадку, якщо програма встановлює з'єднання з SQL Server, не вказуючи контекст і мову бази даних, SQL Server використовує властивості цього імені входу для цього з'єднання за замовчуванням.

Примітка. SQL Server 2005 використовує самозаверяющій сертифікат для шифрування пакетів входу, щоб запобігти несанкціонованому доступу до інформації про вхід в систему. Однак після того як процес входу завершений і ім'я входу підтверджено, SQL Server пересилає всі наступні пакети інформації в незашифрованому вигляді. Якщо необхідно забезпечити безпеку і конфіденційність комунікацій, можна використовувати два методи: протокол Secure Sockets Layer (SSL) і протокол Internet Protocol Security (IPSec).

Доступ до примірника SQL Server можна надати, створивши ім'я входу SQL Server або шляхом безпосереднього введення команд SQL, або через інтерфейс SQL Server Management Studio. У наступному прикладі ми створюємо ім'я входу SQL Server "Mary" і призначаємо для користувача Mary базу даних Adventure Works в якості бази даних за замовчуванням.

```
CREATE LOGIN Mary
WITH PASSWORD = '34TY $ $ 543 ',
DEFAULT_DATABASE = AdventureWorks;
```

У процесі установки SQL Server 2005 створюється одне ім'я входу SQL Server - sa. Ім'я входу sa створюється в будь-якому випадку, навіть якщо ви вибрали в процесі установки режим перевірки автентичності Windows.

3.5 Примусово застосовуємо політику паролів

При використанні імен входу SQL Server необхідно реалізувати сильні політики паролів для цих імен входу щоб уникнути ослаблення системи безпеки SQL Server з плином часу. SQL Server 2005 надає можливість

примусового застосування парольного політики операційної системи до імен входу SQL Server. Якщо SQL Server виконується у середовищі Windows 2003 Server, то SQL Server використовує API (інтерфейс для прикладного програмування) NetValidatePasswordPolicy для управління такими параметрами:

• Складність пароля

• Закінчення строку дії пароля

• Блокування облікового запису

Якщо сервер SQL Server виконується у середовищі Windows 2000 Server, то він використовує правило SQL Server Native Password Complexity rule, яке було введено програмою Microsoft Baseline Security Analyzer для примусового застосування наступних правил:

• Пароль не може бути порожнім або NULL

• Пароль не може співпадати з ім'ям входу

• Пароль не може співпадати з ім'ям комп'ютера

• В якості пароля не можна вибирати слова "Password", "Admin" або "Administrator".

Парольний політику можна включити за допомогою наступного коду Transact SQL:

```
CREATE LOGIN Mary
WITH PASSWORD = '34TY$$543'
 MUSTCHANGE,
 CHECK EXPIRATION = ON,
 CHECK POLICY = ON;
```

Керуємо дозволами для примірника

Тепер ви знаєте, як надати доступ користувачеві до примірника SQL Server, але до цих пір нічого не було сказано про те, які дозволи можуть мати ці імена входу в SQL Server. Як правило, користувачеві необхідний доступ до

яких-небудь даних. Проте можливо вам доведеться створити деякі імена входу з дозволами на виконання завдань адміністрування.

Для виконання цього завдання SQL Server надає серверні ролі на рівні екземпляра. (Серверні ролі є фіксованими, не можна створити нові ролі на рівні екземпляри). У табл. 3.2 перераховані фіксовані серверні ролі, створені SQL Server 2005.

Таблиця 3.2. Фіксовані серверні ролі

Фіксована серверна роль	Опис
bulkadmin	Може виконувати пропозицію BULK INSERT
dbcreator	Може створювати, змінювати, видаляти і відновлювати бази даних
diskadmin	Може управляти файлами на диску
processadmin	Може завершувати процеси
securityadmin	Може управляти іменами входу і призначати дозволу
serveradmin	Може змінювати параметри сервера і завершувати роботу сервера
setupadmin	Може управляти пов'язаними серверами і виконувати системні процедури, що зберігаються
sysadmin	Може виконувати на сервері будь-які дії

3.6 Забороняємо доступ користувачам

У деяких ситуаціях, наприклад, коли користувач звільняється з організації, необхідно заборонити доступ певного імені входу. Якщо ця заборона тимчасовий, можна не видаляти ім'я входу з примірника, а просто

відключити його. При відключенні доступу властивості імені входу і його зіставлення користувачам бази даних зберігаються. Повторно включивши це ім'я входу, ви можете працювати з колишніми властивостями. Щоб відключити і включити ім'я входу, виконайте наступну інструкцію ALTER:

• Відключаємо ім'я входу

ALTER LOGIN Mary DISABLE;

• Включаємо ім'я входу

ALTER LOGIN Mary ENABLE;

Можна перевірити, відключені чи імена входу, виконавши запит до подання каталогу sql_logins, як показано в наступному прикладі:

• Відключаємо ім'я входу

ALTER LOGIN Mary DISABLE; GO

• Виконуємо запит до системного поданням каталогу

SELECT * FROM sys.sql_logins

WHERE is_disabled = 1; GO

• Включаємо ім'я входу

ALTER LOGIN Mary ENABLE;

Рада. У SQL Server Management Studio відключені імена входу позначаються червоною стрілкою. Ця стрілка відображається в правому нижньому кутку значка імені входу, який знаходиться в папці Security / Logins (Безпека / Імена входу) в панелі Object Explorer (Оглядача об'єктів). З іншого боку, якщо необхідно видалити ім'я входу з даного екземпляра, слід використовувати посібник DROP LOGIN. Наступний приклад видаляє ім'я входу.

DROP LOGIN Mary;

Попередження. При видаленні імені входу SQL Server 2005 не видаляє користувачів бази даних, зіставлених цьому імені входу.

Попередження. Видалення імені входу, якому зіставлені користувачі або групи Windows не гарантує, що ці користувачі або члени груп не зможуть

отримати доступ до SQL Server. Врахуйте, що такі користувачі можуть належати і до будь-якої іншої групи Windows з чинним ім'ям входу.

Управління доступом до схем

У SQL Server 2005 реалізована концепція ANSI для схем. Схеми - це контейнери об'єктів, які дозволяють групувати об'єкти бази даних. Схеми дуже впливають на те, як користувачі посилаються на об'єкти бази даних. У SQL Server 2005 об'єкт бази даних називається ім'ям, що складається з чотирьох компонентів наступної структури:

<Server>. <Database>. <Schema>. <Object>.

3.7 Управління доступом до таблиць і стовпців

Таблиця і стовпці зберігають дані, які витягують і створюють додатки. Управління доступом до цих даних здійснюється через ієрархію дозволів SQL Server 2005. Керувати цією ієрархією дозволів можна за допомогою інструкцій GRANT, DENY і REVOKE.

GRANT. Дозволяє ролі або користувачеві виконувати операції, визначені у момент надання дозволу.

DENY. Забороняє користувачеві або ролі певні дозволи і запобігає успадкування цих дозволів від інших ролей ..

REVOKE. Відкликає раніше заборонені або надані дозволу.

Зміна прав доступу до таблиці

Доступ до таблиці управляється діючими дозволами, які надані користувачеві на цю таблицю. Доступом користувача до таблиць можна керувати за допомогою управління дозволами на таблицю. Дозволи, якими можна управляти для таблиць, перераховані в табл. 3.3. Ці дозволи можна призначати користувачам бази даних і ролям.

Таблиця 3.3. Дозволи на доступ до таблиці	
Дозволи	Опис
ALTER	Дозволяє змінювати властивості таблиці
CONTROL	Надає дозволи, аналогічні володінню
DELETE	Дозволяє видаляти рядки з таблиці
INSERT	Дозволяє додавати стовпці в таблицю
REFERENCES	Дозволяє посилатися на таблицю із зовнішнього ключа
SELECT	Дозволяє здійснювати вибірку рядків з таблиці
TAKE OWNERSHIP	Дозволяє присвоєння схеми чи таблиці
UPDATE	Дозволяє змінювати рядки в таблиці
VIEW DEFINITION	Дозволяє доступ до метаданих таблиці

Надаємо доступ до таблиці

Доступ користувачам бази даних і ролям можна надати за допомогою інструкції GRANT. У наступному прикладі дозволу SELECT, INSERT і UPDATE на таблицю Sales.Customer надаються користувачеві Sara (код для управління доступом до таблиць в цьому і наступних розділах мається на файлах прикладів під ім'ям ManagingAccessToTables.sql.).

• Змінюємо контекст з'єднання на базу даних AdventureWorks.

```
USE AdventureWorks;
GO
```

• Надаємо користувачеві Sara деякі дозволи

• для таблиці Sales.Customer table.

```
GRANT SELECT, INSERT, UPDATE
ON Sales.Customer TO Sara;
```

Надаємо доступ до стовпцях

Доступ до окремих стовпцях можна надати за допомогою інструкції GRANT. У наступному прикладі дозволу SELECT та UPDATE надаються користувачеві Sara на стовпці Demographics і Modified Date таблиці Sales.Individual. (Код для управління доступом до стовпцях таблиці в цьому і наступних розділах мається на файлах прикладів під ім'ям ManagingAccessToColumns. sql.)

• Змінюємо контекст з'єднання на базу даних AdventureWorks.

```
USE AdventureWorks;
GO
```

• Надаємо дозволу SELECT та UPDATE користувачеві Sara на певні стовпці таблиці Sales.Individual

```
GRANT SELECT, UPDATE (
Demographics, ModifiedDate) ON Sales.Individual TO Sara;
```

3.8 Управління доступом до програмованим об'єктам

Такі програмовані об'єкти, як збережені процедури і визначені користувачем функції, мають свій контекст безпеки. Щоб виконувати збережені процедури, функції і збірки, користувачам бази даних необхідні дозволи. Після того, як ядро бази даних виконає перевірку на наявність дозволів на виконання програмованого об'єкта, воно перевіряє наявність дозволів на виконання операцій, в яких використовуються програмовані об'єкти. Коли об'єкти бази даних послідовно звертаються один до одного, ця послідовність формує ланцюжок володіння.

4. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

4.1 Специфіка використання стандарту IEEE 802.11n

Як відомо з першого розділу розрізняють три типи бездротових мереж (рис. 4.1): WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) і WPAN (Wireless Personal Area Network).

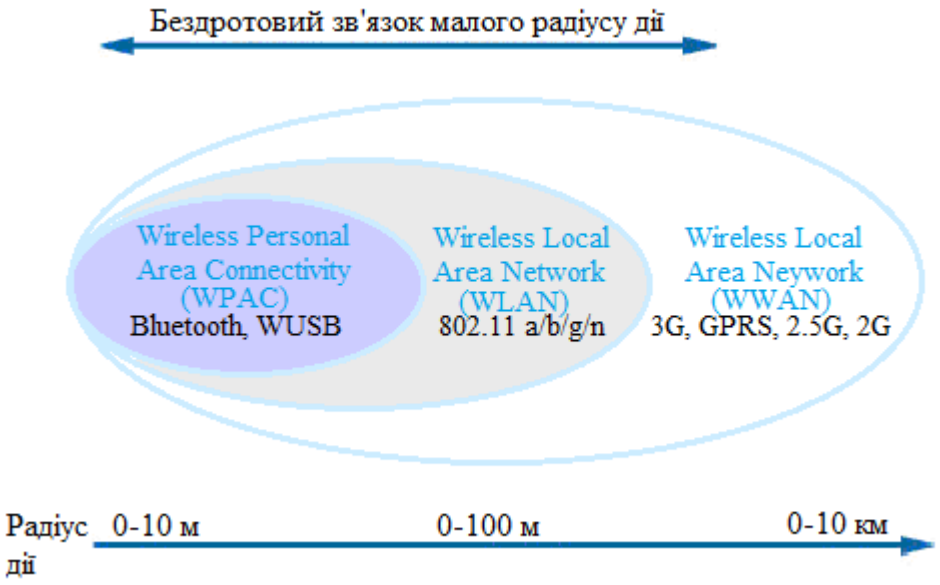

Рисунок 4.1 Радіус дії персональних, локальних та глобальних бездротових мереж

При побудові мереж WLAN і WPAN, а також систем широкосмугового бездротового доступу (BWA - Broadband Wireless Access) застосовуються подібні технології. Ключове розходження між ними (рис. 4.2) - діапазон робочих частот і характеристики радіоінтерфейсу. Мережі WLAN і WPAN працюють в неліцензійних діапазонах частот 2,4 і 5 ГГц, тобто при їх розгортання не потрібно частотного планування і координації з іншими радіомережами, що працюють в тому ж діапазоні. Мережі BWA (Broadband Wireless Access) використовують як ліцензійні, так і неліцензійні діапазони (від 2 до 66 ГГц).

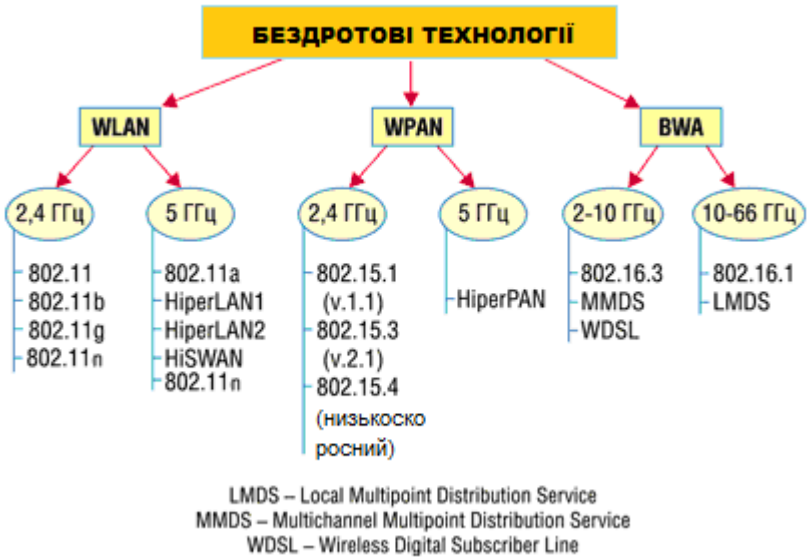

Рисунок 4.2 Класифікація бездротових технологій

Детальніше розглянемо стандарт на базі якого реалізується бездротова мережа.

Стандарт IEEE 802.11n

Цей стандарт був затверджений 11 вересня 2009. 802.11n за швидкістю передачі порівнянна 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 (близько 300 Мбіт / с);

- Рівномірний, стійке, надійне і якісне покриття зони дії станції, відсутність непокритих ділянок;

- Сумісність з попередніми версіями стандарту Wi-Fi.

Недоліки:

- Велика потужність споживання;

- Два робочих діапазону (можлива заміна обладнання);

- Ускладнена і більш габаритна апаратура.

Збільшення швидкості передачі в стандарті IEEE 802.11n досягається, по-перше, завдяки подвоєння ширини каналу з 20 до 40 МГц, а по-друге, за рахунок реалізації технології MIMO. Технологія MIMO (Multiple Input Multiple Output) припускає застосування декількох передаючих і приймаючих антен. За аналогією традиційні системи, тобто системи з однієї передавальної і однієї приймаючої антеною, називаються SISO (Single Input Single Output). Стандарт IEEE 802.11n заснований на технології OFDM-MIMO. Дуже багато реалізовані в ньому технічні деталі запозичені 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. Тобто пристрої, що підтримують стандарт IEEE 802.11n, можуть працювати в частотному діапазоні або 5, або 2,4 ГГц.

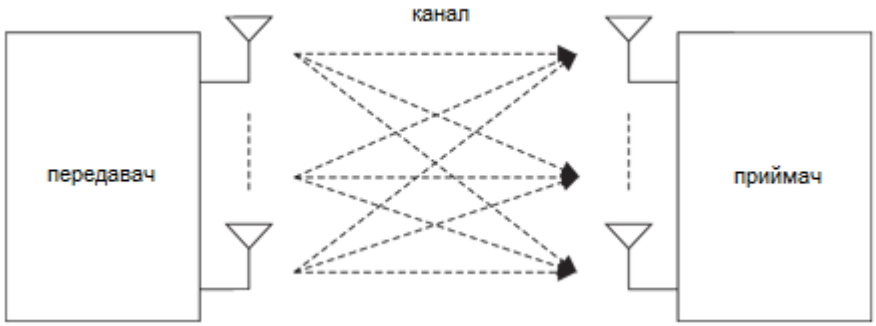

Рисунок 4.3 Принцип реалізації технології MIMO

Передана послідовність ділиться на паралельні потоки, з яких на приймальному кінці відновлюється вихідний сигнал. Тут виникає деяка складність - кожна антена приймає суперпозицію сигналів, які необхідно відокремлювати один від одного. Для цього на приймальному кінці застосовується спеціально розроблений алгоритм просторового виявлення сигналу. Цей алгоритм заснований на виділенні піднесе і виявляється тим складніше, чим більше їх число. Єдиним недоліком використання MIMO є

складність і громіздкість системи і, як наслідок, більш високе споживання енергії. Для забезпечення сумісності MIMO-станцій і традиційних станцій передбачено три режими роботи:

- Успадкований режим (legacy mode).
- Змішаний режим (mixed mode).
- Режим зеленого поля (green field mode).

Кожному режиму роботи відповідає своя структура преамбули - службового поля пакету, яке вказує на початок передачі і служить для синхронізації приймача і передавача. У преамбулі міститься інформація про довжину пакета і його тип, включаючи вид модуляції, обраний спосіб кодування, а також всі параметри кодування. Щоб не допустити конфліктів у роботі станцій MIMO і звичайних (з одного антеною) під час обміну між станціями MIMO пакет супроводжується особливою преамбулою і заголовком. Отримавши таку інформацію, станції, що працюють в успадкованому режимі, відкладають передачу до закінчення сеансу між станціями MIMO. Крім того, структура преамбули визначає деякі первинні завдання приймача, такі як оцінка потужності сигналу, що для системи автоматичного регулювання посилення, виявлення початку пакету, зміщення за часом і частотою.

Режими роботи станцій MIMO. Успадкований режим. Цей режим передбачений для забезпечення обміну між двома станціями з одного антеною. Передача інформації здійснюється по протоколах 802.11a. Якщо передавачем є станція MIMO, а приймачем - звичайна станція, то в передавальної системі використовується тільки одна антена і процес передачі йде так само, як і в попередніх версіях стандарту Wi-Fi. Якщо передача йде у зворотному напрямку - від звичайної станції в многоантенну, то станція MIMO використовує багато прийомних антен, однак у цьому випадку швидкість передачі не максимальна. Структура преамбули в цьому режимі така ж, як у версії 802.11a. Змішаний режим. У цьому режимі обмін

здійснюється як між системами MIMO, так і між звичайними станціями. У зв'язку з цим системи MIMO генерують два типи пакетів, в залежності від типу приймача. Із звичайними станціями робота йде повільно, оскільки вони не підтримують роботу на високих швидкостях, а між MIMO - значно швидше, однак швидкість передачі нижче, ніж в режимі зеленого поля. Преамбула в пакеті від звичайної станції така ж, що і в стандарті 802.11a, а в пакеті MIMO вона трохи змінена. Якщо передавачем виступає система MIMO, то кожна антена передає не цілу преамбулу, а циклічно зміщену. За рахунок цього знижується потужність споживання станції, а канал використовується більш ефективно. Однак не всі успадковані станції можуть працювати в цьому режимі. Справа в тому, що якщо алгоритм синхронізації пристрою заснований на взаємній кореляції, то відбудеться втрата синхронізації. Режим зеленого поля. У цьому режимі повністю використовуються переваги систем MIMO. Передача можлива тільки між многоантенними станціями при наявності успадкованих приймачів. Коли йде передача MIMO-системою, звичайні станції чекають звільнення каналу, щоб уникнути конфліктів. У режимі зеленого поля прийом сигналу від систем, що працюють за першими двома схемами, можливий, а передача їм - ні. Це зроблено для того, щоб виключити з обміну одноантенні станції і тим самим підвищити швидкість роботи. Пакети супроводжуються преамбулами, які підтримуються тільки станціями MIMO. Всі ці заходи дозволяють максимально використовувати можливості систем MIMO-OFDM. У всіх режимах роботи повинна бути передбачений захист від впливу роботи сусідньої станції, щоб запобігти спотворення сигналів. На фізичному рівні моделі OSI для цього використовуються спеціальні поля в структурі преамбули, які сповіщають станцію про те, що йде передача і необхідно певний час очікування. Деякі методи захисту приймаються і на канальному рівні. Залежно від використовуваної смуги пропускання режими роботи класифікуються наступним чином:

1. Наслідуваний режим. Цей режим потрібний для узгодження з попередніми версіями Wi-Fi. Він дуже схожий на 802.11a / g як з обладнання, так і по смузі пропускання, яка складає 20 МГц.

2. Подвійний наслідуваний режим. Пристрої використовують смугу 40 МГц, при цьому одні і ті ж дані посилаються по верхньому і нижньому каналу (кожен шириною 20 МГц), але зі зміщенням фази на 90 °. Структура пакета орієнтована на те, що приймачем є звичайна станція. Дублювання сигналу дозволяє зменшити викривлення, підвищуючи тим самим швидкість передачі. 3. Режим з високою пропускною здатністю. Пристрої підтримують обидві смуги частот - 20 і 40 МГц. У цьому режимі станції обмінюються тільки пакетами MIMO. Швидкість роботи мережі максимальна.

4. Режим верхнього каналу. У цьому режимі використовується тільки верхня половина діапазону 40 МГц. Станції можуть обмінюватися будь-якими пакетами.

5. Режим нижнього каналу. У цьому режимі використовується тільки нижня половина діапазону 40 МГц. Станції також можуть обмінюватися будь-якими пакетами.

Методи підвищення швидкодії. Швидкість передачі даних залежить від багатьох факторів (таблиця 1.3) і, перш за все, від смуги пропускання. Чим вона ширше, тим вище швидкість обміну. Другий фактор - кількість паралельних потоків. У стандарті 802.11n максимальне число каналів дорівнює 4. Також велике значення мають тип модуляції і метод кодування. Перешкодостійкі коди, які звичайно застосовуються у мережах, припускають внесення деякої надмірності. Якщо захисних бітів буде занадто багато, то швидкість передачі корисної інформації знизиться. У стандарті 802.11n максимальна відносна швидкість кодування становить до 5 / 6, тобто на 5 бітів даних припадає один надлишковий. У таблиці 3 наведено швидкості обміну при квадратурної модуляції QAM і BPSK. Видно, що за інших однакових параметрах модуляція QAM забезпечує набагато більшу швидкість роботи.

У стандарті IEEE 802.11n допускається використання до чотирьох антен у точки доступу і бездротового адаптера. Обов'язковий режим передбачає підтримку двох антен у точки доступу і однієї антени і бездротового адаптера. У стандарті IEEE 802.11n передбачено як стандартні канали зв'язку шириною 20 МГц, так і канали з подвоєною шириною. Загальна структурна схема передавача зображена на рис. 4.4 Передані дані проходять через скремблер, який вставляє в код додаткові нулі або одиниці (так зване маскування псевдовипадковим шумом), щоб уникнути довгих послідовностей однакових символів. Потім дані розділяються на N потоків і надходять на кодер з прямою корекцією помилок (FEC). Для систем з однією або двома антенами N = 1, а якщо використовуються три або чотири передавальних каналу, то N = 2.

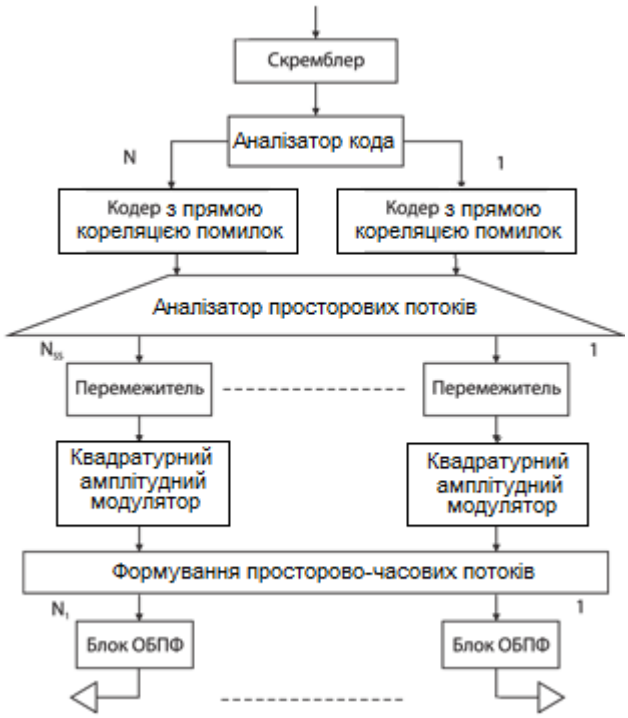

Рисунок 4.4 Загальна структура передавача MIMO-OFDM

Кодована послідовність поділяється на окремі просторові потоки. Біти в кожному потоці перемежовуються (для усунення блокових помилок), а потім модулюються. Далі відбувається формування просторово-часових потоків, які проходять через блок зворотного швидкого перетворення Фур'є і надходять на

антени. Кількість просторово-часових потоків дорівнює кількості антен. Структура приймача аналогічна структурі передавача зображена на рис. 4.5, але всі дії виконуються в зворотному порядку.

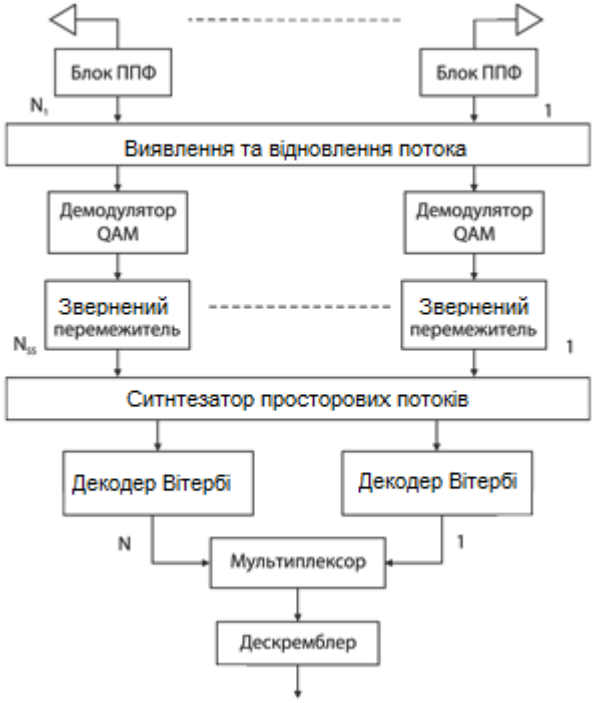

Рисунок 4.5 Загальна структура приймача

Фактори більш високої швидкості передачі даних стандарту 802.11n

Стандарт 802.11n застосовує три основних механізмі для збільшення швидкості передачі даних:

- Застосування декількох приймачів і спеціальних алгоритмів передачі і прийому радіосигналу, відомий за абревіатурою MIMO;

- Збільшення смуги частот сигналу з 20 до 40 МГц;

- оптимізація протоколу рівня доступу до мережі.

Розглянемо кожний з цих механізмів трохи докладніше.

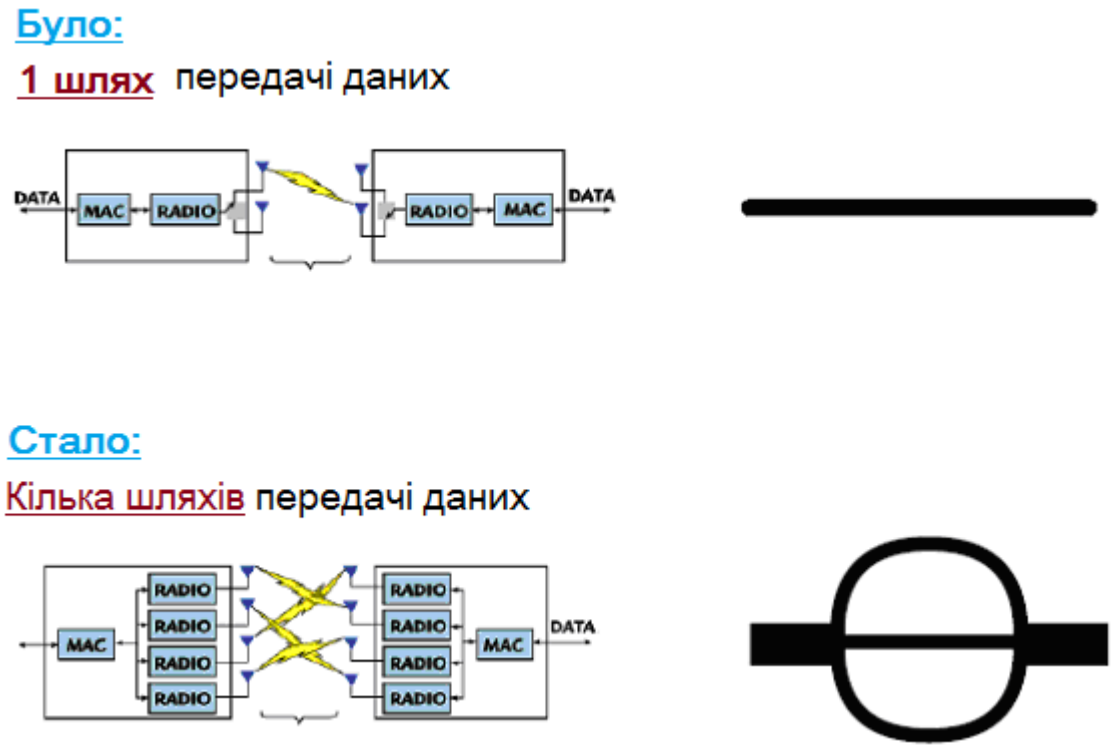

Рисунок 4.7 Перший фактор збільшення швидкості передачі даних

Перший чинник. Із застосуванням MIMO з'являється можливість одночасно передавати кілька потоків даних в одному і тому ж каналі, а потім за допомогою складних алгоритмів обробки відновлювати їх на прийомі. Проводячи аналогію з автодорогами, можна сказати, що раніше існував лише 1 шлях, що з'єднує точки А і Б. Тепер таких шляхів декілька і загальна пропускна здатність системи збільшилася.

Другий фактор - збільшення доступною ширини смуги частот. Теоретично досяжна пропускна здатність каналу зв'язку безпосередньо залежить від ширини займаної ним смуги частот. У новому стандарті з'явилася можливість об'єднувати сусідні канали по 20 МГц і таким чином збільшувати пропускну здатність практично в 2 рази. За аналогією з автомагістралями можна вважати, що вдвічі збільшується кількість доступних для руху смуг.

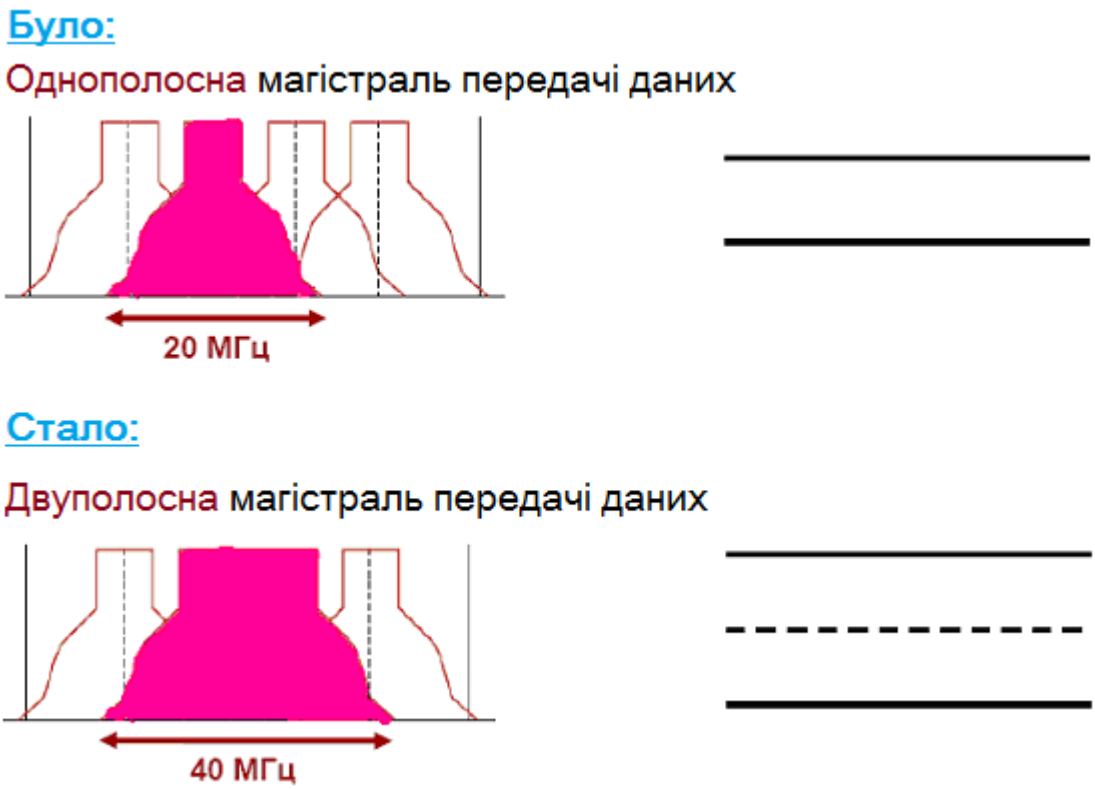

Рисунок 4.6 Другий фактор збільшення швидкості передачі даних

Рисунок 4.7 Третій фактор підвищення швидкості передачі даних

Перші два чинники ставилися до фізичного каналу. Третій важливий фактор збільшення продуктивності - оптимізація протоколу передачі даних на рівні доступу до середовища. У попередніх версіях прийом кожного переданого кадру (порції даних) мав підтверджуватися приймальні стороною. У новій версії введена можливість блокового підтвердження. Приймач інформації повідомляє одне підтвердження відразу на кілька успішно прийнятих кадрів, що зменшує завантаження загальної пропускної здатності каналу службовими повідомленнями. Крім того, зменшено часовий проміжок між кадрами, що також дозволило підвищити корисну пропускну здатність. Проводячи аналогії з повсякденним життям, можна порівняти кадри з контейнерами для перевезень вантажів. Нові правила 802.11 n дозволили зменшити дистанцію між контейнерами і дозволили диспетчеру підтверджувати не кожен вантаж окремо, а відразу партію вантажів.

4.2 Налаштування клієнта бездротового зв'язку

Для відкриття діалогового вікна для налаштування в операційній системі Windows 7 проходимо «Пуск»- « Панель управління » (рис. 4.8).

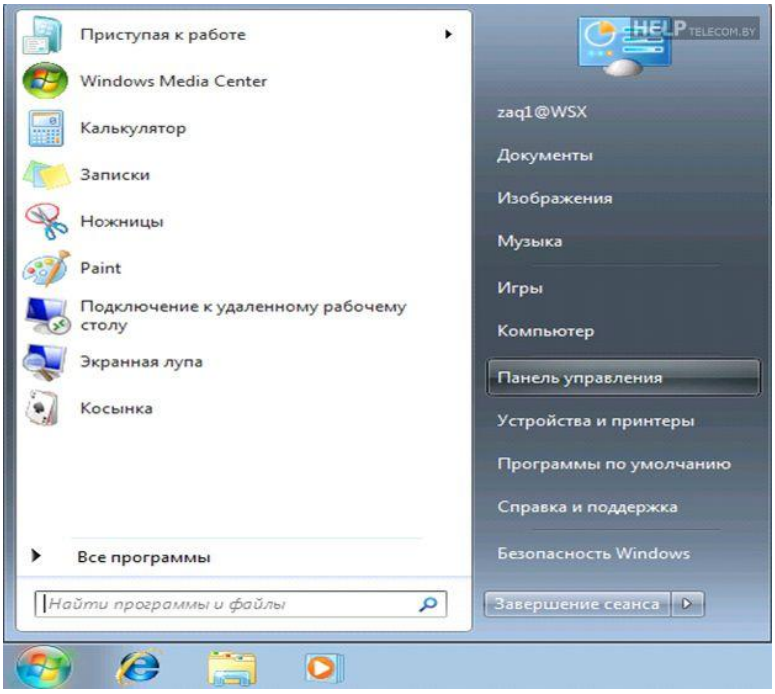

Рисунок 4.8 Панель управління

Вибираємо «Мережа і інтернет»(рис. 4.9).

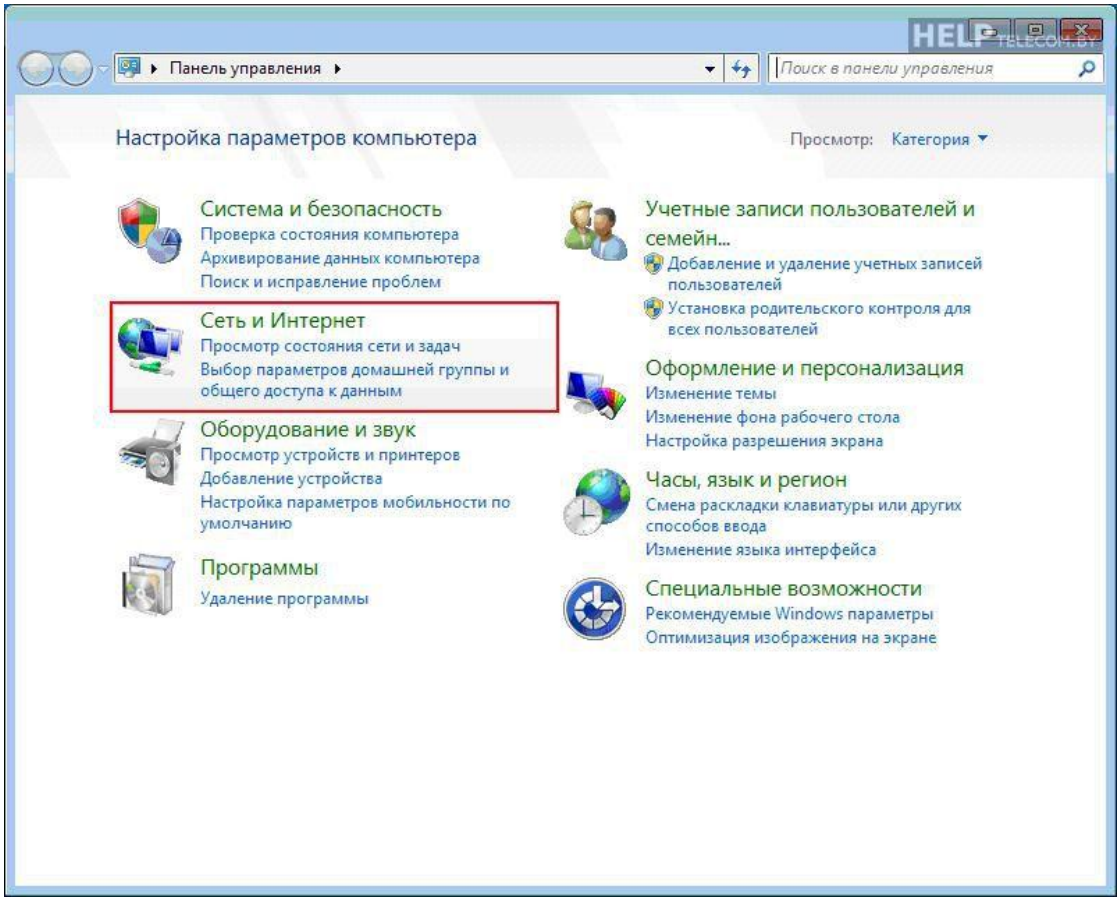

Рисунок 4.9 Налаштування параметрів мережі

Далі переходимо в «Центр управління мережами та загальним доступом»(рис. 4.10).

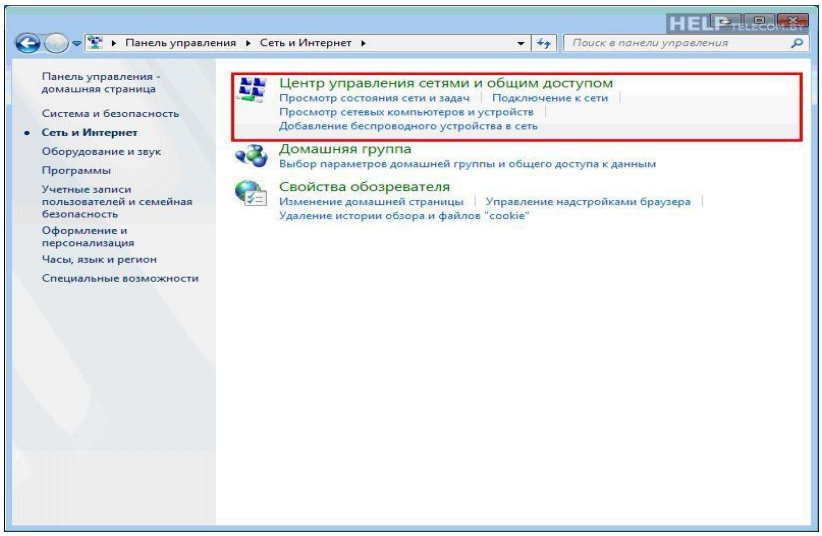

Рисунок 4.10 Управління мережевим та загальним доступом

У вікні «Центр управління мережами та загальним доступом» зліва вибираємо «Зміна параметрів адаптерів» (рис. 4.11).

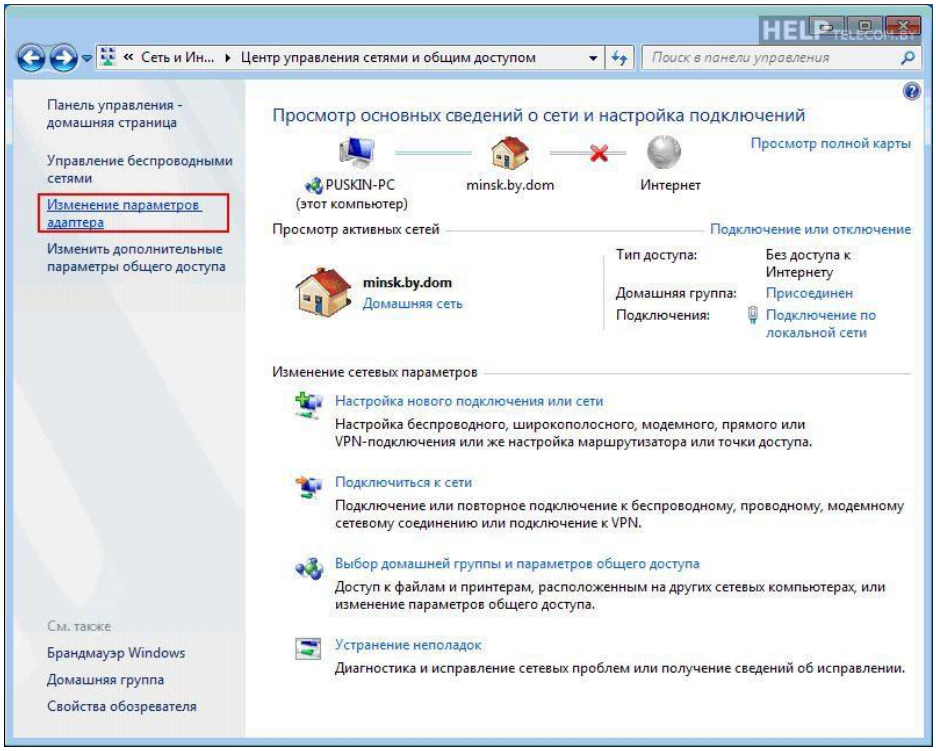

Рисунок 4.11 Налаштування підключення

У відкритому вікні клацнути на ярлику «Бездротове мережне з’єднання» правою кнопкою миші і вибрати пункт «Підключення/Відключення» (рис. 4.12).

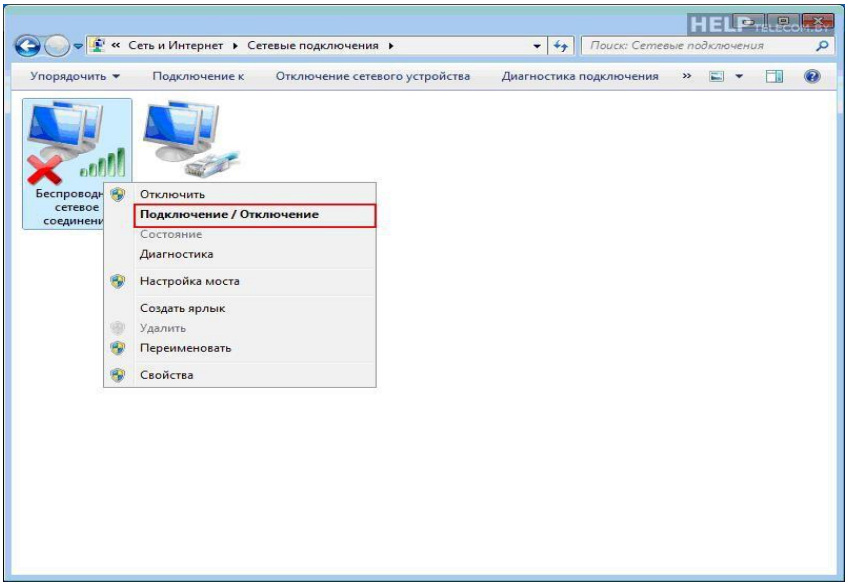

Рисунок 4.12 Підключення бездротового мережевого з’єднання

У переліку знайдених бездротових мереж знаходимо і виділяємо нашу мережу. Потім натискаємо кнопку «Підключення» (рис. 4.13).

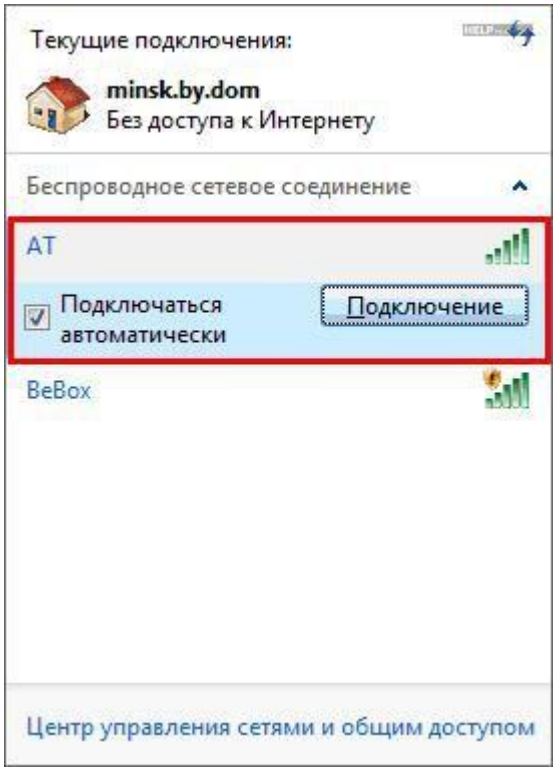

Рисунок 4.13 Поточне підключення

У наступному вікні вводимо ключ доступу до бездротової мережі, який був придуманий і введений при налаштуванні wi-fi точки доступу. Вводимо пароль і натискаємо кнопку «Ok» (рис 4.14)

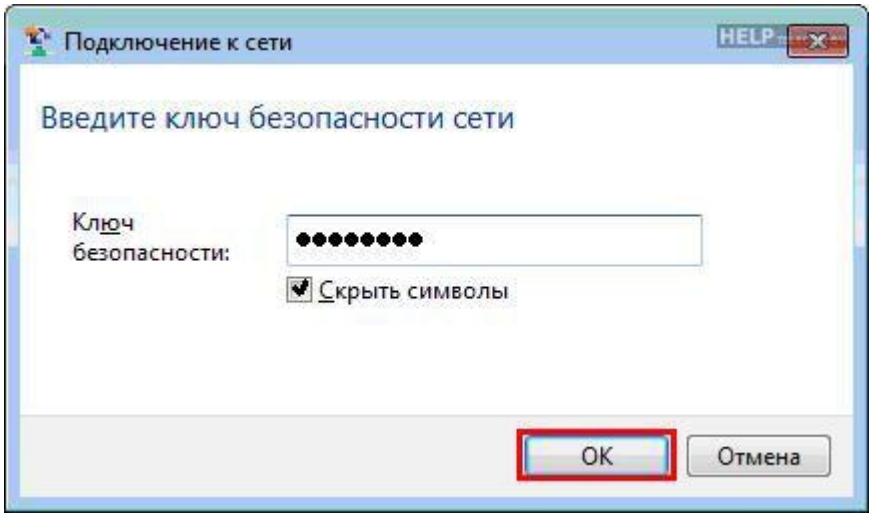

Рисунок 4.14 Введення ключа безпеки мережі

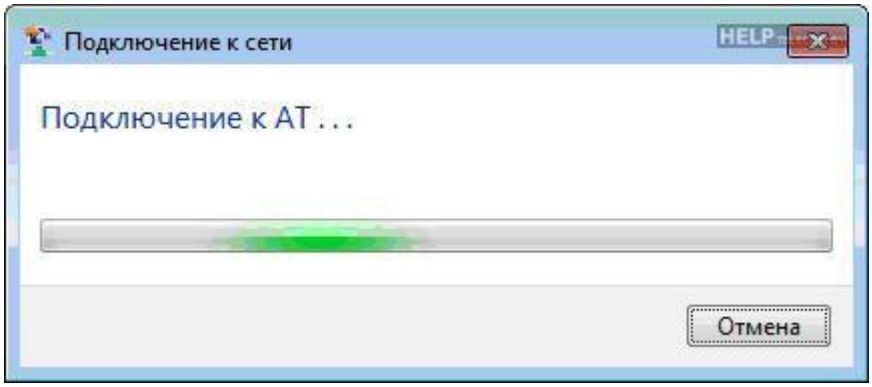

Рисунок 4.15 Перевіряємо підключення

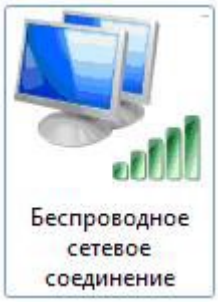

Рисунок 4.16 Бездротове мережеве з’єднання

5. ТЕСТОВИЙ ПРИКЛАД ПРОГРАМИ

5.1 Забезпечення захисту унікального ідентифікатора

Точки доступу, що поставляються, мають стандартні мережеві імена, наприклад, "tsunami", "default", "linksys" і т.д., інформація про які передається в широкомовному режимі клієнтам мережі, щоб прорекламувати доступність точки доступу. Цю настройку необхідно змінити відразу ж після завершення установки точки доступу. При перейменуванні ідентифікатора SSID точок доступу потрібно вибирати що-небудь, не пов'язане безпосередньо з діяльністю того чи іншого підприємства компанією. Не слід вибирати як SSID назву компанії, номер її телефону або іншу інформацію про підприємство, яку можна легко обчислити або знайти в Інтернет. За замовчуванням точки доступу передають дані про SSID в широкомовному режимі всім бездротовим клієнтам, що працюють в заданому діапазоні частот. В деяких випадках, наприклад для хот-спотів або гостьового доступу, ця можливість дозволяє користувачам знайти мережу без чиєї-небудь допомоги. Проте для корпоративних мереж широкомовну передачу SSID необхідно відключити, щоб обмежити число випадкових користувачів, що шукають можливість підключитися до відкритої бездротової мережі. Рішення Cisco Unified Wireless Network дозволяє гарантувати можливість підключення будь-яких клієнтів до мережі тільки в межах встановленого оператором числа спроб. Якщо клієнту не вдається дістати доступ до мережі в межах заданого числа спроб, він автоматично блокується до тих пір, поки не закінчиться час встановленого оператором таймера. Операційна система дозволяє заборонити широкомовну передачу SSID для кожної окремої

мережі WLAN. Це дає можливість ще більше скоротити число випадкових "підслуховуючих" користувачів.

5.2 Налаштування точок доступу

При проектуванні бездротової мережі я залишила свій вибір на обладнані компанії D-Link.

Точка доступу DAP-1360 підтримує стандарт бездротового зв'язку 802.11n з технологією MIMO, яка помітно покращує швидкість передачі даних в бездротовій мережі і підвищує якість радіопокриття.

Розглянемо налаштування однієї з точок доступу.

Щоб увійти в меню установки точки доступу D-link DAP-1360 потрібно змінити TCP / IP параметри мережевої карти наступним чином:

- IP: 192.168.0.51
- Маска підмережі: 255.255.255.0
- Шлюз: 192.168.0.50

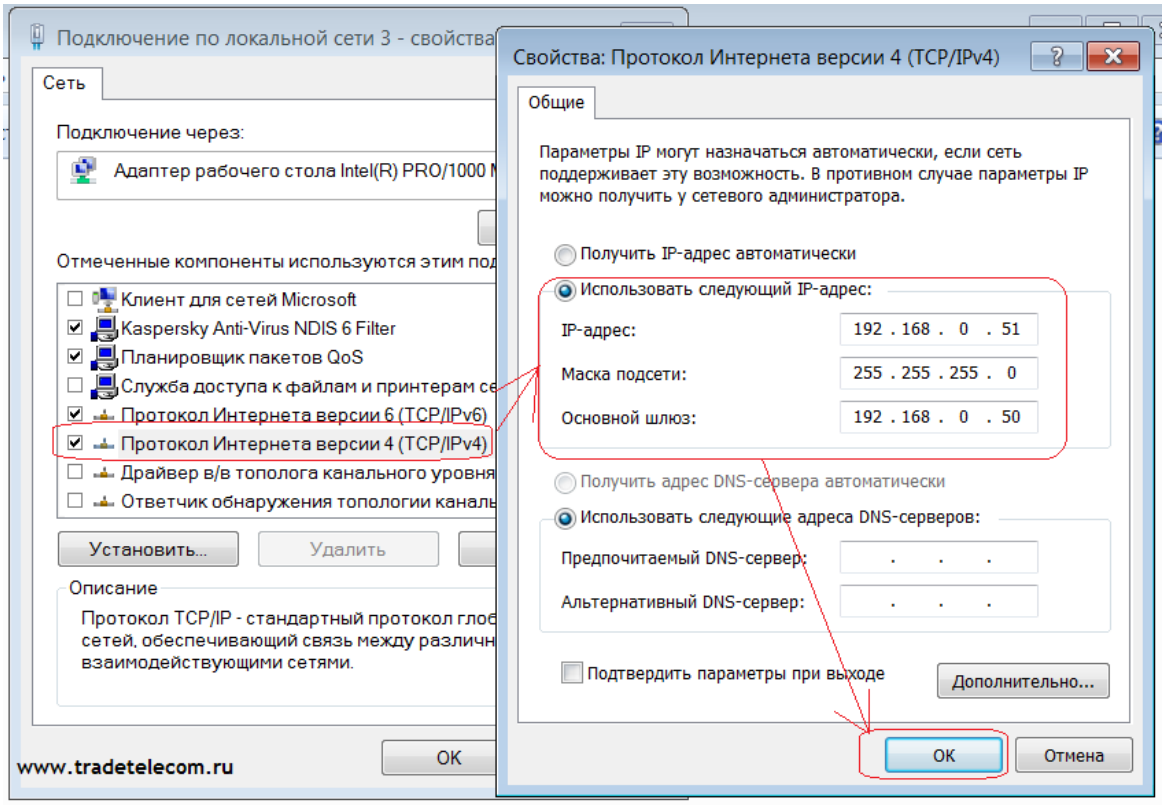

Рисунок 5.1 Зміна параметрів TCP / IP

Налаштування точки доступу D-Link DAP-1360 здійснюється через ВЕБ інтерфейс. Отже, після підключення точки доступу до свого комп'ютера запускаємо браузер (internet explorer, Mozilla, opera, chrome) і здійснюємо в ньому перехід за адресою http://192.168.0.50

Після цього вай-фай точка доступу D-link DAP-1360 видасть запрошення ввести логін та пароль для входу в інтерфейс адміністратора. За замовчуванням логін і пароль для входу в вайфай точку доступу DAP-1360: логін - admin, пароль - порожнє поле (рис. 5.2):

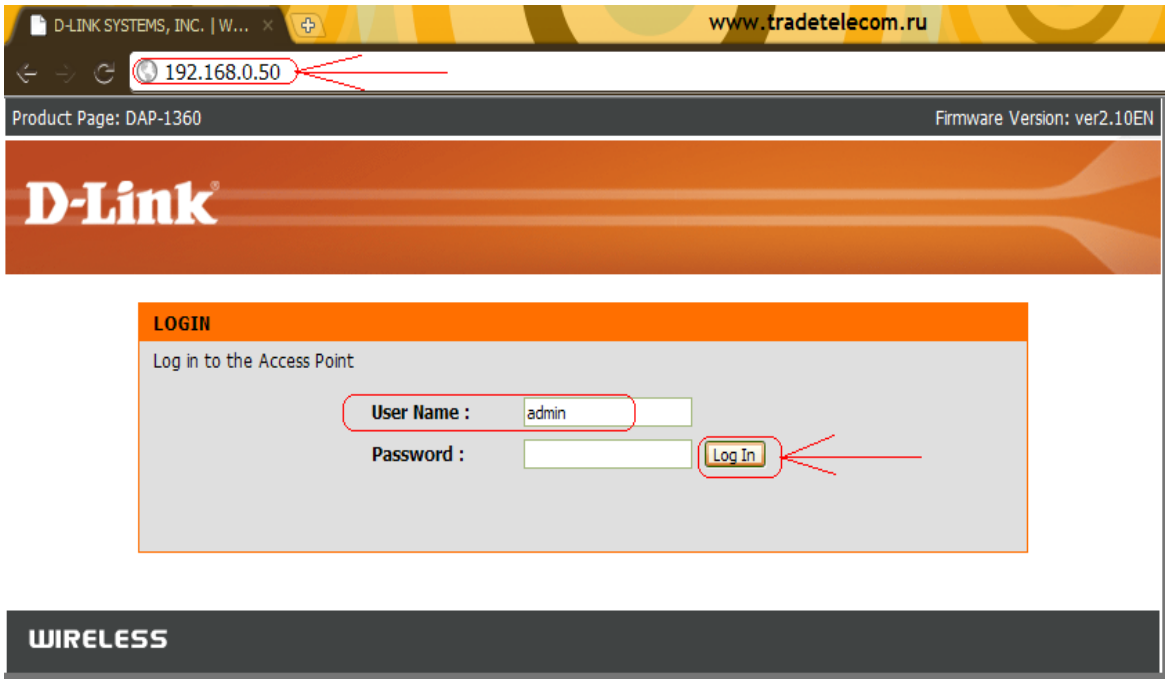

Рисунок 5.2 Задаємо логін і пароль

У відкритому вікні в лівому верхньому меню вибираємо п. Wireless Setup (рис. 5.3)

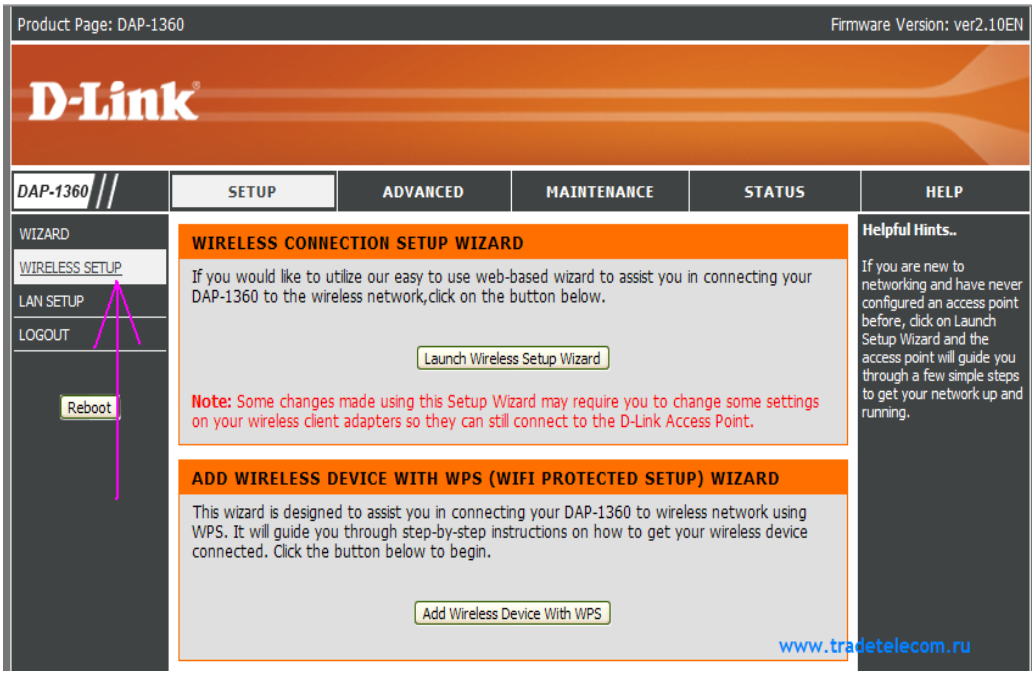

Рисунок 5.3 п. Wireless Setup

Потім налаштовуємо параметри бездротової мережі (рис. 5.4).

Рисунок 5.4 Вікно налаштування точки доступу

П. Enable Wireless – залишаємо галочку для активізації точки доступу, розклад залишаємо не змінним.

У п. Wireless Mode задаємо режим роботи нашої точки доступу. У рамках даного керівництва ми розглянемо налаштування DAP-1360 саме в якості точки доступу - Access Point, тому залишаємо даний варіант.

У п. Wireless Network Name вказуємо назву нашої бездротової мережі (SSID).

П. Enable Auto Channel Scan активує автоматичне призначення каналу бездротового зв'язку. Тому для ручної настройки знімаємо галочку.

П. Wireless channel задаємо номер каналу безпровідного Wi-Fi зв'язку. Для уникнення інтерференції вибираємо 1 або 11.

П. 802.11mode вибраємо - з якими протоколами вай-фай буде сумісна точка доступу D-Link DAP-1360. Залишаємо варіант Mixed 802.11g and 802.11n - він забезпечить сумісність з актуальними протоколами і не дасть «просадити» швидкість мережі при підключенні застарілого обладнання .

П. Channel Width визначає ширину смуги під бездротовий канал зв'язок. Виставляємо Auto 20/40MHz.

У пункті Transmission Rate можна примусово задати максимальну швидкість передачі даних в бездротовій мережі. Залишити в положенні Auto.

Enable Hidden Wireless ховає бездротову мережу (а саме - розсилку SSID) від непрошених гостей. За допомогою даної опції додатково забезпечуємо захист бездротової мережі від початківців хакерів.

В області Wireless Security Mode налаштовуємо шифрування бездротової мережі. Це дозволить захистити Wi-Fi мережу від небажаних вторгнень з боку зловмисників і любителів безкоштовного доступу в Інтернет. Вибираємо в п. Security Mode варіант Enable WPA2-Auto Wireless Security (enhansed).

5.3 Налаштування RADIUS

Клієнтські логіни і паролі користувачів передаються через бездротову мережу до Vantage RADIUS, де вони перивіряються згідно зі списком. Це гарантує, що тільки користувач з праильною комбінацією буде допущений до мережі.

Web Конфігуратор. Запускаємо браузер. Вводимо IP адресу пристрою (за замовчуванням 192.168.1.3). (рис. 5.5).

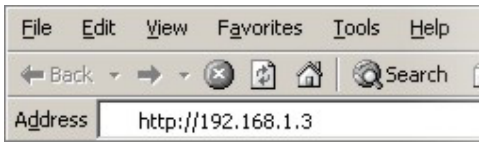

Рисунок 5.5 Адреса пристрою у вікні браузера

Вводимо логін та пароль за замовчуванням (admin та 1234), натискаємо кнопку Login. (рис. 5.6).

Рисунок 5.6 Вікно для вводу логіну та паролю

Після чого опиняємося у вікні конфігурації головного меню. Далі в меню обираємо ADVANCED для налаштування пристрою та натискаємо IP, щоб опинитися у вікні основної конфігурації мережі. (Рис. 5.7)

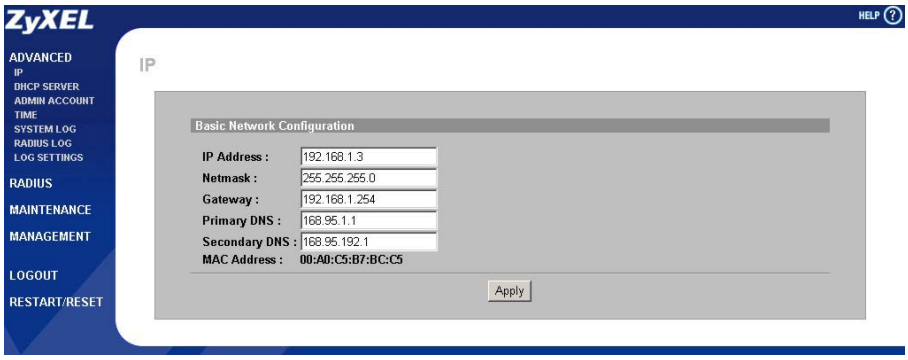

Рисунок 5.7 Вікно основної конфігурації мережі

У вікні основної конфігурації мережі водимо необхідні параметри та натискаємо кнопку Apply. (рис. 5.8)

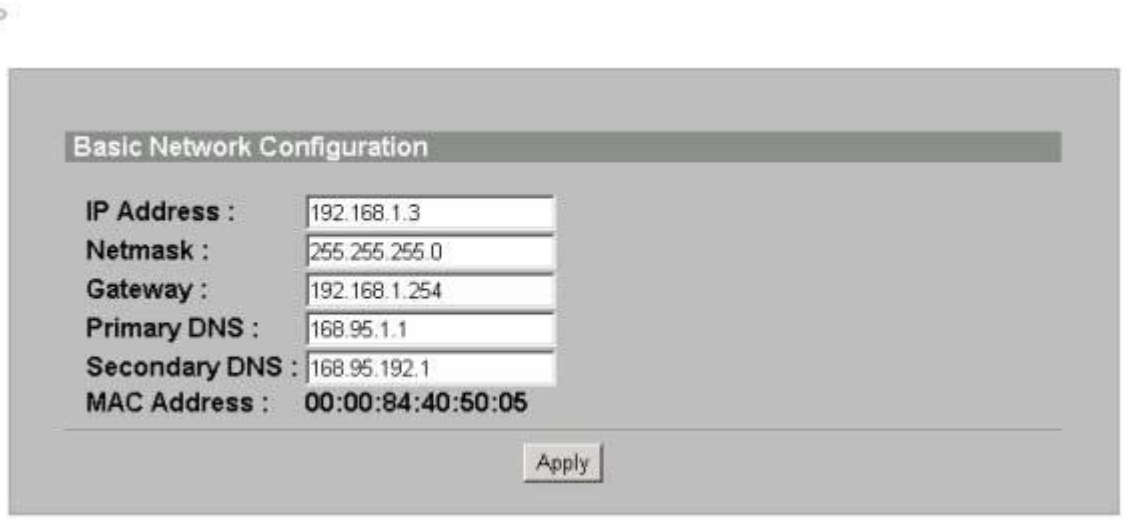

Рисунок 5.8 Параметри основної конфігурації мережі

Налаштування Параметрів Часу. Vantage RADIUS використовує системний годинник, щоб синхронізувати час через мережу і згенерувати log файли. Час може бути отриманий від сполучного комп'ютера, або Сервера NTP (Протокол Часу Мережі). Щоб встановити параметри часу, клацаємо на ADVANCED в головному меню, а потім натискаємо TIME. У вікні, що з’явилось встановлюємо параметри часу і натискаємо кнопку Apply (рис 5.9).

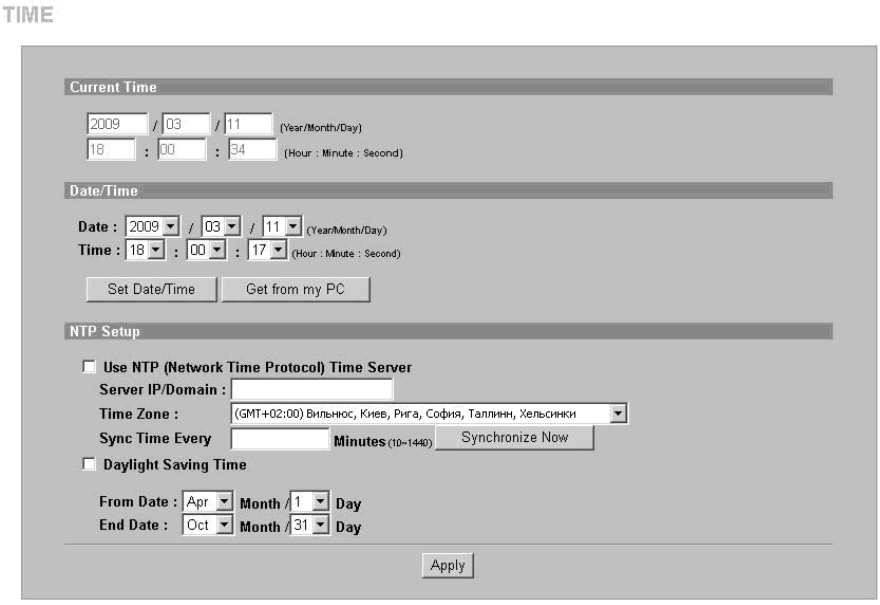

Рисунок 5.9 Вікно налаштування параметрів часу

Огляд EAP Authentication. EAP (Extensible Authentication Protocol) – протокол авторизації стандарту IEEE802.1x, дозволяючий застосовувати різні типи авторизації користувачів. Vantage RADIUS підтримує PEAP і EAP-MD5 (Message-Digest Algorithm 5). Наші точки доступу підтримують авторизацію бездротових клієнтів по стандарту 802.1x з використанням віддаленого серверу RADIUS.

Для налаштування підключень з точоками доступу, клацаємо на RADIUS в головному меню, а потім натискаємо RADIUS SERVER. У вікні, що з'явилось вибираємо RADIUS Type = Local Account/Remote Account, натискаємо кнопку Apply, встановлюємо порти аутентифікації і видачі облікових записів такимиж які були встановлені на точках доступу. Є також можливість обрати діапазон IP для якого буде застосовуватися аутинтифікація. Встановлюємо пункт визначити аутентифікацію для будь-якого IP, а також задаємо ключове слово і натискаємо кнопку Apply (рис. 5.10)

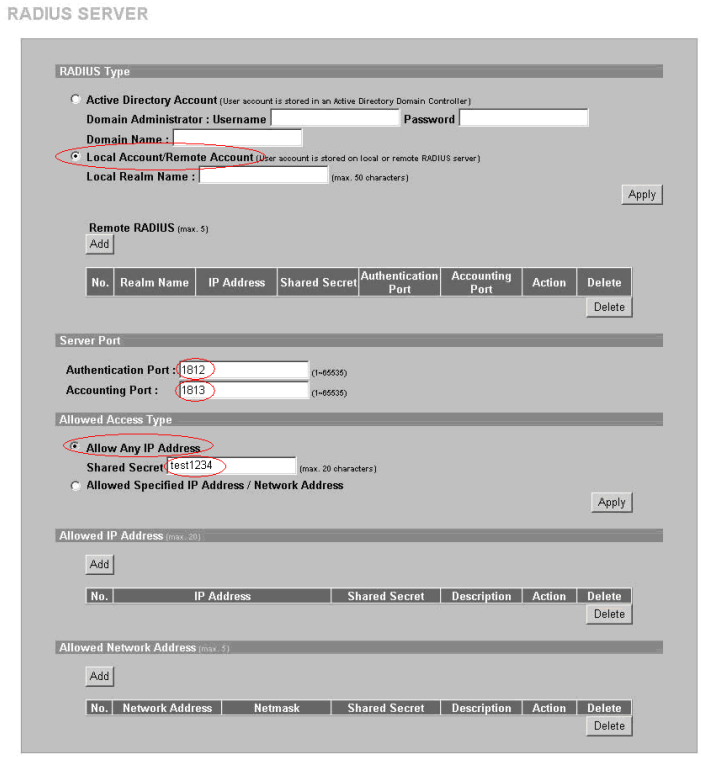

Рисунок 5.10 Вікно налаштування RADIUS SERVER

Тепер необхідно додати Користувачів. Для цього знову клацаємо на RADIUS в головному меню, а потім натискаємо USER ACCOUNT.

Кожен користувач, що потребує доступу у мережу, повинен мати логін і пароль. Натиснув кнопку Add New User, створюємо запис користувача (рис 5.11)

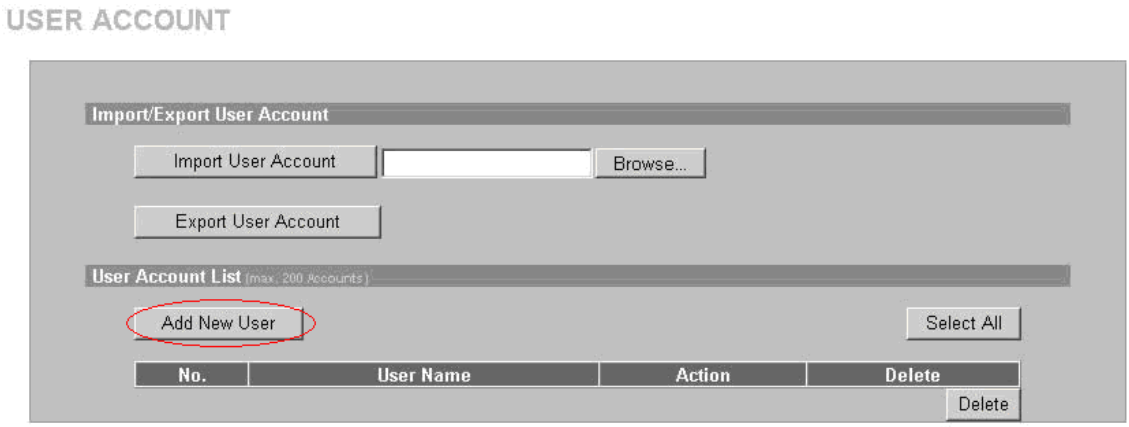

Рисунок 5.11 Вікно додавання користувачів

У вікні, що з’явилося додаємо імя користувача і пароль. (рис 5.12). Це треба зробити для кожного користувача.

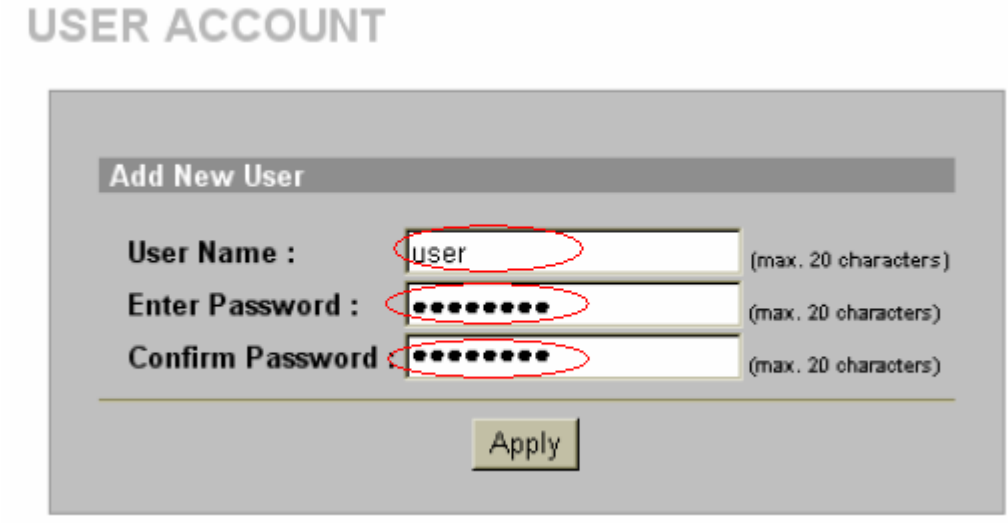

Рисунок 5.12 Вікно додавання нового користувача

6. ЕРГОНОНОМІКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

6.1 Розрахунок часу евакуації людей при пожежі в приміщенні

Підприємство є одноповерховою будівлею, що відображена на рис. 6.1 розмірами 10 м. на 20м.; кількість робочих кімнат 8; кількість працюючих 13; кількість виходів 1.

Для розрахунку загального часу евакуації необхідно розрахувати час на кожній ділянці руху людей, починаючи від максимально віддаленої точки.

Рух людей під час процесу евакуації є вимушеним, тобто пов’язаним із необхідністю покинути приміщення чи будівлю через виниклу небезпеку. Вимушений рух людей має свої специфічні особливості, вже на початковій стадії, людині погрожує небезпека в результаті того, що пожежа супроводжується виділенням теплоти, продуктів повного й неповного згорання, токсичних речовин, обвалення конструкцій, що так чи інакше погрожує людині. Із цього слід зробити висновок, що при плануванні будівлі і устрої приміщень в них необхідно прийняти заходи, щоб процес евакуації міг закінчитися безпечно і в необхідний час.

Друга особливість полягає у тому, що в силу погрожуючої людині небезпеки рух інстинктивно починається одночасно в один і той же напрям – у сторону виходів. Це призводить до того, що проходи швидко заповнюються людьми при визначеній щільності потоків. Із збільшенням щільності потоків швидкість руху зменшується, що створює певний визначений ритм руху. В цій ситуації з’являється погроза утворення затору, і дуже важко запобігти їй.

Показником ефективності процесу вимушеної евакуації є час, на протязі якого люди можуть при необхідності покинути окремі приміщення і будівлю в цілому. Безпечність, досягнута тоді, коли цей час менший, ніж тривалість пожежі. Короткочасність процесу евакуації повинна досягатися не тільки конструктивно-планувальними рішеннями, на які звертали увагу раніше, але й організаційними рішеннями.

Процес евакуації людей можна поділити на три етапи :

- рух людей від найбільш віддаленої точки приміщення до евакуаційних виходів;
- рух людей від евакуаційних виходів до виходів на зовні ;
- рух людей від виходів із будівлі та їх розсіювання.

При евакуації основними параметрами, які характеризують процес руху людей є :

1) щільність людського потоку – *D*, люд/м2;

2) швидкість руху людського потоку – *v*, м/хв;

3) пропускна спроможність шляху (виходів) - *Q* ;

4) інтенсивність руху людського потоку - *q* ;

1) Щільність людського потоку *D*, яка складається з *N* людей, дорівнює:

$$D_1 = \frac{N_1 f}{A}, \text{ м}^2/\text{м}^2 \qquad (6.1),$$

де $A = g \cdot l$ – площа шляху евакуаційної ділянки [м²];

l – довжина ділянки; *g*- ширина ділянки;

f – площа горизонтальної проекції людини.

Якщо $D < 0.05$ людина має повну свободу пересування;

Якщо $0.05<D<0.15$ людина не може вільно змінювати напрямок свого руху;

Якщо $0.15<D<=0.92$ люди рухаються вкупі. Величина 0.92 є верхньою межею, коли люди рухаються вкупі, та нею обмежується щільність при проектуванні евакуаційних шляхів.

2) Швидкість руху людського потоку *v* залежить від його щільності *D* та виду шляху (горизонтальні чи похилі). Значення швидкості v , а також інтенсивності руху людського потоку q в залежності від його цільності D приведено в табл. 6.1.

3) Пропускна спроможність шляху *Q* (м/хв чи люд/хв)

$$Q = D \cdot v \cdot \delta \text{ , м}^2/\text{хв.} \qquad (6.2)$$

4) Інтенсивністю руху людського потоку q (м/хв чи люд/хв)

$$q = D \cdot v \tag{6.3}$$

Таблиця 6.1 Значення швидкості v і інтенсивності q руху людського потоку залежно від його щільності D

Щільність потоку м²/м², Д	Горизонтальний шлях		Дверний проем	Сходи вниз		Сходи вверх	
	Швидкість м/хв. v	Інтенсивність, q м/хв.	Інтенсивність, q м/хв.	Швидкість м/хв. v	Інтенсивність, q м/хв.	Швидкість м/хв. v	Інтенсивність, q м/хв.
0,01	100	1	1	100	1	60	0,6
0,05	100	5	5	100	5	60	3
0,1	80	8	8,7	95	9,5	53	5,3
0,2	60	12	13,4	68	13,6	40	8
0,4	40	16	18,4	40	16	26	10,4
0,6	27	16,2	19	24	14,4	18	10,8
0,8	19	15,2	17,3	13	10,4	13	10,4
0,9 и більше	15	13,5	8,5	8	7,2	11	9,9

Інтенсивність руху не залежить від ширини шляху і являється характеристикою потоку. Інтенсивністю руху людського потоку на кожному відрізку дорівнює:

$$q_i = \frac{q_{i-1}\delta_{i-1}}{\delta_i}, \text{ м/хв.} \tag{6.4}$$

де: δ_{I}, $\delta_{\text{i-1}}$ – ширина розглядаючого і-го і перед ним (і – 1) відрізків шляху, м;

q_i, q_{i-1} – значення інтенсивності руху потоку на розглядаючому і-му і перед ним (і - 1) відрізках шляху, м/хв.

Якщо q_i менше чи рівно q_{max}, то час руху на відрізку можна визначити по формулі:

$$t_1 = \frac{l_1}{v_1}, \tag{6.5}$$

при цьому значення q_{max} треба приймати рівним, м/хв.:

- для горизонтальних шляхів 16,5
- для дверних пройомів 19,6
- для сходів вниз 16
- для сходів вверх 11

Розрахунковий час евакуації людей із приміщення й будівлі *tp* встановлюється по розрахунку часу руху людських потоків від найбільш віддалених місць розташування. При розрахунку весь шлях руху людського потоку поділяється на ділянки (прохід, коридор, сходинковий марш, дверний проріз, тамбур) довжиною l_i і шириною g_i.

Початковими ділянками являються проходи між робочими місцями.

Розрахунковий час евакуації дорівнює :

$$t_p = t_1 + t_2 + t_3 + \ldots + t_i = t \ [\text{хв}], \qquad t_i = l_i / v_i \ [\text{хв}].$$

де t_i – час руху людського потоку на кожній окремій ділянці.

Умова безпечної евакуації характеризується виразом $t_p <= t_{нб}$, тобто розрахункова тривалість вимушеної евакуації на різноманітних ділянках при розрахункових швидкостях людей і розрахунковій пропускній спроможності евакуаційних дверей повинна бути рівна або менша необхідного часу тривалості евакуації. Необхідний час евакуації $t_{нб}$ визначається по таблиці.

Використовуючи вище зазначений опис, за винятком таких ділянок як дверний проріз та тамбур (не передбачена у будівлі), проведемо розрахунок часу евакуації людей для прийнятого приміщення.

Маршрут евакуації розбивається на дев'ять етапів (ділянок). Для проведення розрахунку представимо план евакуації людей (рис. 6.1).

Перша ділянка

Час руху людського потоку – вихід людей з кімнати № 1:

де l= 13 м – довжина ділянки ; v – швидкість руху на ділянці.

f = 0.113 м^2 – середня площа горизонтальної проекції людини ;

N = 2 – кількість людей ; S= 3 м – ширина ділянки .

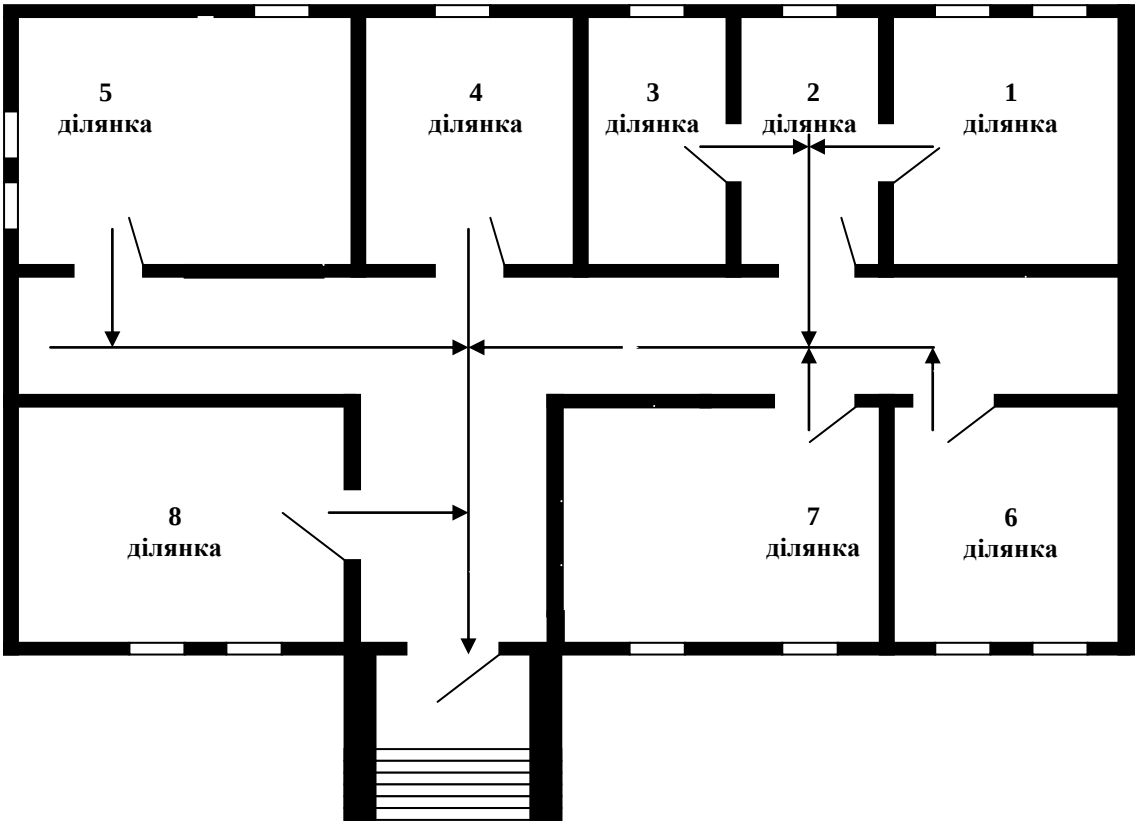

Рисунок 6.1 План евакуації людей

$D_1 = 2\left(\frac{0.113}{3 \cdot 13}\right) = 0.006$ [м^2/м^2], тоді v_1 = 100 м/хв ; q_1= 1 м/хв.

t_1 = 13/100 =0,13 хв.

Друга ділянка

Час руху людського потоку – вихід людей з кімнати № 2:

$D = 3\left(\frac{0.113}{11 \cdot 3}\right) = 0.01$ [м^2/м^2], тоді v_3 = 100 м/хв ; q_3= 1 м/хв.

t_2 = 11/100 =0,11 хв.

де l = 11 м; f = 0.113 м^2; N = 3; S = 3 м.

Третя ділянка

Час руху людського потоку – вихід людей з кімнати № 3:

$D = 1\left(\frac{0.113}{12 \cdot 3}\right) = 0.003$ [м^2/м^2], тоді v_2 = 100 м/хв; q_2= 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 1; S = 3 м.

Четверта ділянка

Час руху людського потоку – вихід людей з кімнати № 4:

$D = 2\left(\frac{0.113}{5 \cdot 3}\right) = 0.01$ [м^2/м^2], тоді v_4 = 100 м/хв; q_4 = 1 м/хв.

t = 5/100 =0,05 хв.

де l = 5 м; f = 0.113 м^2; N = 2; S = 3 м.

П'ята ділянка

Час руху людського потоку – вихід людей з кімнати № 5:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_5 = 100 м/хв ; q_5 = 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 2; S = 3 м.

Шоста ділянка

Час руху людського потоку – вихід людей з кімнати № 6:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_6 = 100 м/хв; q_6 = 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 2; S = 3 м.

Сьома ділянка

Час руху людського потоку – вихід людей з кімнати № 7:

$D = 2\left(\frac{0.113}{9 \cdot 3}\right) = 0.008$ [м^2/м^2], тоді v_7 = 100 м/хв; q_7 = 1 м/92в..

Т = 9/100 =0,09 хв.

Де l = 9 м; f = 0.113 м^2; N = 2; S = 3 м.

Восьма ділянка

Час руху людського потоку – вихід людей з кімнати № 8:

$D = 2\left(\frac{0.113}{3 \cdot 3}\right) = 0.02$ [м^2/м^2], тоді v_8 = 100 м/хв; q_8 = 1 м/хв.

t = 3/100 =0,03 хв.

де l = 3 м; f = 0.113 м^2; N = 2; S = 3 м.

Дев'ята ділянка

Час руху людського потоку – вихід людей з кімнати № 9:

$D = 7\left(\frac{0.113}{9 \cdot 3}\right) = 0.03$ [м^2/м^2], тоді v_9 = 100 м/хв; q_9 = 1 м/хв.

t = 9/100 =0,09 хв.

де l = 9 м; f = 0.113 м^2; N = 7; S = 3 м.

Десята ділянка

Час руху людського потоку – вихід людей з кімнати № 10:

$D = 11\left(\frac{0.113}{5 \cdot 3}\right) = 0.08$ [м^2/м^2], тоді v_{10} = 100 м/хв; q_{10} = 1 м/93в..

T = 5/100 =0,05 хв.

Де l = 5 м; f = 0.113 м^2 ; N = 11; S = 3 м.

Одинадцята ділянка

Час руху людського потоку – вихід людей з кімнати № 11:

$D = 13\left(\frac{0.113}{3 \cdot 3}\right) = 0.1632$ [м^2/м^2], тоді v_{11} = 60 м/хв; q_{11} = 12 м/хв.

t = 3/60 =0,05 хв.

де l = 3 м; f = 0.113 м^2 ; N = 13; S = 3 м.

Загальний час евакуації : $t = t_1 + t_2 + ... + t_{18}$ = 1,01 [хв].

$t_{нб}$ = 2,5 хвилин для одноповерхового будинку (з СНиП 2.01.02-85, табл. 12)

t = 1,01 < $t_{нб}$ = 2,5 хв, тобто вимоги пожежної безпеки виконуються.

В зв'язку з можливістю виникнення пожежі на території будівлі внаслідок несправної роботи комп'ютерні техніки, яка підключена до електромережі, я вирішив вибрати вуглекислотні вогнегасники моделі ОУ-8 та порошкові – моделі ОП-8Б. Розмістити їх необхідно на пожежних щитах в вестибюлі та біля пожежного, по одному екземпляру кожного типу.

За допомогою вогнегасника ОУ-8 можна гасити різні речовини, крім тих, які можуть горіти без доступу повітря. Також їм можна тушити пожежу в пристроях під напругою до 1000V, при умові приближення по струмопровідних частин не ближче одного метру.

Механізм припинення горіння за допомогою використання вуглекислого газу базується на його властивостях шляхом розбавлення знижувати концентрацію реагуючих речовин до рівня, при якому горіння становиться неможливим.

За допомогою вогнегасника ОП-8Б можна тушити палаюче електрообладнання під напругою до 1000V, легкозаймисті рідини, тліючі матеріали (навіть ті що горять без доступу повітря) праці в робочому приміщенні.

6.2 Ергономічні вимоги до організації і обладнання робочих місць з комп`ютерною технікою

Оператор обробки інформації при виконанні своєї роботи майже весь робочий час знаходиться в сидячому положенні за робочим столом, на якому розташоване його робоче обладнання. Для запобігання виникнення, пов`язаних з таким видом робіт, хвороб (скаліоз, хвороби очей та ін.), а також для усунення загального дискомфорту, зменшення втомлюваності працівника, підвищенню його продуктивності необхідно правильно організувати робоче місце.

Організація робочого місця передбачає:

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічного обґрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;

- раціональну компоновку обладнання на робочих місцях;
- урахування характеру та особливостей трудової діяльності;
- ДНАОП 0.00-1.31-99, ГОСТ 12.2.032-78, ДСанПІН 3.3.2.007-98

регламентує такі вимоги до організації робочого місця користувача ВДТ (візуальний дисплейний термінал):

1) Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400 мм, глибина – 80-1000 мм. Робочий стіл повинен мати простір для ніг висотою не менше ніж 450 мм, на рівні витягнутої ноги не менше 650 мм.

Робоче місце має бути обладнане підставкою для ніг шириною не менше ніж 300 мм, глибиною не менше ніж 400 мм, з можливістю регулювання по висоті в межах 150 мм та кута нахилу опорної поверхні – в межах 20°. Підставка повинна мати рифлену поверхню і бортик по передньому краю заввишки 10 мм.

2) Робочий стілець користувача ВДТ повинен мати такі основні елементи: сидіння, спинку та стаціонарні або знімні підлокітники. Робочий стілець має бути підйомно – поворотним, регульованим за висотою, за кутом нахилу сидіння та спинки і за відстанню від спинки до попереднього краю сидіння. Поверхня сидіння має бути плоскою, передній край заокругленим.

Висота поверхні сидіння має регулюватися в межах 400…500 мм, а ширина і глибина становити не менше ніж 400 мм. Кут нахилу сидіння – до 15° вперед і до 5° назад.

Висота спинки має становити (300 ± 20) мм, ширина – не менше ніж 380 мм, радіус кривизни горизонтальної площини – 400 мм. Кут нахилу спинки має регулюватися в межах 0…30° від вертикального

положення. Відстань від спинки до переднього краю сидіння має регулюватися в межах 260…400 мм.

Для зниження статичного навантаження м`язів верхніх кінцівок слід використовувати стаціонарні або знімні підлокітники довжиною не менше ніж 250 мм, шириною не менше ніж 50…70 мм. Що регулюються за висотою над сидінням у межах 230…260 мм і відстанню між підлокітниками в межах 350…500 мм.

Поверхня сидіння і спинки стільця має бути напівм`якою з нековзним, повітронепроникненим покриттям, що легко очиститься і не електризується.

Конструкція виробничих меблів для користувача ВДТ має бути такою, щоб забезпечувати йому підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; верхні частини рук – вертикальні; кут ліктьового суглоба (між плечем та передпліччям) – 70 - 90°; зап`ястки зігнуті під кутом не більше 20° відносно горизонтальної площини, нахил голови вперед в межах 15-20° до вертикалі.

3) Дисплей має розташуватися на столі на відстані від очей користувача не більше 700 мм (оптимальна відстань 450 – 500 мм). Розташування екрану має забезпечувати зручність зорового спостереження у вертикальній площині під кутом + 30° до нормальної лінії погляду працюючого. В горизонтальній площині кут спостереження екрану не повинен перевищувати 60°.

4) Клавіатуру слід розташувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачатися опорний пристрій, який дає змогу змінювати кут нахилу поверхні клавіатури у межах 5…10°. Висота середнього рядка клавіш має не перевищувати 30 мм. Поверхня клавіатури має бути матовою з коефіцієнтом відбиття 0,4.

5) Документ для вводу даних розташовується на відстані 450…500 мм від очей працівника, переважно зліва, кут між екраном дисплея та документом в горизонтальній площині має бути 30 - 40°.

6) Розміщення принтера або іншого пристрою введення – виведення інформації на робочому місці має забезпечувати добру видимість екрана ВДТ, зручність ручного керування пристроєм введення – виведення інформації в зоні досяжності: по висоті 900 – 1300 мм, по глибині 400 – 500 мм. Під принтери ударної дії потрібно підкладати вібраційні килимки для гасіння вібрації та шуму. На рис. 6.2 зображено вид робочого місця з ВДТ: A-принтер. B-монітор. C-системний блок. D-клавіатура. E-папка для документів.

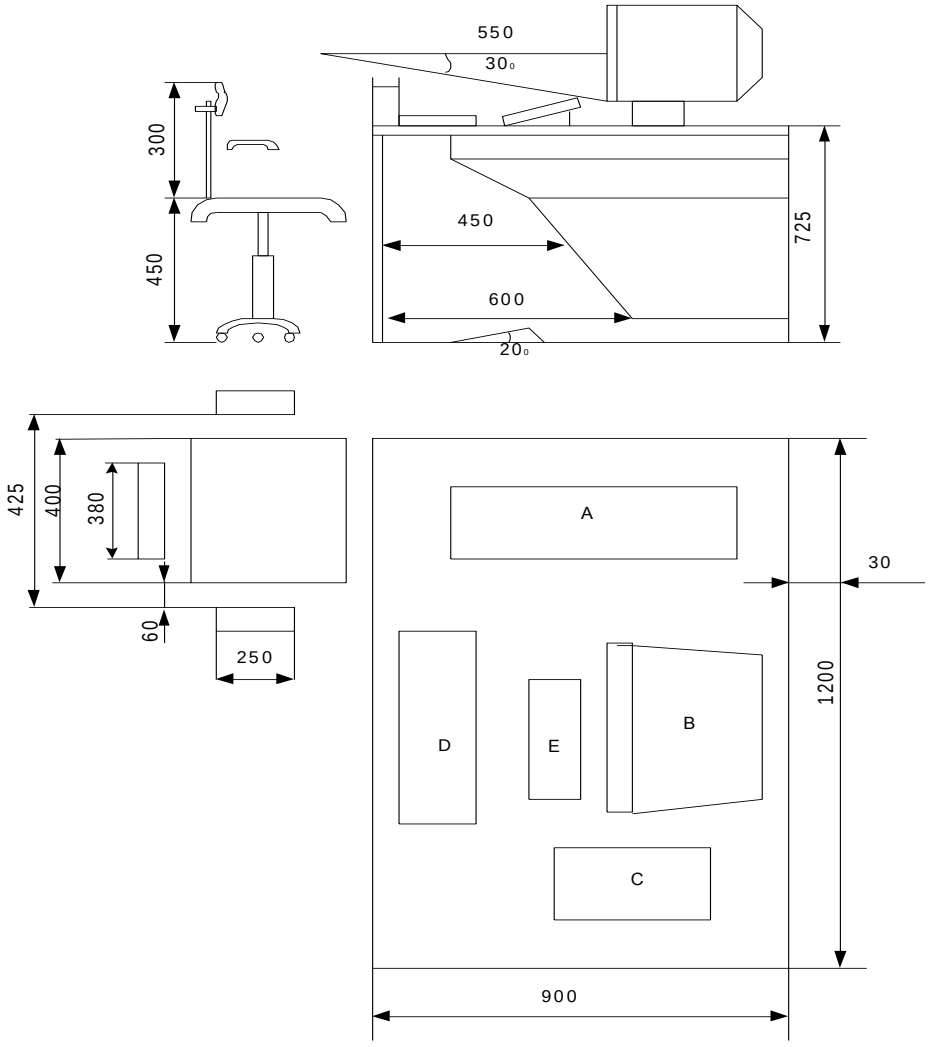

Рисунок 6.2 Вид робочого місця з ВДТ

ВИСНОВКИ

Використовуючи бездротову технологію, можна добитися величезних переваг. Вона дає користувачам відчуття вільного пересування без втрати зв'язку, конструкторам мережі - дає більше можливостей для організації з'єднань, а також сприяє появі безлічі нових пристроїв для доступу в мережу. Але при цьому бездротова технологія несе в собі набагато більше загроз, ніж звичайні дротові мережі.

Для реалізації поставленої задачі було виконано наступне:

- вивчено роботу бездротових мереж на фізичному рівні;
- проаналізовано можливості протоколів автентифікації та їх характеристики;
- розглянуто сучасні можливості технологій;
- була протестована можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж;
- проведено аналіз та використано одне із типів з'єднань з точкою доступу
- вивчено ринок серверів та налаштовано один з серверів для точки доступу.

В результаті атестаційної випускної роботи було проведено:

1. Проведений аналіз предметної області.
2. Проведена розробка інформаційного забезпечення системи.
3. Проведена розробка програмного забезпечення системи.
4. Впроваджений програмно – технічний продукт системи в сучасних умовах.
5. Проведені ергономічні дослідження в галузі інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. http://www.cnews.ru/
2. WiFiver.com - український Wi-Fi портал
3. http://wifi.nau.edu.ua/- WI-FIмережа НАУ
4. WI-FI.ru - російський Wi-Fi портал
5. Щербо В.К. «Стандарти обчислювальних мереж» - М.: Кудиц - Образ, 2000
6. Шахнович І. «Сучасні Технології бездротового зв'язку» - М.: Техносфера, 2004
7. Джим Гейер. «Бездротові Мережі. Перший крок »- М.: Видавництво: Вільямс, 2005
8. "Основы построения беспроводных локальных сетей стандарта 802.11", Рошан, Издательский дом "Вильямс", Москва, 2004
9. Wi-fi: «боевые» приемы взлома и защиты безпроводных сетей» А.А. Владимиров; К. В. Гавриленхо; А. А. Михайловский. Москва 2005
10. В. Г. Олифер, Н. А. Олифер Компьютерные сети. Принципы, технологии, протоколы.4-е изд.-2008, СПб, Издательский дом "Питер", 958 стр.
11. Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей.- М.: Горячая линия- Телеком, 2008.- 288 с.:.
12. http://www.dlink.com.tr
13. http://www.tradetelecom.ru
14. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видатничій Центр, 2002. – 520 с.
15. 2Тененбаум Э. Компьютерные сети. 4-е изд. – СПБ. Питер. 2005. – 992 с.

16. Рослякв А.В., Ваняшин С.В., Самсонов М.Ю. и др. Сети следующего поколения NGN / Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2008. – 424 с.

17. Величко В.В., Катунин Г.П., Шувалов В.П. Оснолвы инфокоммуникационных технологий. Учебное пособие для вузов/Под ред. В.П. Шувалова. – М.: Горячая линия – Телеком, 2009. – 712 с.

18. Иртегов Д.В. Введение в сетевые иехнологии. – СПБ.: БХВ-Петербург, 2004. – 560 с.

19. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.

20. Brassard G. Modern Cryptology. - N.Y.: Springer-Verlag, 1988. - 107 p.

21. Cisco Systems, Designing a Campus Network for High Availability. – 2006 – 60c.

22. Cisco Systems, Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design. – 2006. – 91c.

23. Cisco Systems, Understanding Rapid Spanning Tree Protocol (802.1w) (Document ID: 24062). - 2006. – 14c.

24. Cisco Systems, Understanding Multiple Spanning Tree Protocol (802.1s) (Document ID: 24248). – 2005. – 14c.

25. David Hucaby. CCNP Self-Study: CCNP BCMSN Exam Certification Guide, Third Edition. – Cisco Press, 2005. – 624c.

26. Dave Hucaby, Steve McQuerry. Cisco Field Manual: Catalyst Switch Configuration. – Cisco Press, 2002. – 560c.

27. Eric Ouellet, Robert Padjen, Arthur Pfund, Ron Fuller, Tim Blankenship ―Building a Cisco Wireless LAN‖ - Syngress Publishing, Inc, 2002.