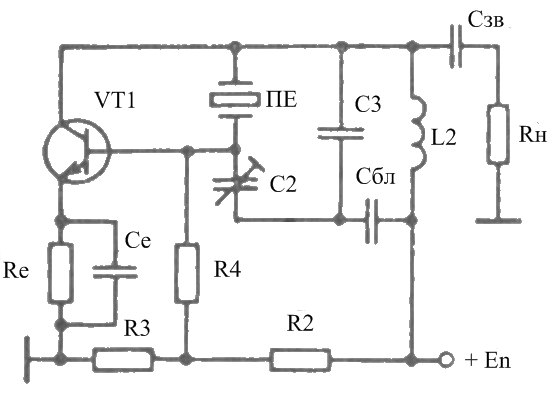
**Вступ**

Мета даного дипломного проекту полягає в огляді існуючих можливостей на базі сучасних і економічно доцільних технологій, розробці й розгортанні локальної мережі на основі технології Wi-Fi.

Введення.

У всьому світі стрімко росте потреба в бездротових з'єднаннях, особливо у сфері бізнесу. Користувачі з бездротовим доступом до інформації - завжди і скрізь можуть працювати набагато більш продуктивно і ефективно, ніж їх колеги, прив'язані до дротових телефонним та комп'ютерним мережам.  
Зазвичай бездротові мережеві технології групуються в три типи, що розрізняються за масштабом дії їх радіосистем, але всі вони з успіхом застосовуються в бізнесі.  
 PAN (персональні мережі) - короткодействующих, радіусом до 10 м мережі, які пов'язують ПК і інші пристрої - КПК, мобільні телефони, принтери і т. п. За допомогою таких мереж реалізується проста синхронізація даних, усуваються проблеми з великою кількістю кабелів в офісах, реалізується простий обмін інформацією в невеликих робочих групах. Найбільш перспективний стандарт для PAN - це Bluetooth.  
 WLAN (бездротові локальні мережі) - радіус дії до 100 м. З їх допомогою реалізується бездротовою доступ до групових ресурсів в будівлі, університетському кампусі і т. п. Зазвичай такі мережі використовуються для продовження дротяних корпоративних локальних мереж. У невеликих компаніях WLAN можуть повністю замінити дротяні з'єднання. Основний стандарт для WLAN - 802.11.  
 WWAN (бездротові мережі широкої дії) - бездротовий зв'язок, яка забезпечує мобільним користувачам доступ до їх корпоративних мереж та Інтернету. Поки тут немає домінуючого стандарту, але найбільш активно впроваджується технологія GPRS - найшвидше в Європі і з деяким відставанням в США.  
 На сучасному етапі розвитку мережевих технологій, технологія бездротових мереж Wi-Fi є найбільш зручною в умовах вимагають мобільність, простоту установки і використання. Wi-Fi (від англ. Wireless fidelity - бездротовий зв'язок) - стандарт широкосмугового бездротового зв'язку сімейства 802.11 розроблений у 1997р. Як правило, технологія Wi-Fi використовується для організації бездротових локальних комп'ютерних мереж, а також створення так званих гарячих точок високошвидкісного доступу в Інтернет.   
1.1 Архітектура, компоненти мережі і стандарти   
Стандарт RadioEthernet IEEE 802.11 - це стандарт організації бездротових комунікацій на обмеженій території в режимі локальної мережі, тобто коли декілька абонентів мають рівноправний доступ до загального каналу передач. 802.11 - перший промисловий стандарт для бездротових локальних мереж (Wireless Local Area Networks), або WLAN. Стандарт був розроблений Institute of Electrical and Electronics Engineers (IEEE), 802.11 може бути порівняний зі стандартом 802.3 для звичайних дротових Ethernet мереж.   
 Стандарт RadioEthernet IEEE 802.11 визначає порядок організації бездротових мереж на рівні управління доступом до середовища (MAC-рівні) і фізичному (PHY) рівні. У стандарті визначений один варіант MAC (Medium Access Control) рівня та три типи фізичних каналів.   
Подібно провідникового Ethernet, IEEE 802.11 визначає протокол використання єдиного середовища передачі, що отримав назву carrier sense multiple access collision avoidance (CSMA / CA). Вірогідність колізій бездротових вузлів мінімізується шляхом попереднього посилки короткого повідомлення, званого ready to send (RTS), воно інформує інші вузли про тривалість майбутньої передачі і адресата. Це дозволяє іншим вузлам затримати передачу на час, рівне оголошеній тривалості повідомлення. Приймальна станція повинна відповісти на RTS посилкою clear to send (CTS). Це дозволяє передати вузлу дізнатися, чи вільна середовище та чи готовий приймальний вузол до прийому. Після отримання пакета даних прийомний вузол повинен передати підтвердження (ACK) факту безпомилкового прийому. Якщо ACK не отримано, спроба передачі пакету даних буде повторена.   
У стандарті передбачено забезпечення безпеки даних, яке включає аутентифікацію для перевірки того, що вузол, що входить в мережу, авторизований в ній, а також шифрування для захисту від підслуховування.   
 На фізичному рівні стандарт передбачає два типи радіоканалів і один інфрачервоного діапазону.   
 В основу стандарту 802.11 покладена стільникова архітектура. Мережа може складатися з однієї або кількох комірок (сот). Кожна сота управляється базовою станцією, званої точкою доступу (Access Point, AP). Точка доступу і знаходяться в межах радіуса її дії робочі станції утворюють базову зону обслуговування (Basic Service Set, BSS). Точки доступу многосотовой мережі взаємодіють між собою через розподільну систему (Distribution System, DS), що представляє собою еквівалент магістрального сегменту кабельних ЛЗ. Вся інфраструктура, що включає точки доступу та розподільну систему, утворює розширену зону обслуговування (Extended Service Set). Стандартом передбачений також односотовий варіант бездротової мережі, який може бути реалізований і без точки доступу, при цьому частина її функцій виконується безпосередньо робочими станціями.

**1.2 Обгрунтування вибраної технології**

   
2. Аналіз вимог, що перед'являються до перспективних технологій.

Проведемо аналіз вимог що пред'являються до побудови корпоративних мереж передачі даних:   
  
2.1 Вибір передаючого середовища.   
 Найчастіше перед розробниками і творцями корпоративних мереж передачі інформації стоїть завдання вибору передавальної середовища.   
Як передає середовища можуть використовуватися наступні:

- Мідний кабель;   
- Волокно - оптичний кабель;   
- Радіоканал;   
- Оптичний канал;   
- Лазерний канал.

Вибір передавальної середовища обумовлений, як правило, вимогами, що пред'являються до мережі доступу корпоративної системи передачі даних:

- Мережа повинна бути недорогою;   
- Мережа повинна мати широку інфраструктуру;   
- Мати можливість до масштабування.

Найчастіше мережа доступу не може бути розширена, за рахунок дротових мереж з цілого ряду причин:

- проблема прокладки кабелю, що призводить до високої вартості мережі.   
- високая вартість робіт.   
- відсутність телефонних ліній

У цьому випадку завдання може бути вирішене за рахунок використання систем фіксованого широкосмугового радіодоступу. Передача даних по радіоканалу в багатьох випадках надійніше і дешевше, ніж передача по комутованих або орендованим каналах, і особливо по каналах стільникових мереж зв'язку. У ситуаціях, у зв'язку з відсутністю розвиненої інфраструктури зв'язку, використання радіозасобів для передачі даних часто є єдино розумним варіантом організації зв'язку.   
 Мережа передачі з використанням радіомодемів може бути розгорнута практично в будь-якому географічному регіоні. Залежно від використовуваних радіостанцій така мережа може обслуговувати своїх абонентів у зоні радіусом від одиниць до сотень кілометрів. Величезну практичну цінність радіомодеми мають там, де необхідна передача невеликих обсягів інформації (документів, довідок і т.д.).   
 Радіомодеми часто називають пакетними контроллерами (TNC - Terminal Node Controller) унаслідок того, що до їх складу входить спец. контролер, який здійснює обмін даними з комп'ютером, управління форматування кадрів і доступом до загального радіоканалу відповідно до реалізованим методом множинного доступу. Радіомодеми орієнтовані для роботи в єдиному радіоканалі з багатьма користувачами (в каналі множинного доступу), а не в каналі "точка - точка" (модем для комутованих ліній).

 1.Гнучкість конфігурації.

Всі бездротові мережі підтримують як режим інфраструктури (підключення через точку доступу) так і режим "рівний з рівним" (без застосування точки доступу). Можна додавати нових користувачів і встановлювати нові вузли мережі в будь-якому місці. Бездротові мережі можуть бути встановлені для тимчасового використання в приміщеннях, де немає інстальованої кабельної мережі або якщо прокладка мережевих кабелів ускладнена.

2. Простота розширення мережі.

Бездротові робочі станції можуть додаватися без погіршення продуктивності мережі. Перевантаження мережі трафіком можна легко уникнути додаванням точки доступу для скорочення часу відгуку мережі.

3. Бездротовий доступ в Інтернет

.   
 До точці доступу можна підключити маршрутизатор. Дана схема приваблива тим, що бездротові користувачі можуть розділяти загальний доступ в Інтернет.

4.Підтримка роумінгу.

Завдяки підтримці роумінгу між точками доступу користувачі можуть продовжувати працювати з ресурсами мережі навіть під час переміщення.

5. Середовище передачі.

У фізичному середовищі IEEE 802.11b розповсюджується за допомогою малопотужного шумоподібних сигналу, маючи більше десятка частотних каналів шириною 22 MГц в області 2,4 ГГц. Щадні режими експлуатації дозволяють використовувати частотний ресурс вельми інтенсивно. Характер сигналу дозволяє встановлювати зв'язок на дальності до 110 км за наявності не тільки прямий оптичної видимості між кінцевими точками, але і за відсутності перешкод в області так званої першої зони Френеля. В умовах разновисотной забудови, сніжно-дощового клімату, про офіційну реєстрацію зв'язку на дальність більше 5 км говорити можна, але потрібно дуже серйозно поставитися до вибору обладнання. На таких відстанях у містах застосовується каналоутворюючого обладнання. Cтандарт 802.11, є своєрідним проривом в області бездротових мереж. Можна виділити три принципових переваги цих технологій над кабельними мережами:

- неможливість приєднання рухомих (інакше, мобільних) абонентів є принципово нездоланною обмеженням чисто кабельних мереж (тобто мереж, що використовують кабелі і на мережевих магістралях, і для під'єднання абонентів). Це обмеження відноситься до будь-якого виду комунікацій - як до звичайного телефонного та факсимільного зв'язку, так і до передач даних. Фактор мобільності радіомереж набуває першорядного значення, коли користувач не має можливості підключення до звичайної дротової мережі та повинен переміщатися в межах певного району.

- інша перевага бездротових мереж має не технологічний а економічний характер - фактор віддаленості. Воно стосується приєднання віддалених абонентів до мережі. Це можуть бути абоненти, розкидані по великій, малонаселеній або важкодоступній території, або згруповані у віддаленому пункті. У таких випадках протягувати кабель не завжди економічно доцільно.

- нарешті, третій чинник специфічний для країн з економікою, що розвивається і частково відстає в розвитку телефонних мереж загального користування. До цієї категорії можна віднести і нашу країну. Фактор терміновості виражається в тому, що надійні комунікації потрібні зараз, а для прокладання кабельної мережі потрібні колосальні інвестиції і тривалий час.

**1.3 Аналіз перспективних технологій побудови. Абонентські частини мережі**.

**1.3.1** **Система фіксованого широкосмугового радіодоступу**.

Аналіз результатів розвитку технологій користувацького доступа за останнє десятиріччя показує, що для надання послуг мультимедіа в даний час існує широкий вибір бездротових технологій користувацького доступу. В даний час, системи радіодоступу будуються у відповідності з наступними стандартами:

1. HiperLAN2;   
2. MMDS;   
3. WLL;   
4. IEEE 802.11/b/g.

**1.3.1.1 HiperLAN2**

HiperLAN2 базується на нещодавно розробленої радіотехнології, створеної спеціально для взаємодій по локальній мережі в рамках проекту Broadband Radio Access Networks (BRAN), що реалізується Європейським інститутом стандартів у галузі електрозв'язку (ETSI), радіотехнологія - так зване ущільнення з ортогональним поділом частот (Orthogonal Frequency Division Multiplexing , OFDM), реалізація якого є вельми серйозною технічною задачею. Найбільш привабливою рисою HiperLAN2 є її висока швидкість, як якою іноді помилково називається величина 54 Мбіт / с. Дійсно, номінальна швидкість радіопередачі складатиме 54 Мбіт / с, але типова швидкість для додатків буде ближче до 20 Мбіт / с. Інша характерна риса - підтримка QoS, що вельми важливо для таких додатків, як відео і мова. Архітектура HiperLAN2 забезпечує з'єднання з безліччю типів мереж, в тому числі Ethernet (вона буде підтримуватися в числі перших), IP, ATM і PPP. Функції захисту включають аутентифікацію і шифрування. Цілком Побудова мереж на основі технології HiperLAN2 потребують значних інвестицій. По-перше, єдиний стандарт по бездротові локальні мережі, на сьогоднішній день широко застосовуваний був запропонований IEEE, а зовсім не ETSI. По-друге, IEEE вже має декілька стандартів на бездротові локальні мережі, в тому числі стандарт 802.11a, який забезпечує швидкість передачі 54 Мбіт / с. І по-третє, жодна компанія з числа підтримали проект HiperLAN2 не є визнаним лідером в області локальних мереж. Працює дана технологія в 5Ггц діапазоні який в даний момент ще не ліцензований. Щоб колективні мережі в стандарті HiperLAN2 дійсно забезпечували широкосмуговий доступ, вони повинні мати безліч точок доступу і безліч каналів, які забезпечують свободу пересувань в межах певної території.   
MMDS   
 Система MMDS (Microwave Multipoint Distribution Service - Мікрохвильові багатокрапкові розподільчі системи) отримали в останні роки широке поширення як альтернатива класичним кабельним мережам, в яких розподільна мережа будується за рахунок прокладки коаксіальних або оптичних кабелів. Можливість інтеграції систем MMDS з високошвидкісним бездротовим обміном цифровими даними, дозволяє легко вирішити проблему «останньої» милі, забезпечуючи радіус мовлення, обмежений лінією горизонту (близько 60 км).   
Запитувані користувачем дані транслюються спадними потоками в цифрових каналах, що використовують модуляцію QPSK, 16 -, 32 -, 64 -, 128 - або 256-QAM. При цьому, залежно від ширини каналу й обраної схеми модуляції сигналу, в одному каналі шириною до 8 МГц забезпечується швидкість передачі даних до 56 Мбіт / сек. часу, що в 1000-1500 разів швидше, ніж дозволяє аналоговий телефонний модем (33,6 Кбіт / с), в 200-400 разів швидше, ніж по лінії ISDN (64 і 128 Кбіт / с). Радіус зони обслуговування системи ММDS визначається висотою підвісу передавальної антени, потужністю передавача, кількістю переданих каналів, втратами в антенно-фідерного тракту і коефіцієнтом посилення передавальної і приймальної антен. В процесі будівництва і експлуатації виявлено ряд переваг системи MMDS. Головним недоліком технології є висока вартість обладнання, велика кількість обслуговуючого персоналу.

**1.3.1.2 WLL**

Перші системи фіксованого бездротового доступу (WLL-Wireless Local Loop) були розроблені в кінці 1980-х - початку 1990-х років для вирішення вельми актуальної задачі - розширення зони обслуговуван ¬ ня АТС. Назва цього класу систем визначає і їх призначення-надання послуг традиційної телефонії абонентам, розташовані за межами зони обслування.   
 Системи WLL є системами типу "точка - багатоточка", працюють в діапазонах частот від 1,5 до 3,5 ГГц, а мережі на базі систем WLL будуються по стільниковому принципом. До складу систем WLL входять:   
- центральна станція (ЦС), що забезпечує підключення й управління всією мережею в цілому;   
- ретрансляційні станції (PC), що дозволяють забезпечити суцільне покриття обслуговуваної території і розширити зону обслуговування до декількох сотень кілометрів (в залежності від кількості послідовно включених ретрансляторів);   
- термінальні станції (ТЗ), встановлюють у зонах обслуговування;   
- система технічного обслуговування, реалізована у вигляді програмного забезпечення на рівні управління мережевими елементами і встановлюється на персональному комп'ютері.   
 Системи WLL надають послуги ТФОП (телефонія, факс і передача даних з використанням dial-up-модемів) абонентам, віддаленим на десятки кілометров. Основний недолік даних систем є висока вартість, складність установки та експлуатації устаткування.   
 Розвиток систем класу FBWA в кінці 1990-х років обумовлено кількома факторами:

- практично загальної інформатизація;   
- появою широкого набору високошвидкісних транспортних технологій.   
- розробкою концепції побудови мереж наступного покоління, що забезпечують єдине управління всіма видами трафіку в сучасних мультисервісних мережах зв'язку.

Таким чином, системи FBWA призначені для надання індивідуальним і корпоративним користувачам сучасних послуг.   
Представлені в даний час на ринку рішення класу FBWA практично не мають PC, що обмежує радіус їх зони обслуговування в межах одного осередку.   
У системах FBWA використовується секторний принцип побудови ЦС, до складу якої входять кілька приймально-передавальних пристроїв, обслуговуючих кожен свій сектор, причому в кожному секторі можуть бути організовані колька радіоканалів.   
 Термінальні станції сучасних систем FBWA забезпечують підключення до різних послуг широкого кола як індивідуальних, так і корпоративному користувачів, включаючи ЛВС, УАТС, мережі Frame Relay та ін.   
І нарешті, окрім надання послуг користувацького доступу, системи FBWA широко використовуються в якості бездротових міських мереж для надання транспортних послуг (наприклад, для підключення базових станцій до комутаторов мобільних мереж зв'язку).

**1.3.2 Організація радіоінтерфейсу**

Смуги частот для систем FBWA визначені міжнародним регламентом радіозв'язку, в діапазонах частот від 3 кГц до 400 ГГц. Під останніми слід розуміти три категорії смуг частот, призначених для використання:

- переважно РЕЗ урядового призначення (категорія ПР);   
- переважно РЕЗ громадського призначення (категорія ГР);   
- спільно РЕЗ урядового і громадського призначення (категорія СІ).

Сучасні системи FBWA працюють у діапазонах частот 2,4; 3,5; 5; 10,5; 26/28 ГГц, аж до 40 ГГц, котрі відносяться до категорії ПР або СІ .. Крім того, частотний ресурс у кожному конкретному регіоні досить обмежений. Тому оператору, який вирішив надавати послуги з використанням систем FBWA, слід перед вибором обладнання з'ясувати ситуацію з наявністю частотного ресурсу в регіоні розгортанням системи у відповідному центрі радіочастот.   
 Переклад систем FBWA в область більш високих частот пов'язаний, з одного боку, із зайнятістю низькочастотних діапазонів, особливо у великих містах, а з іншого - з необхідністю забезпечення достатнього частотного ресурсу для широкого розвитку систем даного класу . Так, наприклад, якщо для систем стандартів IEEE 802.11b / g виділений частотний ресурс 83,5 МГц у діапазоні 2,4 ГГц, то для розгортання систем FBWA регулюючі органи в галузі телекомунікацій виділили смугу частот 300 МГц у діапазоні 10,5 ГГц і по 2 ГГц - в діапазонах 26/28 ГГц. Для розвитку особливого класу систем фіксованого широкосмугового бездротового доступу, що одержали назву MWS (Multimedia Wireless System), в діапазоні 40 ГГц виділений частотний ресурс 3 ГГц.   
 Слід зазначити, що при проектуванні мереж FBWA, що працюють у діапазонах вище 15-20 ГГц, необхідно враховувати вплив атмосферних явищ на якість радіозв'язку, а радіус зони обслуговування однієї ЦС при цьому не буде перевищувати кількох кілометрів.   
 Більш вузькосмугові системи можуть встановлюватися в регіонах з обмеженим частотним ресурсом, розгортання ж широкосмугових систем хоча і вимагає наявності більшої частотного ресурсу, проте забезпечує високу масштабованість створюваної мережі доступу.

**1.3.3 Загальні характеристики систем**

Радіус зони обслуговування ЦС у великій мірі залежить від діапазону частот, у якому працює дане обладнання, а від виду використовуваної в системі модуляції. Для систем FBWA, що працюють в діапазонах 2,4 і 3,5 ГГц, радіус зони обслуговування складає 15-20 км, а в діапазоні 26-28 ГГц він зменшується до 3-5 км. Таким чином, якщо для надання послуг доступу на значній території оператор планує використовувати обладнання, працююче в більш високочастотному діапазоні, то витрати на організацію мережі збільшаться у зв'язку з необхідністю встановлення декількох ЦС. У той же вона буде мати високу масштабованість і операторові буде простіше отримати дозвіл на частоти для експлуатації обладнання.   
 Потенційна ємність сучасних систем FBWA (тобто максимальна кількість ТЗ, які може прослужити одна ЦС) досягає 1000 ТЗ і більше. Однак реальна ємність мережі оператора на базі систем FBWA буде залежати від цілої низки чинників: методу доступу; використовуваної в радіотракті мережевої технології; способів представлення каналів і т.д., а в першу чергу - від виду надаваних пос луг. При наданні тільки транспортних послуг на базі виділених ліній кількість ТЗ буде повністю визначатися пропускної здатністю системи і надаваних в оренду виділених ліній. У разі надання оператором переважно послуг телефонії ємність системи залежить від пропускної здатності системи, типу вживаного кодека, середньго телефонного навантаження і відсотка відмов в обслуговуванні викликів. Якщо ж абонентами мережі доступу будуть переважно користувачі послуг передачі даних, то при визначенні ємності мережі необхідно орієнтуватися на узгоджену швидкість передачі (CIR), яка вказується в угоді про рівень обслуговування (SLA), що укладається між оператором та користувачами мережі доступу.   
 При побудові мереж на базі систем FBWA необхідно також враховувати, що часто заявлені виробниками швидкості в кілька десятків мегабіт в секунду є не пропускною здатністю системи, а швидкістю передачі інформації в радіотракту. Реальна ж пропускна здатність залежить, зокрема, від використовуваного методу доступу і від числа обслуговуваних користувачів.

**1.4 ХАРАКТЕРИСТИКИ СТАНДАРТІ**В **СЕРІЇ 802.11**

Стандарт має назву IEEE 802.11, розроблений на базі стандарту Ethernet для локальних мереж і є його повним аналогом. Існують три основні схеми роботи користувачів, що використовують обладнання даного типу: «точка-точка», «зірка», «все з кожним».

**«Точка-точка»**

Цей тип з'єднання найбільш часто застосовується для організації постійного з'єднання між двома віддаленими абонентами. У цьому випадку важлива не мобільність абонентів, а надійність при передачі даних. Тому, як правило, обладнання встановлюється стаціонарно. Використання вузьконаправлених антен і підсилювачів дозволяє в окремих випадках забезпечувати стійкий зв'язок на відстані понад 50 кілометрів. Подібне рішення ідеально підходить для магістральних ліній з малою завантаженістю і корпоративних мереж (зв'язок між двома локальними мережами, розташованими у віддалених офісах). При з'єднанні Ad-Hoc (точка-точка) всі комп'ютери оснащені бездротовими картами (клієнтами) і з'єднуються безпосередньо один з одним по радіоканалу працює за стандартом 802.11b і забезпечують швидкість обміну 11 Мбіт / с, чого цілком достатньо для нормальної роботи.



Рисунок 1.1 З'єднання Ad-Hoc (точка-точка).

**«Зірка»**

Використовується при підключенні як стаціонарних, так і мобільних абонентів. Принцип побудови такої мережі дуже схожий з принципами побудови мережі. У якості базової станції («соти») використовується обладнання з широконаправленною (кругової) антеною (кут горизонтального огляду 360 градусів). На боці абонента в залежності від ступеня мобільності використовується або вузьконаправлена, або широконаправлена антена.

**«Всі з кожним».**

Таке рішення найчастіше застосовується всередині будівель для організації локальної мережі, абоненти якої не прив'язані до своїх робочих місць. Кожна станція оснащується всенаправленною антеною, що дозволяє підтримувати зв'язок з кожним з абонентів в радіусі 200 метрів. Крім забезпечення свободи пересування, дане рішення дозволяє уникнути витрат на розгортання кабельної інфраструктури всередині будівлі.   
 Обладнання стандарту 802.11 ділиться на різні категорії за трьома ознаками: дальність, метод і швидкість передачі.   
 Кожне приймально-передавальний пристрій, що працює на радіохвилях, займає певну ділянку радіоспектра. Кожен такий діапазон характеризується центральної частотою, яка також називається «несучою», і шириною діапазону. Дальність роботи напряму залежить від несучої частоти діапазону. Чим вище частота, тим більше прямолінійно поширюється радіохвиля. Звідси ясно, що обладнання, яке працює на великих частотах, найбільш ефективно використовується в умовах прямої видимості. Для передачі на великі відстані має сенс використовувати більш низькочастотного устаткування, що дозволяє огинати предмети, які перешкоджають поширенню сигналу.   
 Швидкість передачі даних залежить від ширини смуги і не залежить від несучої частоти. Таким чином, неважливо, в якому місці радіоспектру розташовується канал - швидкість буде однаковою. Використання більш високої несучої частоти дозволяє збільшити кількість одночасно працюючих каналів. Існуюче на сьогоднішній день обладнання працює в трьох діапазонах: 915 МГц, 2,4 ГГц і 5 ГГц.

**1.5 Методи передачі даних**

**1.5.1 Організація мережі**

Стандарт IEEE 802.11 працює на двох нижніх рівнях моделі ISO / OSI: фізичному і канальному. Іншими словами, використовувати обладнання Wi-Fi так само просто, як і Ethernet: протокол TCP / IP накладається поверх протоколу, що описує передачу інформації по каналу зв'язку. Розширення IEEE 802.11b не зачіпає канальний рівень і вносить зміни в IEEE 802.11 тільки на фізичному рівні.   
 У бездротової локальної мережі є два типи обладнання: клієнт (звичайно це комп'ютер, укомплектований бездротової мережевої картою, але може бути і інший пристрій) і точка доступу, яка виконує роль моста між бездротовою та провідний мережами. Точка доступу містить приймач, інтерфейс провідної мережі, а також вбудований мікрокомп'ютер та програмне забезпечення для обробки даних.   
    
**1.5.1.1 Фізичний рівень IEEE 802.11**

Стандарт IEEE 802.11 передбачає передачу сигналу одним із двох методів - прямої послідовності (Direct Sequence Spread Spectrum, DSSS) і частотних стрибків (Frequency Hopping Spread Spectrum, FHSS) розрізняються способом модуляції, але використовують одну й ту ж технологію розширення спектру. Основний принцип технології розширення спектру (Spread Spectrum, SS) полягає в тому, щоб від вузькосмугового спектру сигналу, що виникає при звичайному потенційному кодуванні, перейти до широкосмугового спектру, що дозволяє значно підвищити перешкодостійкість передаваних даних   
 Метод FHSS передбачає зміну несучої частоти сигналу при передачі інформації. Для підвищення завадостійкості потрібно збільшити спектр передаваного сигналу, для чого несуча частота міняється по псевдовипадковому законом, і кожен пакет даних передається на своїй несучої частоті. При використанні FHSS конструкція прийомопередавача виходить дуже простий, але цей метод застосуємо, тільки якщо пропускна здатність не перевищує 2 Мбіт / с, так що в доповненні IEEE 802.11b залишився один DSSS. З цього випливає, що спільно з пристроями IEEE 802.11b може застосовуватися тільки те обладнання стандарту IEEE 802.11, яке підтримує DSSS, при цьому швидкість передачі не перевищить максимальної швидкості в "вузькому місці" (2 Мбіт / с), яким є обладнання, що використовує старий стандарт без розширення.   
 В основі методу DSSS лежить принцип фазової маніпуляції (тобто передачі інформації стрибкоподібним зміною початкової фази сигналу). Для розширення спектру переданого сигналу застосовується перетворення інформації, що передається в так званий код Баркера, який є псевдовипадковою послідовністю. На кожен передаваний біт припадає 11 біт в послідовності Баркера. Розрізняють пряму і інверсної послідовності Баркера. Через велику надмірності при кодуванні ймовірність того, що дія перешкоди перетворить пряму послідовність Баркера в інверсної, близька до нуля. Одиничні біти передаються прямим кодом Баркера, а нульові - інверсним.   
 Під бездротові комп'ютерні мережі в діапазоні 2,4 ГГц відведений досить вузький "коридор" шириною 83 МГц, розділений на 14 каналів. Для виключення взаємних перешкод між каналами необхідно, щоб їх смуги відстояли один від одного на 25 Мгц. Нескладний підрахунок показує, що в одній зоні одночасно можуть використовуватися тільки три канали. У таких умовах неможливо вирішити проблему відбудови від перешкод автоматичною зміною частоти, ось чому в бездротових локальних мережах використовується кодування з високою надмірністю. У ситуації, коли і цей захід не дозволяє забезпечити задану достовірність передачі, швидкість з максимального значення 11 Мбіт / с послідовно знижується до одного з наступних фіксованих значень: 5,5; 2; 1 Мбіт / с. Зниження швидкості відбувається не тільки при високому рівні перешкод, але і якщо відстань між елементами бездротової мережі досить велика.

    
**1.5.1.2. Канальний рівень IEEE 802.11**

Подібно провідної мережі Ethernet, в бездротових комп'ютерних мережах Wi-Fi канальний рівень включає в себе підрівні управління логічним з'єднанням (Logical Link Control, LLC) і управління доступом до середовища передачі (Media Access Control, MAC). У Ethernet і IEEE 802.11 один і той же LLC, що значно спрощує об'єднання дротяних і бездротових мереж. MAC у обох стандартів має багато спільного, проте є деякі тонкі відмінності, принципові для порівняння дротяних і бездротових мереж.   
 У Ethernet для забезпечення можливості множинного доступу до загального середовища передачі (в даному випадку кабелю) використовується протокол CSMA / CD, що забезпечує виявлення і обробку колізій (у термінології комп'ютерних мереж так називаються ситуації, коли декілька пристроїв намагаються почати передачу одночасно).   
 У мережах IEEE 802.11 використовується напівдуплексний режим передачі, тобто в кожен момент часу станція може або приймати, або передавати інформацію, тому виявити колізію в процесі передачі неможливо. Для IEEE 802.11 був розроблений модифікований варіант протоколу CSMA / CD, що отримав назву CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance). Працює він у такий спосіб. Станція, яка збирається передавати інформацію, спочатку "слухає ефір". Якщо не знайдено активності на робочій частоті, станція спочатку чекає протягом деякого випадкового проміжку часу, потім знову "слухає ефір" і, якщо середовище передачі даних все ще вільна, здійснює передачу. Наявність випадкової затримки необхідно для того, щоб мережа не зависла, якщо кілька станцій одночасно захочуть отримати доступ до частоти. Якщо інформаційний пакет приходить без спотворень, приймаюча станція посилає назад підтвердження. Цілісність пакета перевіряється методом контрольної суми. Отримавши підтвердження, станція передачі вважає процес передачі даного інформаційного пакету завершеним. Якщо підтвердження не отримано, станція вважає, що сталася колізія, і пакет передається знову через випадковий проміжок часу.   
 Ще одна специфічна для бездротових мереж проблема - дві клієнтські станції мають поганий зв'язок одна з одною, але при цьому якість зв'язку кожної з них з точкою доступу добра. У такому випадку передавальна клієнтська станція може надіслати на точку доступу запит на очищення ефіру. Тоді за командою з точки доступу інші клієнтські станції припиняють передачу на час "спілкування" двох точок з поганою зв'язком. Режим примусової очищення ефіру (протокол Request to Send / Clear to Send - RTS / CTS) реалізований далеко не у всіх моделях устаткування IEEE 802.11 і якщо він є, то включається лише в крайніх випадках.   
 У Ethernet при передачі потокових даних використовується управління доступом до каналу зв'язку, розподілене між всіма станціями. Навпаки, в IEEE 802.11 у таких випадках застосовується централізоване управління з точки доступу. Клієнтські станції послідовно опитуються на предмет передачі потокових даних. Якщо яка-небудь зі станцій повідомляє, що вона буде передавати потокові дані, точка доступу виділяє їй проміжок часу, в який з усіх станцій мережі буде передавати тільки вона.   
 Слід зазначити, що примусова очищення ефіру знижує ефективність роботи бездротової мережі, оскільки пов'язана з передачею додаткової службової інформації і короткочасними перервами зв'язку. Крім цього, в дротяних мережах Ethernet при необхідності можна реалізувати не тільки напівдуплексний, але і дуплексний варіант передачі, коли колізія виявляється в процесі передачі (це підвищує реальну пропускну здатність мережі). Тому, на жаль, за інших рівних умов реальна пропускна здатність бездротової мережі IEEE 802.11b буде нижче, ніж у проводового Ethernet. Таким чином, якщо мереж Ethernet 10 Мбіт / с і IEEE 802.11b (максимальна швидкість передачі інформації 11 Мбіт / с) з однаковим числом користувачів давати однакову навантаження, поступово збільшуючи її, то, починаючи з деякого порога, мережа IEEE 802.11b почне "гальмувати ", а Ethernet все ще буде функціонувати нормально.   
 Оскільки клієнтські станції можуть бути мобільними пристроями з автономним живленням, в стандарті IEEE 802.11 велика увага приділена питанням управління живленням. Зокрема, передбачено режим, коли клієнтська станція через певні проміжки часу "прокидається", щоб прийняти сигнал включення, який, можливо, передає точка доступу. Якщо цей сигнал прийнятий, клієнтське пристрій включається, в іншому випадку її знову "засинає" до наступного циклу прийому інформації.

Стандарт 802.11 передбачає використання двох методів передачі даних. Один з них отримав назву Direct Sequence Spread Spectrum (DSSS) - «метод прямої послідовності», а другий - Frequency Hopping Spread Spectrum (FHSS) - «метод частотних стрибків». Обидва ці методи використовують принцип широкосмугової передачі сигналу.

**1.5.2 ТЕХНОЛОГІЯ DSSS**

Під час потенційного кодуванні інформаційні біти - логічні нулі й одиниці передаються прямокутними імпульсами напруги. Прямокутний імпульс тривалості T має спектр, ширина якого обернено пропорційна тривалості імпульсу. Тому чим менша тривалість інформаційного біта, тим більший спектр займає такий сигнал.   
 Для навмисного розширення спектру спочатку у вузькосмуговий сигнал в кожен передаваний інформаційний біт (логічний 0 або 1) у буквальному сенсі вбудовується послідовність так званих чіпів. Якщо інформаційні біти - логічні нулі або одиниці за потенційного кодування інформації можна уявити у вигляді послідовності прямокутних імпульсів, то кожен окремий чіп - це теж прямокутний імпульс, але його тривалість у кілька разів менша тривалості інформаційного біта. Послідовність чіпів являє собою послідовність прямокутних імпульсів, тобто нулів та одиниць, проте ці нулі й одиниці не є інформаційними. Оскільки тривалість одного чіпа в n разів менше тривалості інформаційного біта, то й ширина спектру перетвореного сигналу буде в n-разів більше ширини спектру початкового сигналу. При цьому і амплітуда переданого сигналу зменшиться в n разів.   
 Чипові послідовності, що вбудовуються в інформаційні біти, називають шумоподібних кодами (PN-послідовності), що підкреслює та обставина, що результуючий сигнал стає шумоподібним і його важко відрізнити від природного шуму.   
 Як розширити спектр сигналу і зробити його невідмінним від природного шуму, зрозуміло. Для цього можна скористатися довільною (випадковою) чіповою послідовністю. Проте, виникає питання: а як такий сигнал приймати? Адже якщо він стає шумоподібним, то виділити з нього корисний інформаційний сигнал не просто, якщо взагалі можливо. Виявляється, можливо, але для цього потрібно відповідним чином підібрати чіпову послідовність. Використані для розширення спектру сигналу чипові послідовності повинні відповідати певним вимогам автокореляції. Під терміном автокореляції в математиці мають на увазі ступінь подібності функції самій собі в різні моменти часу. Якщо підібрати таку чіпову послідовність, для якої функція автокореляції буде мати різко виражений пік лише для одного моменту часу, то такий інформаційний сигнал можливо буде виділити на рівні шуму. Для цього у приймачі отриманий сигнал помножується на ту ж чіпову послідовність, тобто обчислюється автокореляційна функція сигналу. В результаті сигнал стає знову вузькосмуговим, тому його фільтрують у вузькій смузі частот і будь-яка перешкода, яка потрапляє в смугу вихідного широкосмугового сигналу, після множення на чіпову послідовність, навпаки, стає широкосмуговою і обрізується фільтрами, а у вузьку інформаційну смугу потрапляє лише частина перешкоди, по потужності значно менша, ніж перешкода, яка діє на вході приймача (рис. 1.1).

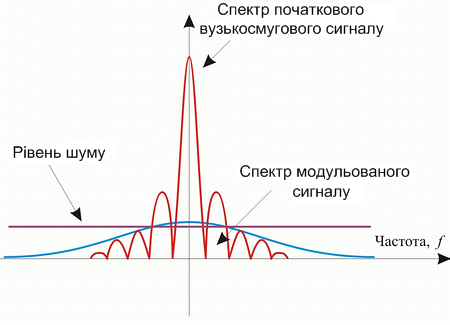


Рисунок 1.2 Використання технології розширення спектру дозволяє зраджувати дані на рівні природного шуму.

Метод DSSS використовує всю смугу одночасно, розбиваючи її на 11 однакових смуг. Сигнал передавача кодується таким чином, що кожен біт інформації, що передається перетвориться в послідовність з 11 біт. Після чого ця послідовність передається паралельно і одночасно з усіх 11 смугах. Приймач, що отримав цю послідовність, виробляє зворотне перетворення сигналу. Кожна пара «передавач-приймач» використовує свій алгоритм кодування, що виключає перехоплення сигналу іншим приймачем.   
 Перше перевага даного методу полягає в надійному захисту переданої інформації. Вірогідність збігу схем кодування двох різних пристроїв практично виключена. Розшифрувати ж такий сигнал, не знаючи алгоритму, неможливо.   
 Друге гідність полягає в тому, що завдяки одиннадцатикратной надмірності інформації для передачі сигналу можна використовувати малопотужну апаратуру. При цьому немає необхідності використовувати дорогі підсилювачі або змінювати конструкцію антен. Крім того, «розмазування» сигналу призводить до того, що ставлення сигналу до шуму стає близьким до одиниці. З точки зору вузькосмугової апаратури такий сигнал практично не відрізняється від шуму (звідси відбулося друга назва - «метод шумоподібних сигналу»). У свою чергу, вузькосмуговий апаратура не впливає на DSSS, оскільки часткова втрата інформації на одній або кількох смугах не псує сигнал з-за надмірності інформації, що передається. Це дозволяє одночасно використовувати в одному діапазоні вузькосмуговий і DSSS-апаратуру.

**1.5.3 ТЕХНОЛОГІЯ FHSS**

Метод частотних стрибків використовує смугу по-іншому. Весь діапазон, відведений для передачі, відповідно до стандарту 802.11 ділиться на 79 каналів. Передавач використовує в одиницю часу тільки один з цих каналів, перемикаючись між ними відповідно до закладеного в нього алгоритмом. Частота таких «стрибків» стандартом не визначена і варіюється в залежності від того, в якій країні використовується дане устаткування. У свою чергу, приймач синхронно здійснює такі ж «стрибки», використовуючи ту ж «випадкову» послідовність, що й передавач. Випадкова послідовність є унікальною для кожної пари «передавач-приймач».   
 На відміну від методу прямої послідовності метод FHSS має два істотні недоліки. Перший з них полягає в тому, що при достатньо великому числі одночасних сеансів роботи різко збільшується ймовірність колізії. Це обумовлено кінцевим числом каналів і вузькосмугового передається в одиницю часу сигналу. Два різні сигналу, зіткнувшись на одній частоті, заглушать один одного і ініціюють повторну передачу на наступному стрибку. Тому перешкодозахищеність реалізується за рахунок зменшення пропускної здатності. Другий недолік - створення перешкод для вузькосмугової апаратури, що в ряді випадків робить неможливим їх спільне використання. Ця обставина різко звужує коло можливих застосувань. Апаратура FHSS, як правило, використовується в закритих приміщеннях або на невеликій території (виняток становить випадок, коли необхідно організувати з'єднання «точка-точка»).

**1.6 АНАЛІЗ ІСНУЮЧИХ СТАНДАРТІВ ТЕХНОЛОГІЇ IEEE 802.11**

На сьогоднішній день існують наступні різновиди даного стандарту побудови бездротових локальних мереж IEEE 802.11 a / b / g. Стандарт IEEE 802.11, прийнятий в 1997 р., став першим стандартом даного сімейства. Він передбачає використання діапазону частот 2,4 ГГц, а також технології розширення спектру стрибкоподібною зміною частоти (Frequency Hopping Spread Spectrum або технології розширення спектру за методом прямої послідовності. [Direct Sequence Spread Spectrum DSSS. Стандарт IEEE 802.11 забезпечує пропускну спроможність до 2 Мбіт / с у розрахунку на одну точку доступу.

Таблиця 1.1 Характеристика стандартв IEEE 802.11

|  |  |  |  |
| --- | --- | --- | --- |
| Стандарт | 802.11b | 802.11g | 802.11a |
| Кількість використаних радіоканалів | 3  не перекриваються | 3  не перекриваються | 8  не перекриваються |
| Частотний діапазон | 2.4 ГГц | 2.4 ГГц | 5 ГГц |
| Макс. швидкість передачі даних | 11 Мб/с | 54 Мб/с | 54 Мб/с |
| Приблизна відстань дії | 30 м при 11 Мб/с  100 м при 1 Мб/с | 15 м при 54 Мб/с  50 м при 11 Мб/с | 12 м при 54 Мб/с  100 м при 6 Мб/с |

**1.6.1 СТАНДАРТ IEEE 802.11а**

Стандарт IEEE 802.11а передбачає використання нового, що не потребує ліцензування частотного діапазону 5 ГГц і модуляції за методом ортогонального мультиплексування з поділом частот (Orthogonal Frequency Domain Multiplexing - OFDM). Застосування цього стандарту дозволяє збільшити швидкість передачі в кожному каналі з 11 Мбіт / с до 54 Мбіт / с. При цьому одночасно може бути організовано до восьми непересічних каналів (або точок присутності), а не три, як у діапазоні 2,4 ГГц. Продукти стандарту IEEE 802.11а (мережеві адаптери NIC і точки доступу) не мають зворотної сумісності з продуктами стандартів 802.11b і 802.11g, так як вони працюють на різних частотах.

**1.6.2 СТАНДАРТ IEEE 802.11b**

Стандарт IEEE 802.11b був прийнятий в 1999 р. як розвиток прийнятого раніше стандарту IEEE 802.11. Він також передбачає використання діапазону частот 2,4 Ггц, але тільки з модуляцією DSSS. Даний стандарт забезпечує пропускну здатність до 11 Мбіт / с в розрахунку на одну точку доступу.   
 Продукти стандарту IEEE 802.11b, що поставляються різними виготівниками, тестуються на сумісність і сертифікуються організацією Wireless Ethernet Compatibility Alliance (WECA), яка в даний час більше відома під назвою Wi-Fi Alliance. Сумісні бездротові продукти, що пройшли випробування за програмою "Альянсу WH можуть бути маркіровані знаком Wi-Fi.   
 В даний час IEEE 802.11b це найпоширеніший стандарт, на базі якого побудована більшість бездротових локальних мереж.

**1.6.3 СТАНДАРТ IEEE 802.11g**

Проект стандарту IEEE 802.11g був затверджений у жовтні 2002 р. Цей стандарт передбачає використання діапазону частот 2,4 ГГц, забезпечуючи швидкість передачі 54 Мбіт / с і перевершуючи, таким чином, нині чинний стандарт 802.11b. Крім того, він гарантує зворотну сумісність зі стандартом 802.11b. Зворотна сумісність стандарту IEEE 802.11g може бути реалізована в режимі модуляції DSSS, і тоді швидкість передачі буде обмежена одинадцятьма мегабіта на секунду або в режимі модуляції OFDM, при якому швидкість складає 54 Мбіт / с. Таким чином, даний стандарт є найбільш прийнятним при побудові бездротових мереж.

**1.6.4 ФIЗИЧНИЙ РIВЕНЬ ПРОТОКОЛУ 802.11g**

Стандарт IEEE 802.11g є логічним розвитком стандарту 802.11b / b + і передбачає передачу даних в тому ж частотному діапазоні, але з більш високими швидкостями. Крім того, стандарт 802.11g повністю сумісний з 802.11b, тобто будь-який пристрій 802.11g повинна підтримувати роботу з пристроями 802.11b. Максимальна швидкість передачі в стандарті 802.11g становить 54 Мбіт / с.   
 При розробці стандарту 802.11g розглядалися кілька конкуруючих технологій: метод ортогонального частотного поділу OFDM і метод двійкового пакетного згортальної кодування PBCC.   
 У протоколі 802.11g передбачена передача на швидкостях 1, 2, 5,5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48 і 54 Мбіт / с. Деякі з даних швидкостей є обов'язковими, а деякі - опціональними. Крім того, одна і та ж швидкість може реалізовуватися при різній технології кодування. Ну і як вже зазначалося, протокол 802.11g включає в себе як підмножина протоколи 802.11b / b +.   
 Технологія кодування PBCC опціонально може використовуватися на швидкостях 5,5; 11; 22 і 33 Мбіт / с. Взагалі ж в самому стандарті обов'язковими є швидкості передачі 1; 2; 5,5; 6; 11; 12 і 24 Мбіт / с, а більш високі швидкості передачі (33, 36, 48 і 54 Мбіт / с) - опціональними.   
 Відзначимо, що для обов'язкових швидкостей в стандарті 802.11g використовується тільки кодування CCK і OFDM, а гібридне кодування та кодування PBCC є опціональним.   
 Для передачі на більш високих швидкостях використовується квадратурна амплітудна модуляція QAM (Quadrature Amplitude Modulation), при якій інформація кодується за рахунок зміни фази та амплітуди сигналу. У протоколі 802.11g використовується модуляція 16-QAM і 64-QAM. У першому випадку є 16 різних станів сигналу, що дозволяє закодувати 4 біта в одному символі. У другому випадку мається вже 64 можливих станів сигналу, що дозволяє закодувати послідовність 6 біт в одному символі. Модуляція 16-QAM застосовується на швидкостях 24 і 36 Мбіт / с, а модуляція 64-QAM - на швидкостях 48 і 54 Мбіт / с.

**1.7 МЕТОД ДОСТУПУ**

Для доступу до середовища використовується метод CSMA / CA (Carrier Sense Multiple Acsses Collision Avoidance) - множинний доступ з контролем несучої і запобіганням колізій. Перед початком передачі пристрій слухає ефір і чекає, коли канал звільниться. Канал вважається вільним за умови, що не виявлено активності протягом певного проміжку часу - міжкадрового інтервалу певного типу. Якщо протягом цього проміжку канал залишався вільним, пристрій очікує ще в плині випадкового проміжку часу і якщо ще канал не зайнятий починає передавати пакет.

**1.8 АЛГОРИТМ КОНФОДЕНЦІЙНОСТІ. ДРОТОВІ ЕКВІВАЛЕНТИ.**

**Безпека Wi-Fi мереж**

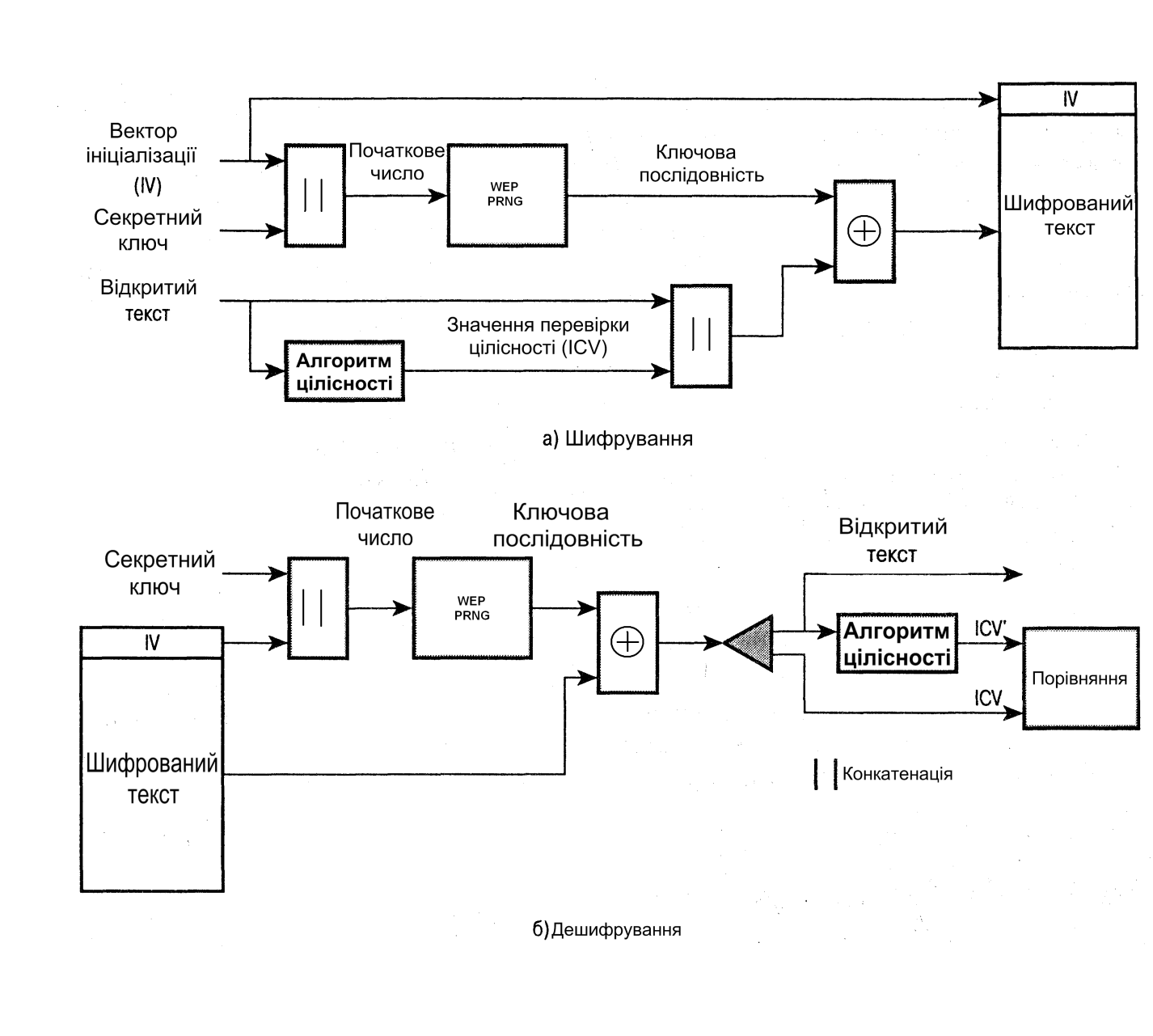
Як і будь-яка комп'ютерна мережа, Wi-Fi - є джерелом підвищеного ризику несанкціонованого доступу. Крім того, проникнути в бездротову мережу значно простіше, ніж у звичайну, - не потрібно підключатися до проводів, досить виявитися в зоні прийому сигналу.   
 Бездротові мережі відрізняються від кабельних тільки на перших двох - фізичному (Phy) і частково канальному (MAC) – рівнях семирівневої моделі взаємодії відкритих систем. Більш високі рівні реалізуються як в дротових мережах, а реальна безпека мереж забезпечується саме на цих рівнях. Тому різниця в безпеці тих і інших мереж зводиться до різниці в безпеці фізичного і MAC-рівнів. Хоча сьогодні в захисті Wi-Fi-мереж застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних і контролю цілісності їх передачі, тим не менш, вірогідність доступу до інформації сторонніх осіб є дуже істотною. І якщо настроювання мережі не приділити належної уваги зловмисник може:

- роздобути доступ до ресурсів та дискам користувачів Wi-Fi-мережі, а через неї і до ресурсів LAN;   
- підслуховувати трафік, вилучати з нього конфіденційну інформацію;   
- спотворювати проходи в інформаційній мережі;   
- скористатися інтернет-трафіком;   
- атакувати ПК користувачів і сервери мережі   
- впроваджувати підроблені точки доступу;   
- розсилати спам, і здійснювати інші протиправні дії від імені вашої мережі.

Для захисту мереж 802.11 передбачено комплекс заходів безпеки передачі даних.  На ранньому етапі використання Wi-Fi мереж таким був пароль SSID (Server Set ID) для доступу в локальну мережу, але згодом виявилося, що дана технологія не може забезпечити надійний захист.   
 Головним захистом довгий час було використання цифрових ключів шифрування потоків даних за допомогою функції Wired Equivalent Privacy (WEP). Самі ключі представляють із себе звичайні паролі з довжиною від 5 до 13 символів ASCII. Дані шифруються ключем з розрядністю від 40 до 104 біт. Але це не цілий ключ, а тільки його статична складова. Для посилення захисту застосовується так званий вектор ініціалізації Initialization Vector (IV), який призначений для рандомізації додаткової частини ключа, що забезпечує різні варіації шифру для різних пакетів даних. Даний вектор є 24-бітним. Таким чином, в результаті ми отримуємо загальне шифрування з розрядністю від 64 (40 +24) до 128 (104 +24) біт, в результаті при шифруванні ми оперуємо і постійними, і випадково підібраними символами.   
 Але, як виявилося, зламати такий захист можна відповідні утиліти присутні в Інтернеті (наприклад, AirSnort, WEPcrack). Основне її слабке місце - це вектор ініціалізації. Оскільки ми говоримо про 24 бітах, це має на увазі близько 16 мільйонів комбінацій, після використання цієї кількості, ключ починає повторюватися. Хакеру необхідно знайти ці повтори (від 15 хвилин до години для ключа 40 біт) і за секунди зламати решту ключа. Після цього він може входити в мережу як звичайний зареєстрований користувач.   
 Як показав час, WEP теж виявилася не самою надійною технологією захисту. Після 2001 року для дротових і бездротових мереж був впроваджений новий стандарт IEEE 802.1X, який використовує варіант динамічних 128-розрядних ключів шифрування, тобто періодично змінюються в часі. Таким чином, користувачі мережі працюють сеансами, по завершенні яких їм надсилається новий ключ. Наприклад, Windows XP підтримує даний стандарт, і за замовчуванням час одного сеансу рівне 30 хвилинах. IEEE 802.1X - це новий стандарт, який виявився ключовим для розвитку індустрії бездротових мереж в цілому. За основу взято виправлення недоліків технологій безпеки, що застосовуються в 802.11, зокрема, можливість злому WEP, залежність від технологій виробника і т. п. 802.1X дозволяє підключати в мережу навіть PDA-пристрої, що дозволяє більш вигідно використовувати саму ідею бездротового зв'язку. З іншого боку, 802.1X і 802.11 є сумісними стандартами. У 802.1X застосовується той же алгоритм, що і в WEP, а саме - RC4, але з деякими відмінностями. 802.1X базується на протоколі розширеної аутентифікації (EAP), протоколі захисту транспортного рівня (TLS) і сервер доступу Remote Access Dial-in User Server. Протокол захисту транспортного рівня TLS забезпечує взаємну аутентифікацію та цілісність передачі даних. Всі ключі є 128-розрядними за замовчуванням.   
 Наприкінці 2003 року було запроваджено стандарт Wi-Fi Protected Access (WPA), який поєднує переваги динамічного оновлення ключів IEEE 802.1X з кодуванням протоколу інтеграції тимчасового ключа TKIP, протоколом розширеної аутентифікації (EAP) і технологією перевірки цілісності повідомлень MIC. WPA - це тимчасовий стандарт, про який домовилися виробники обладнання, поки не набув чинності IEEE 802.11i. По суті, WPA = 802.1X + EAP + TKIP + MIC, де:

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

Стандарт TKIP використовує автоматично підібрані 128-бітові ключі, які створюються непередбачуваним способом і загальне число варіацій яких досягає 500 мільярдів. Складна ієрархічна система алгоритму підбору ключів та динамічна їх заміна через кожні 10 Кбайт (10 тис. переданих пакетів) роблять систему максимально захищеною.   
 Від зовнішнього проникнення і зміни інформації також обороняє технологія перевірки цілісності повідомлень (Message Integrity Check). Досить складний математичний алгоритм дозволяє звіряти відправлені в одній точці і отримані в іншій дані. Якщо помічені зміни і результат порівняння не сходиться, такі дані вважаються помилковими і викидаються.   
 Правда, TKIP зараз не є кращим в реалізації шифрування, оскільки в силу вступають нові алгоритми, засновані на технології Advanced Encryption Standard (AES), яка, вже давно використовується у VPN. Що стосується WPA, підтримка AES вже реалізована в Windows XP, поки тільки опціонально.   
 Крім цього, паралельно розвивається безліч самостійних стандартів безпеки від різних розробників, зокрема, в даному напрямку процвітають Intel і Cisco. У 2004 році з'являється WPA2, або 802.11i, який, в даний час є максимально захищеним.   
 Таким чином, на сьогоднішній день у звичайних користувачів та адміністраторів мереж є всі необхідні засоби для надійного захисту Wi-Fi, і за відсутності явних помилок (людський фактор) завжди можна забезпечити рівень безпеки, відповідний цінності інформації, що знаходиться в такій мережі. Сьогодні бездротову мережу вважають захищеною, якщо в ній функціонують три основні складові системи безпеки: аутентифікація користувача, конфіденційність і цілісність передачі даних.У бездротової локальної мережі питання прослуховування має особливу важливість. Для забезпечення сучасного рівня безпеки стандарт IEEE 802.11 включає схему WEP. Для забезпечення конфіденційності (а також цілісності даних) використовується алгоритм, заснований на алгоритмі шифрування RC4. Алгоритм забезпечення цілісності - це проста 32-бітова послідовність циклічної перевірки парності з надмірністю (CRC), що приєднується до кінця кадру MAC (рис. 1.2 а). Для процесу шифрування 40-бітовий секретний ключ ділиться між двома сполученими сторонами. До секретного ключа приєднується вектор ініціалізації (IV). Одержаний блок - це початкове число генератора псевдовипадкової послідовності (PRNG), визначеного в RC4. Генератор створює послідовність бітів, довжина якої дорівнює довжині кадру MAC плюс CRC. Після побітового застосування операції виключного АБО до кадру MAC і псевдовипадкової послідовн істі отримується незашифрований текст. До даного тексту приєднується вектор ініціалізації, і результат передається. Вектор ініціалізації періодично змінюється (при кожній новій передачі), отже, змінюється і псевдовипадкових послідовностей, що ускладнює завдання розшифровки перехопленого тексту.

  
                                         Рис.1.8.1 Алгоритм шифрування

Після отримання повідомлення рис. 1.8.1б приймач витягує вектор ініціалізації і приєднує його до спільно використовуваного секретного ключа, після чого генерує ті ж псевдовипадкові послідовності, що і джерело. Таким чином проходить позбавлення від ключа і вступ даних для побітового застосування операції, що виключає АБО, результатом чого є вихідний текст.   
 Таким чином, якщо взяти вихідний текст, застосувати до нього і ключовий послідовності операцію виключає АБО, а потім застосувати операцію виключає АБО до результату і тієї ж ключовою послідовності, то в результаті вийде вихідний текст.   
   
 На закінчення приймач порівнює поступаючу послідовність CRC, обчислену за відновленими даними: якщо величини співпадають, дані вважаються непошкодженими.

**Аутентифікація**

Стандарт IEEE 802.11 пропонує два типи аутентифікації: "відкрита система" і "загальний ключ".   
 Аутентифікація відкритих систем просто дозволяє двом сторонам домовитися про передачу даних без розгляду питань безпеки. У цьому випадку одна станція передає іншій керуючий кадр MAC, іменований кадром аутентифікації. У даному кадрі вказується, що має місце аутентифікація відкритих систем. Інша сторона відповідає власним кадрам аутентифікації та процес завершено. Таким чином, при аутентіфікації відкритих систем сторони просто обмінюються інформацією про себе.   
  
 Аутентифікація з загальним ключем вимагає, щоб дві сторони спільно володіли секретним ключем, не доступним третій стороні. Процедура аутентифікації між двома сторонами, А і В, виглядає наступним чином:

.   
1. А посилає кадр аутентифікації, у якому зазначений тип "загальний ключ" та ідентифікатор станції, що визначає станцію-відправника.   
2. У відповідає кадром аутентифікації, який включає 128-октетний текст запиту. Текст запиту створюється з використанням генератора випадкових чисел WEP. Ключ і вектор ініціалізації, використовувані при генерації тексту запиту, не важливі, оскільки далі в процедурі вони не використовуються.   
3. А переда кадр аутентифікації, який включає отриманий від В текст запиту. Кадр шифрується з використанням схеми WEP.

**1.2.1 Визначення дальності зв'язку бездротових пристроїв.**

Якщо посилення надмірне для необхідної дальності, його можна зменшити до необхідного значення, вибравши більш дешеві антени з меншим підсиленням.   
 Якщо підсилення тракту недостатньо для забезпечення необхідної дальності, необхідно збільшити його, вибираючи антени з більшим підсиленням; зменшуючи довжину і, відповідно, загасання коаксіальних кабелів. Якщо цього виявляється недостатньо, необхідним є використання додаткових підсилювачів. Для ефективного зв'язку за допомогою високочастотних хвиль потрібно забезпечити безперешкодну лінію прямої видимості між передавачем і приймачем. Виникає питання: скільки ж простору навколо прямого тракту між передавачем і приймачем має бути вільна від перешкод ? При відповіді на нього зручно використовувати таке поняття, як зони Френеля. Поняття зон Френеля засноване на принципі Гюйгенса, згідно з яким кожна точка середовища, до якої доходить обурення, сама стає джерелом вторинних хвиль, і поле випромінювання може розглядатися як суперпозиція всіх вторинних хвиль. На основі цього принципу можна показати, що об'єкти лежать всередині концентричних кіл, проведених навколо лінії прямої видимості двох трансіверов, можуть впливати на якість як позитивно, так і негативно. Всі перешкоди, що потрапляють всередину першої кола, першої зони Френеля, надають найбільш негативний вплив. Розглянемо точку, що знаходиться на прямому тракті (Рисунок 1.2.1.1) між передавачем і приймачем, причому відстань від точки до передавача одно S, а відстань від точки до приймача одно D, тобто відстань між передавачем і приймачем одно S + D.

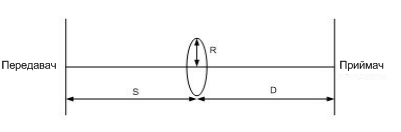


Рисунок 1.2.1.1 Зона Френеля

Відстань між двома трансивером дорівнює 10 км, а частота несучої - 2,4 ГГц. Тоді радіус першої зони Френеля в точці, розташованій посередині між трансивером, дорівнює 17,66 м. Якщо всередині кола, радіус якої становить приблизно 0,6 радіуса першої зони Френеля, проведеної навколо будь-якої точки між двома трансивером, немає ніяких перешкод, то загасанням сигналу, обумовленим наявністю перешкод, можна знехтувати. Однією з таких перепон є земля. Отже, висота двох антен повинна бути такою, щоб вздовж тракту не було ні однієї точки, відстань від якої до землі було б менше, ніж 0,6 першої зони Френеля.

При придбанні обладнання Wi-Fi (карт, точок доступу, антенн і т. і.) і розгортанн і за його допомогою мереж і покриття як правило виникають питання про зону дії WiFi пристроїв, необхідної комплектації WiFi мереж, ризики їх використання. Тому від того наскільки точно буде визначена можливість використання WiFi обладнання та його комплектність на етапі придбання, в кінцевому рахунку, залежить успішність проекту щодо використання Wi-Fi мереж.

Технічні ризики при використання Wi-Fi мереж можна умовно розділити на:

- Ризики пов'язані, з організацією радіочастотного тракту;

- Ризики, пов'язані з незадовільною роботою додатків у WLAN мережі.

- Взаємні перешкоди.

Згідно специфікації 802.11a мінімальна допустима чутливість будь-якої радіостанції WiFi працює на даному стандарті не повинна перевищувати -65 dBm, (для прикладу WiFi бездротовий адаптер PCI модель HW-2454 має чутливість-70dBm), придушення перехресних перешкод 15 дБ (alternate adjacent channel rejection) і -1 дБ придушення перешкод від сусіднього каналу працює на тій же частоті, при швидкості передачі даних 54 Мбіт/сек. Можна зауважити, що обладнання Wi-Fi проектується таким чином, щоб його спектральна маска відповідала відповідним вимогам за рівнем перехресних перешкод.  
 При розгляді джерел перешкод для приладів, що працюють у діапазоні 2,4 ГГц, необхідно враховувати пристрої Bluetooth, інші WiFi пристрої, що працюють на тих самих каналах.  
 У таблиці 1.2.1.1 представлені значення ефективної ізотропно випромінюваної потужності (EIRP) різних класів пристроїв Bluetooth, які можуть враховуватися при розрахунку радіочастотного тракту Wi-Fi.

На даній частоті перешкоди створюються також мікрохвильовими печами і деякими типами радіотелефонів.

|  |  |  |
| --- | --- | --- |
| № | Клас передавача | EIRP (dBm) |
| 1 | Клас 1 | 20 dBm |
| 2 | Клас 2 | 4dBm |
| 3 | Клас 3 | 0 dBm |

Таблиця 1.2.1.1 Значення ефективної ізотропно випромінюваної потужності (EIRP) різних класів

4. Ризики, пов'язані з використанням фірмових стандартів WiFi.  
На момент написання статті ряд компаній просували пристрої WiFi зі швидкістю передачі 108 Mb / s (Super G) в WiFi дана швидкість передачі досягається за рахунок використання одночасно декількох каналів, так як дана швидкість передачі не стандартизовані, то два пристрої будуть мати можливість працювати на даній швидкості у випадку якщо вони побудовані на базі одного і того-ж чіпа. Крім того на момент написання статті швидкість 108 Mb / s могла бути отримана тільки у режимі інфраструктура, а не в режимі точка-точка, що характерно для організації Wi-Fi мостів.

**2.2.Розрахунок зони покриття Wi**-**Fi мережі.**

Фірма-виробник WiFi обладнання, як правило, вказує зону стійкої роботи Wi-Fi радіостанції. Для обладнання Wi-Fi при потужності передавача 16-18 dBm зона стійкої роботи становить 200 м (HW-2454), виходячи з цього та враховуючи те, що потужність сигналу зменшується пропорційно квадрату відстані, можна розрахувати необхідну додаткову потужність сигналу для передачі на будь-яку відстань.

ΔP = 20 (Log10L - 2,3) (2.2.1)  
де:  
ΔP - додаткова потужність [dBm] необхідна системі;  
L - відстань [м]

Необхідну додаткову потужність ΔP можна отримати, використовуючи антенну техніку. Так як маркування продаваних антен проводиться як правило в dBi (коефіцієнт підсилення по відношенню до ізотропної антени), то його необхідно перевести в dBd (коефіцієнт підсилення по відношенню до дипольної антени)  
dBd = dBi - 2,2 (2.2.2)  
 Вцілому при використання антен на коефіцієнт посилення системи будуть впливати:

- Втрати у фідері;

- Коефіцієнт підсилення антени передавача;

- Коефіцієнт підсилення антени приймача;

Втрати у фідері (кабельних збірках) можна розрахувати, виходячи з таких характеристик:

- Втрати в піктейлах - 2 dBm / m;

- Втрати в кабелі RJ-8U - 0,3 dBm / m;

- Втрати в коннекторi - 1-2 dBm / m;

Активне обладнання WiFi стандартизується трьома основними органами стандартизації Wi-Fi Alliance, IEEE, ETSI.  
 Згідно Code of Federal Regulation 47 (USA), неліцензійне використання Wi-Fi допускається при рівнях потужності менших ніж дозволені для первинного користувача (є ліцензія). Це було впроваджено, враховуючи, що на даній частоті працює низка медичних приладів і введення Wi-Fi мережі не повинне призводити до збоїв.  
 Радіостанції стандарту Wi-Fi 802.11 мають потужність передавача від 30 - 100 мВт, тому можуть бути використані без ліцензії.  
Крім того, CFR обумовлює і самі рівні потужності передачі. Допустима пікова потужність 1 Вт (30 dBm) з антеною має коефіцієнт посилення 6 dBi. Іншими словами, якщо радіостанція не бере участь у формування мосту, то її EIRP (еквівалентна ізотропно випромінювана потужність) не повинна перевищувати 36 dBi.  
 Для мостів діє правило, згідно якому потужність передавача має знижуватися на 1 дБ при кожному збільшення підсилення антени на 3 dB понад рівня 6 dBi.  
 Використовуючи перерахованi данi, можна оцінити максимально допустимий радіус охоплення точки доступу для випадку, коли вона не працює як міст:

Lmax ~ 1230 м. (2.2.3)

На радіус дії Wi-Fi зв'язку також мають істотний вплив предмети, що знаходяться в зоні дії Wi-Fi передачі.  
 Дані предмети можуть відображати мікрохвилі і приводити до багатопроменевого завмирання або поглинати їх (тканини, папір).  
 Всі вище наведені формули використовують модель втрат на трасі для вільного простору (мається на увазі дотримання умов по першій зоні Френеля). Нижче наведена таблиця показує необхідний простір зони Френеля для організації надійного зв'язку Wi-Fi антен.

|  |  |  |
| --- | --- | --- |
| Дистанція між антенами (м) | Необхідний радіус першої зоны Френеля на частоті 2,4Ghz (м) | Необхідний радіус першої зоны Френеля на частоті 5Ghz (м) |
| 300 | 3,06 | 2,12 |
| 1600 | 7 | 4,9 |
| 8000 | 15,81 | 10,95 |
| 10000 | 17,68 | 12,25 |
| 15000 | 21,65 | 15 |

Таблиця 2.2.1

У випадку якщо ви організуєте зв'язок в умовах великої кількості відображаючих об'єктів, доцільно використовувати модель втрат на трасі, пропорційних четвертому ступеню радіусу дії.  
 Тоді для найгіршого випадку формула 1 приймає вигляд:

ΔP = 40 (Log10L - 1,14) (2.2.4)

**3. Ризики, пов'язані з незадовільною роботою додатків в WLAN мережі.**

При розрахунку можливості використання додатків при роботі в Wi-Fi мережах необхідно враховувати розрахункову продуктивність у перерахунку на одного клієнта. При швидкості передачі даних 54 Мб / сек, реальна продуктивність складає 22 Мб / с. Досвід використання Wi-Fi мереж показує, що для пульсуючих додатків (WEB, додатку клієнт / сервер) межею вважається 25 користувачів на одну точку доступу. Досвід експлуатації показує що на сьогоднішній момент використання Wi-Fi мереж для використання 1С бухгалтерії можливо тільки при використанні термінального сервера. При проектування бездротових мереж. як правило, використовують дві стратегії, в залежності від призначення мережі:

- мережа орієнтована на максимальну зону покриття;  
- мережа орієнтована на необхідну пропускну здатність;

Дані варіанти розгортання мереж обумовлені залежністю швидкості передачі даних від відстані до точки доступу.

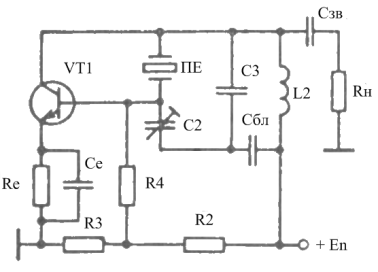
**2.3 Розрахунок автогенератора.**

Складовою частиною будь-якої точки доступу технології Wi-Fi як радіоприймального-радіопередавального пристрою є автогенератор. Від стабільності генеруємої ним частоти залежить стабільність частотних параметрів використовуваного обладнання, тобто працездатність організованого радіоканалу. Тому у цій частині приведено розрахунок кварцевого генератора, який задовольняє передявленi до автогенератора характеристики.

Розраховуємо гармоніковий автогенератор з кварцем між колектором і базою: потужність у навантаженні:

= 0,1 мВт; = 60 МГц.

Вибираємо просту одноконтурну схему гармонікового кварцевого генератора з резонатором між колектором і базою і кварцевий резонатор з параметрами

на третій гармоніці: 

= 50 Ом;  = 5 пФ; =ω1 /=

Допустима потужність розсіювання на резонаторі:

= 2 мВт.

Вибираємо:

де -потужність, розсіювана на кварцевому резонаторі .

Знаходимо:

=2

=2=1), а

та -частота послідовного резонансу і динамічні реактивні опори кварцового резонатора на n-ій гармоніці.

Потужність розсіювання на резонаторі:

=1 мВт.

Оскільки < розрахунок можна продовжувати. Вибираємо транзистор ГТ311. Його параметри:=65МГц; допустимий струм коллектора:

= 50мА; = 150мВт; = 12В; = 0.3В;

обираємо:

=5В,

та амплітуду імпульсів струму колектора:

= 10 мА

Визначаємо , де S - локальна крутизна апроксимованої статичної характеристики транзистора при =0.5.

Отримаємо S = 0.127 А/В. Виберемо =60. При цьому . Нормована по частота коливань:

.

Враховуючи співвідношення

{-

Отримаємо:

·0.2 і

·(1+-

-2}=20.7пФ.

Опори:

=1/

Індуктивність і ємність визначаємо з умови:

1+,

де n та (n2) - номери вибраної для збудження і найближчої нижчої непарної гармоніки. Приймаємо:

з виразу:

знаходимо:

.

При відомій визначаємо:

мкГн.

Відносна різниця між частотами

}=

=1.54/(2.

Для точного налаштування кварцевого генератора необхідно одну з ємностей виконати напівзмінною (±30%).

Режим роботи транзистора

амплітуда напруги на базі, В,

амплітуда напруги на колекторі, В,

, де

=0.998, =2/(0.0039

Потужності, підведена до колекторного кола і розсіювана на колекторі:

Постійна складова струму бази:

= 0.044 мА.

Зміщення на базі:

[=

=0.24 В.

Приймаємо:

Ом = 300 Ом

Опір визначаємо зі співвідношення:

Ом.

Візьмемо = 500 Ом. Напруга джерела живлення

В.

Напруга в точці з`єднання позначимо :

В.

Приймаючи струм через дільник:

мА,

знаходимо:

кОм;

кОм.

**4. АНАЛІЗ ЕКОНОМІЧНИХ ВИТРАТ**.

Загальновідомим є той факт, що при побудові дротових мереж витрати на розгортання систем у більшості випадків становлять трохи менш половини вартості обладнання, а то й більше. У разі побудови системи бездротового широкосмугового радіодоступу як фінансові так і тимчасові витрати на розгортання істотно знижуються за рахунок швидкості розгортання самої системи, установка компонентів якої займає в середньому кілька годин. Крім того існує можливість «переїзду» терміналів на інше місце. Можна об'єктивно стверджувати, що при рівному наданні сервісу конкретна технологія ефективна тоді, коли рентабельність розгортання мережі на її основі виявляється вище рентабельності конкуруючої технології. За цим критерієм технологія ВОЛЗ (яка, як відомо, дорожче радіотехнології) хороша там, де існує високошвидкісний комерційний трафік з раз і назавжди відомими точками прив'язки. Такою властивістю, як відомо, володіють комерційні магістральні мережі. Середня вартість прокладки ВОЛЗ в Україні ~ 3500 у.о. на км. По Києву цей показник досягає 10000 у.о. на км. Практично у всіх випадках дистанцій середньої довжини (тобто від 3 до 15 км) більш ефективної виявляється радіотехнологія, якщо тільки їй не протистоять особливі технічні вимоги замовника. Орієнтовні вартості робіт і устаткування, а також час, необхідний для розгортання різних мереж наведені в таблиці 4.1:

|  |  |  |
| --- | --- | --- |
| **Тип каналу** | **Час на підготовку і проведення монтажу** | **Час на підготовку і проведення монтажу** |
| Мідний кабель | 300-500 у.о. по існуючій каналізації, інакше 2-8 тис. у.о. за 1 км | Підготовка робіт і прокладка: до 1 місяця (без каналізації); встановлення HDSL-модемів: кілька годин |
| Волоконно-оптичний ка­бель | Волоконно-оптичний кабель 500-1000 у.о. по по існуючій каналізації, інакше 5-10 тис. у.о. за 1 км | Підготовка робіт і прокладка: 2-4 місяці (без каналізації) |
| Оптичний канал | Оптичний канал 2-4 тис. у.о. за комплект | Підготовка монтажу: 2-3 дні; встановлення: 2-3 години |
| Лазерний ка­нал | Лазерний канал 12-22 тис. у.о. за комплект | Підготовка робіт: 1-2 тижні; встановлення: кілька годин |

Таблиця 4.1 Показники по розгортанню різних типів мереж

Для доступу до середовища передачі даних в бездротових мережах застосовується метод колективного доступу з виявленням несучої і уникненням колізій (Carrier Sense Multiple Access / Collision Avoidance, CSMA / CA). Власне, цей метод навіть за своєю назвою нагадує технологію колективного доступу, реалізовану в мережах Ethernet, де використовується метод колективного доступу з Упізнання несучої і виявленням колізій (Сarrier-Sense-Multiply-Access With Collision Detection, CSMA / CD). Єдина відмінність полягає в другій частині методу - замість виявлення колізій використовується технологія уникнення колізії. Перед тим як послати дані в "ефір", станція спочатку відправляє спеціальне повідомлення, зване RTS (Ready To Send), яке трактується як готовність цього вузла до відправки даних. Таке RTS-повідомлення містить інформацію про тривалість майбутньої передачі і про адресата і доступно усіх вузлів в мережі. Це дозволяє іншим вузлам затримати передачу на час, рівне оголошеній тривалості повідомлення. Приймальна станція, отримавши сигнал RTS, відповідає посилкою сигналу CTS (Clear To Send), що свідчить про готовність станції до прийому інформації. Після цього передавальна станція посилає пакет даних, а прийомна станція повинна передати кадр ACK, що підтверджує безпомилковий прийом. Якщо АСК не отримано, спроба передачі пакету даних буде повторена. Таким чином, з використанням подібного четирехетапного протоколу передачі даних реалізується регламентування колективного доступу з мінімізацією вірогідності виникнення коллізій. При розгортанні бездротових мереж і систем НВЧ діапазону потрібен розрахунок радіоліній. Подібний розрахунок є традиційною радіорелейного завданням, для вирішення якої потрібне знання великої кількості вихідних даних і професійні знання і навички. У той же час завдання, пов'язані з попередньою оцінкою реалізованості радіолінії, оцінкою складу обладнання та можливостей підключення нових абонентів до існуючої базової станції, не потребують повного розрахунку. Використовувана спрощена методика дозволяє вирішити ці завдання.

**3. ТЕХНІКА БЕЗПЕКИ І ОХОРОНА ПРАЦІ**

**3.1 Охорона праці користувачів персональних комп'ютерів (ПК)**

Широке промислове та побутове використання ПК актуалізувало питання охорони праці їхніх користувачів. Найбільш повним нормативним документом щодо забезпечення охорони праці користувачів ПК є "Державні санітарні норми і правила роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин" ДСанПіН 3.3.2.007-98.

Дотримання вимог цих правил може значно знизити наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відеодисплейними матеріалами, зокрема можливість зорових, нервово-емоційних переживань, серцево-судинних захворювань. Виходячи з цього, роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації ВДТ, робочого середовища, робочих місць з ВДТ, режиму праці і відпочинку при роботі з ВДТ тощо, які викладені у Правилах.

Відповідно до встановлених гігієнічно-санітарних вимог (ГОСТ 12.1.005-88, СН 4088-86) роботодавець зобов'язаний забезпечити в приміщеннях з ВДТ оптимальні параметри виробничого середовища (табл. 3.1).

Таблиця 3.1.1 Норми мікроклімату для приміщень з ВТД

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пора року | Категорія робіт | Температура повітря, С, не більше | Відносна вологість повітря, % | Швидкість  руху повітря, м/с |
| Холодна | Легка - 1 а | 22...24 | 4...6 | 0,1 |
| Легка - 1 б | 21...23 | 4...6 | 0,1 |
| Тепла | Легка - 1 а | 23...25 | 4...6 | 0,1 |
| Легка - 1 б | 22...24 | 4...6 | 0,2 |

Природне освітлення в приміщеннях з ВДТ має здійснюватися через вікна, орієнтовані переважно на північ або північний схід і забезпечувати коефіцієнт природної освітленості не нижче ніж 1,5 %. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски з поверхні екранів ПК і клавіатури повинні бути передбачені сонцезахисні пристрої, вікна повинні мати жалюзі або штори.

Основні вимоги до виробничого приміщення для експлуатації ВДТ

* воно не може бути розміщено у підвалах та цокольних поверхах;
* площа на одне робоче місце в такому приміщенні повинна становити не менше 6,0м2, а об'єм не менше 20,0 м3;
* воно повинно мати природне та штучне освітлення відповідно до СНіПП-4-79;
* в ньому мають бути шафи для зберігання документів, магнітних дисків, полиці, стелажі, тумби тощо, з урахуванням вимог до площі приміщення;
* щоденно проводити вологе прибирання;
* поруч з приміщенням для роботи з ВДТ мають бути обладнані:

• побутова кімната для відпочинку під час роботи;

• кімната психологічного розвантаження.

Таблиця 3.1.2. Рівні іонізації повітря приміщень при роботі на ВДТ

|  |  |  |
| --- | --- | --- |
| Рівні | Число іонів в 1 см3 повітря | |
| *п*+ | *п*- |
| Мінімально необхідні | 400 | 600 |
| Оптимальні | 1500-30000 | 3000-5000 |
| Максимально допустимі | 50000 | 50000 |

Штучне освітлення в приміщеннях з робочим місцем, обладнаним ВДТ, має здійснюватись системою загального рівномірного освітлення. Як джерело штучного освітлення мають застосовуватись люмінесцентні лампи ЛБ.

Вимоги до освітлення приміщень та робочих місць під час роботи з ВДТ:

- освітленість на робочому місці повинна відповідати характеру зорової роботи, який визначається трьома параметрами: об'єктом розрізнення - найменшим розміром об'єкта, що розглядається на моніторі ПК; фоном, який характеризується коефіцієнтом відбиття; контрастом об'єкта і фону;

- необхідно забезпечити достатньо рівномірне розподілення яскравості на робочій поверхні монітора, а також в межах навколишнього простору;

- на робочій поверхні повинні бути відсутні різкі тіні;

- в полі зору не повинно бути відблисків (підвищеної яскравості поверхонь, які світяться та викликають осліплення);

- величина освітленості повинна бути постійною під час роботи;

- слід обирати оптимальну спрямованість світлового потоку і необхідний склад світла.

*УВАГА! Застосування світильників без розсіювачів та екрануючих гратів заборонено.*

Щодо допустимих рівнів звуку та електромагнітних випромінювань і електричного поля в приміщеннях під час роботи з ВДТ, то вони вказані в табл. 3.11.

Гігієнічні норми до організації і обладнання робочих місць з ВДТ. При розташуванні елементів робочого місця користувача ВДТ слід враховувати:

* робочу позу користувача;
* простір для розміщення користувача;
* можливість огляду елементів робочого місця;
* можливість ведення захистів;
* розміщення документації і матеріалів, які використовуються користувачем.

Таблиця 3.1.3.Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вид трудової діяльності | Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц | | | | | | | | | |
| 31,5 | 63 | 125 | 250 | 500 | 1000 | 2000 | 4000 | 8000 | Рівні звуку,  еквівалентні рівні звуку,  дБА/дБАекв. |
| Програмісти ЕОМ | 86 | 7 | 61 | 54 | 49 | 45 | 42 | 40 | 38 | 50 |
| Оператори в залах обробки інформації на ЕОМ та оператори комп'ютерного набору | 96 | 83 | 74 | 68 | 63 | 60 | 57 | 55 | 54 | 65 |
| В приміщеннях для розташування шумних агрегатів ЕОМ | 103 | 91 | 83 | 77 | 73 | 70 | 68 | 66 | 64 | 75 |

Конструкція робочого місця користувача ВДТ має забезпечити підтримання оптимальної робочої пози. Робочі місця з ВДТ слід так розташувати відносно вікон, щоб природне світло падало збоку, переважно зліва.

Робочі місця з ВДТ повинні бути розташовані від стіни з вікнами на відстані не менше 1,5м, від інших стін — на відстані 1 м, відстань між собою - не менше ніж 1,5 м.

Для забезпечення точного та швидкого зчитування інформації в зоні найкращого бачення площина екрана монітора повинна бути перпендикулярною нормальній лінії зору. При цьому повинна бути передбачена можливість переміщення монітора навколо вертикальної осі в межах ±30° (справа наліво) та нахилу вперед до 85° і назад до 105° з фіксацією в цьому положенні.

Клавіатура повинна бути розташована так, щоб на ній було зручно працювати двома руками. Клавіатуру слід розміщати на поверхні столу на відстані 100...300 мм від краю. Кут нахилу клавіатури до столу повинен бути в межах від 5 до 15°, зап'ястя на долонях рук повинні розташовуватись горизонтально до площини столу (рис. 3.1.1).

Принтер повинен бути розміщений у зручному для користувача положенні, так, що максимальна відстань від користувача до клавіш управління принтером не перевищувала довжину витягнутої руки користувача.

Конструкція робочого стола повинна забезпечувати можливість оптимального розміщення на робочій поверхні обладнання, що використовується, з врахуванням його кількості та конструктивних особливостей (розмір монітора, клавіатури, принтера, ПК та ін.) і документів, а також враховувати характер роботи, що виконується.

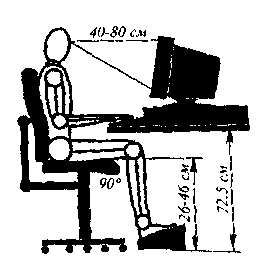


Рисунок 3.1.1 Конструкція робочого місця користувача ВДТ

Вимоги до режимів праці і відпочинку при роботі з ВДТ. Під час роботи з ВДТ для збереження здоров'я працівників, запобігання профзахворюванням і підтримки працездатності встановлюються внутрішньо змінні регламентовані перерви для відпочинку.

Тривалість регламентованих перерв під час роботи з ЕОМ за 8-годинної денної робочої зміни залежно від характеру праці: 15 хвилин через кожну годину роботи - для розробників програм зі застосуванням ЕОМ; 15 хвилин через кожні дві години - операторів із застосуванням ЕОМ; 10 хвилин після кожної години роботи за ВДТ для операторів комп'ютерного набору.

УВАГА! У випадках, коли виробничі обставини не дозволяють стосовувати регламентовані перерви, тривалість безперервної роботи з ВДТ не повинна перевищувати 4 годин.

Для зниження нервово-емоційного напруження, втомленості зорового аналізатора, для поліпшення мозкового кровообігу і запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ, які передбачені ДСанПіН 3.3.2.007-98, в тому числі і для сеансів психологічного розвантаження у кімнаті з відповідним інтер'єром та кольоровим оформленням.

Ігнорування санітарних правил і норм роботи з ВДТ може викликати у осіб, які з ними професійно працюють, загальну втому, зорову втому, болі та відчуття піску в очах, відчуття засміченості та свербіння очей, болі в хребті, закам'янілість та оніміння м'язів шиї та плечового поясу, пошкодження дисків хребта, порушення постави, судоми м'язів ніг, синдром RSI хронічний розтяг зв'язок, синдром тунелю Карпаля, головні болі, поганий сон, депресивні стани тощо.

**3.2 Захист від електромагнітних полів та надвисокочастотного випромінювання.**

Рік у рік зростає забруднення навколишнього середовища фізичними небезпечними факторами, до яких належать і електромагнітні та іонізуючі і теплові випромінювання, транспортний та виробничий шум або, як заведено говорити, акустичне забруднення навколишнього природного середовища. До сьогодні постійний моніторинг параметрів фізичних факторів у багатьох містах і населених пунктах практично не здійснюється. А тим часом такий небезпечний фактор як електромагнітне випромінювання дуже небезпечно впливає на здоров’я людини. Його джерелами є теле та радіостанції, лінії електропередач, виробниче обладнання та численні побутові прилади, в оточенні яких проходить життєдіяльність переважної більшості не лише міського, але й сільського населення.

Сьогодні людство, само того не підозрюючи, існує в океані електромагнітних полів. Ці поля різні за частотою та напруженістю. Їхні характеристики коливаються у часі. Весь цей процес отримав назву “електросмог”, і вчені гаряче обговорюють, яку небезпеку людям створюють джерела найрізноманітніших електромагнітних випромінювань. Високочастотні випромінювання можуть іонізувати атоми та молекули соматичних клітин і порушувати в них біохімічні процеси. Електромагнітні коливання довгохвильового спектра здатні нагрівати органіку та надавати молекулам теплового руху.

#### 3.2.1 Джерела випромінювання і його вплив на людину

Сьогодні в аеропортах і на літаках цивільної авіації широке застосування для зв'язку, радіонавігації, телекерування, телесигналізації і радіолокації одержала радіоапаратура, що працює в діапазоні високих (ВЧ), ультрависоких (УВЧ) і надвисоких частот (НВЧ). Найбільше застосування в ЦА знаходить радіоапаратура і радіосистеми, що працюють у діапазоні УВЧ і НВЧ. До них відносяться: системи інструментальної посадки літаків – курсові і глісадні маяки; системи ближньої навігації; радіолокаційні станції – далекого і ближнього виявлення, посадкові, огляду льотного поля (діапазон міліметрових довжин хвиль), літакові оглядові; передавальні станції КВ і УКВ діапазону – системи автоматичного і напівавтоматичного керування і контролю за повітряним рухом; радіостанції літака і. т. ін. Першоджерелом електромагнітних коливань у радіотехнічних пристроях є генератори ВЧ і НВЧ.

Електромагнітна енергія випромінюється в навколишній простір, у першу чергу, антенним пристроєм. Крім цього, джерелами електромагнітних полів (ЕМП) у робочих приміщеннях радіолокаційних станцій, радіотехнічних майстерень, лабораторій і радіоцентрів можуть бути окремі вузли НВЧ генераторів (магнетрони, лампи біжучої хвилі, клістрони), з’єднані елементи модуляторів з генераторами, лінії передач від генератора до антени, катодні виводи магнетронів, вентиляційні щілини, щілини у хвилеводних трактах і коаксіальних лініях і т.ін.

В процесі експлуатації і ремонту установок з генераторами електромагнітної енергії можливий вплив ЕМП на обслуговуючий персонал, а також на працівників інших об'єктів, що знаходяться в зоні випромінювання спрямованих антен радіолокаційних станцій. На робочих місцях інтенсивність ЕМП залежить від потужності джерела випромінювання і відстані від джерела випромінювання до робочого місця. У джерела електромагнітного випромінювання на відстані близько 1/6 довжини хвилі переважають поля індукції (зона індукції), а за її межами переважають поля випромінювання (зона випромінювання). Безумовно, що коли робоче місце розташоване в зоні індукції, робітник буде піддаватися впливу електричних і магнітних полів, що періодично змінюються.

Таким чином, залежно від частоти генератора робітник може перебувати або в зоні індукції в процесі роботи з УВЧ чи ВЧ генераторами, або в зоні випромінювання в процесі роботи з НВЧ генераторами (зона індукції до 16 см).

Високочастотне випромінювання зумовлює в організмі зміну умовнорефлекторної діяльності (гальмування умовних і безумовних рефлексів), падіння кров'яного тиску, рідкий пульс. Постійний вплив опромінення може призвести до стійких функціональних змін у центральній нервовій і серцево-судинній системах.

При потраплянні людини в зону випромінювання енергія ЕМП частково поглинається тілом людини. Під дією ВЧ полів у тканинах виникають ВЧ струми, що супроводжуються тепловим ефектом. Електромагнітні поля при тривалому впливі можуть викликати підвищену стомлюваність, дратівливість, головний біль чи сонливість, порушення сну, зниження кров'яного тиску, зміну температури тіла і т.ін., пов'язаних з розладом центральної нервової і серцево-судинної систем. Поля НВЧ, особливо сантиметрового і міліметрового діапазонів, викликають також зміни в крові, помутніння кришталика (катаракта), погіршення нюху, а в окремих випадках – трофічні явища: випадіння волосся, ламкість нігтів і т.ін..

Функціональні зрушення, зумовлені впливом ЕМП, є оборотними, якщо припинити опромінення; але варто враховувати, що оборотність функціональних зрушень не є безмежною і, зазвичай, визначається інтенсивністю опромінення, тривалістю впливу, а також індивідуальною особливістю організму. Тому профілактика професійних захворювань повинна передбачати, поряд з розробкою технічних засобів захисту, організаційні заходи.

#### 

**3.2.2 Захист від електромагнітних випромінювань.**

Для зменшення впливу ЕМП на персонал та населення, яке знаходиться в зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа входять організаційні, інженерно-технічні та лікарсько-профілактичні. Здійснення організаційних та інженерно-технічних заходів покладено передусім на органи санітарного нагляду. Підприємства та установи, які використовують джерела ЕМП, повинні проводити поточний санітарний нагляд за об'єктами, здійснювати організаційно-методичну роботу з підготовки спеціалістів та інженерно-технічний нагляд.

Ще на стадії проектування повинне бути забезпечене таке взаємне розташування опромінюючих та опромінюваних об'єктів, яке б зводило б до мінімуму інтенсивність опромінення. Потрібно зменшити імовірність проникнення людей у зони з високою інтенсивністю ЕМП, скоротити час перебування під опроміненням. Потужність джерел випромінювання мусить бути мінімально потрібною.

Важливе значення мають інженерно-технічні методи захисту: колективний, локальний та індивідуальний. Колективний захист спирається на розрахунок поширення радіохвиль в умовах конкретного рельєфу місцевості. Економічно найдоцільніше використовувати природні екрани – складки місцевості, лісонасадження, нежитлові будівлі. Встановивши антену нагорі, можна зменшити інтенсивність поля, яке опромінює населений пункт, у багато разів.

При захисті від випромінювання екрана повинне враховуватись затухання хвилі при проходженні через екран (наприклад, через лісову смугу). Для екранування можна використовувати рослинність. Спеціальні екрани у вигляді відбивальних щитів дорогі і використовуються дуже рідко.

Локальний захист дуже ефективний і використовується часто. Він базується на використанні радіозахисних матеріалів, які забезпечують високе поглинання енергії випромінювання у матеріалі та віддзеркалення від його поверхні. Для екранування шляхом віддзеркалення використовують металеві листи та сітки з доброю провідністю. Захист приміщень від зовнішніх випромінювань можна здійснити завдяки обклеюванню стін металізованими шпалерами, захисту вікон сітками, металізованими шторами. Опромінення у такому приміщенні зводиться до мінімуму, але віддзеркалене від екранів випромінювання перерозповсюджується в просторі та потрапляє на інші об'єкти.

До інженерно-технічних засобів захисту також належать:

* конструктивна можливість працювати на зниженій потужності в процесі налагоджування та профілактики;
* робота на еквівалент навантаження;
* дистанційне керування.

Для персоналу, що обслуговує радіозасоби та знаходиться на невеликій відстані, потрібно забезпечити надійний захист шляхом екранування апаратури. Поряд із віддзеркалюючими широко розповсюджені екрани з матеріалів, що поглинають випромінювання.

Існує велика кількість радіопоглинальних матеріалів як однорідного складу,так і композиційних, котрі складаються з різнорідних діелектричних та магнітних речовин. З метою підвищення ефективності поглинача поверхня екрана виготовляється шорсткою, ребристою або у вигляді шипів.

Радіопоглинальні матеріали можуть використовуватись для захисту навколишнього середовища від ЕМП, яке генерується джерелом, що знаходиться в екранованому об'єкті. Крім того, радіопоглиначами для захисту від віддзеркалнння личкуються стіни безлунких камер – приміщень, де випробовуються випромінювальні пристрої. Радіопоглинальні матеріали використовуються в кінцевих навантаженнях, еквівалентних системах.

**3.2.3. Засоби індивідуального захисту.**

Засоби індивідуального захисту використовуються у тих випадках коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. ЗІЗ застосовують тоді, коли безпека робіт не може бути забезпечена конструкцією та розміщенням устаткування, організацією виробничих процесів, архітектурно-планувальними рішеннямита засобами колективного захисту.

Відповідно до Закону України «Про охорону праці» на роботах із шкідливими та небезпечними умовами праці службовцям безкоштовно видаються спецодяг, спецвзуття та інші засоби індивідуального захисту.

Для захисту тіла використовується одяг із металізованих тканин та радіопоглинаючих матеріалів. Металізована тканина складається із бавовняних чи капронових ниток, спірально обвитих металевим дротом. Таким чином, ця тканина, мов металева сітка (при віддалі між нитками 0,5мм) послаблює випромінювання не меньш, як на 20-30дБ. При зшиванні деталей захистного одягу потрібно забезпечити контакт ізольованих провідників. Тому електрогерметизація швів проводиться електропровідними розчинами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок проводів, котрі не контактують.

Очі захищають спеціальними окулярами зі скла з нанесеною на внутрішній бік провідною плівкою двоокису олова. Гумова оправа окулярів має запресовану металеву сітку або обклеєна металізованою тканиною. Цими окулярами випромінювання НВЧ послаблюється на 20-30дБ. Раніше використовували рукавички та бахили, зараз вважаютьнепотрібними, оскільки допустима величина щільності потоку енергії для рук та ніг у багато разів вища ніж для тіла.

Колективні та індивідуальні засоби захисту можуть забезпечити тривалу безпечну роботу персоналу на об'єктах

Таблиця 3.2 Допустимі параметри електромагнітних випромінювань і електричного поля

|  |  |  |  |
| --- | --- | --- | --- |
| Види поля | Допустимі параметри поля | | Допустима поверхнева щільність потоку енергії (інтенсивність потоку енергії), Вт/м2 |
| за електричною складовою (Е), В/м | за магнітною складовою (Н),  A/M |
| Напруженість електромагнітного поля, 6 кГц...3 МГц | 50 | 5 |  |
| 3 МГц...30МГц | 2 | - |  |
| 30 МГц...5 ГГц | - | - | 10 |
| Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру: УФ-С (220...280 мм) |  |  | 0,001 |
| УФ-В (280...320 мм) |  |  | 0,01 |
| УФ-А (320. ..400 мм) |  |  | 10,0 |
| в інфрачервоній частині спектру: 0,76... 10,0 мкм |  |  | 35,0.. .70,0 |
| Напруженість електричного поля ВДТ |  |  | 20 вВ/м |

**3.3 Пожежна безпека.**

Пожежа - неконтрольоване горіння поза спеціальним вогнищем, яке призводить до матеріальної шкоди.

Пожежна безпека – стан об’єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвиток пожежі і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

Причинами пожеж та вибухів на підприємстві є порушення правил і норм пожежної безпеки, невиконання Закону “Про пожежну безпеку”.

Небезпечними факторами пожежі і вибуху, які можуть призвести до травми, отруєння, загибелі або матеріальних збитків є відкритий вогонь, іскри, підвищена температура, токсичні продукти горіння, дим, низький вміст кисню, обвалення будинків і споруд.

За стан пожежної безпеки на підприємстві відповідають її керівники, начальники цехів, майстри та інші керівники.

На підприємствах існує два види пожежної охорони: професійна і воєнізована. Воєнізована охорона створюється на об’єктах з підвищеною небезпекою. Крім того на підприємствах для посилення пожежної охорони організовуються добровільні пожежні дружини і команди, добровільні пожежні товариства і пожежно-технічні комісії з числа робітників та службовців. При Міністерстві внутрішніх справ існує управління пожежної охорони (УПО) і його органи на місцях. До складу УПО входить Державний пожежний нагляд який здійснює:

-Контроль за станом пожежної бепеки

- Розробляє і погоджує протипожежні норми і правила та контролює їх виконання в проектах і безпосередньо на об’єктах народного господарства

- Проводить розслідування і облік пожеж

- Організовує протипожежну профілактику.

Протипожежна профілактика – це комплекс організаційних і технічних заходів, які спрямовані на здійснення безпеки людей, на попередження пожеж, локалізацію їх поширення, а також створення умов для успішного гасіння пожежі.

Відповідальним керівником робіт по ліквідації пожеж і аварій на підприємстві є головний інженер. Начальник структурного підрозділу, в якому виникла пожежа, є відповідальним виконавцем робіт по її ліквідації.

Пожежо-вибухонебезпечність виробництв визначається агрегатним станом речовин та матеріалів та їх показниками пожежо-вибухонебезпечності.

**3.3.1 Протипожежні вимоги до будинків і споруд.**

Виходячи з властивостей речовин і матеріалів, умов їх застосування і обробки і у відповідності із ОНТП 24-86 “Визначення категорій приміщень і будівель по вибухопожежній і пожежній небезпеці” приміщення по вибухопожежній і пожежній небезпеці діляться на п’ять категорій – А, Б, В, Г, Д.

До категорії А належать приміщення, де перебувають спалимі та легкозаймисті рідини з температурою спалаху, що не перевищує 28(С, а також речовини і матеріали здатні вибухати і горіти при взаємодії з водою, киснем або одне з одним; при утворенні вибухонебезпечних сумішей розвивається розрахунковий надлишковий тиск вибуху 5 кПа.

До категорії Б належать приміщення, в яких є пил та волокна, легкозаймисті рідини з температурою спалаху понад 28(С та спалимі рідини в такій кількості, що можуть утворюватися вибухонебезпечні пилоповітряні та пароповітряні суміші, при займанні яких розвивається розрахунковий надлишковий тиск вибуху 5 кПа.

До категорії В належать приміщення, де перебувають спалимі та важкоспалимі рідини, тверді спалимі та важкоспалимі речовини та матеріали (в тому числі пил та волокна), а також речовини і матеріалиякі здатні при взаємодії з водою, киснем повітря та одне з одним тільки горіти (за умови, що ці приміщення не відносяться до категорії А чи Б).

До категорії Г належать приміщення, в яких є неспалимі речовини та матеріали в гарячому, розпеченому або розплавленому стані, а також спалимі гази, рідини та тверді речовини, які спалюються або утилізуються як паливо; процес їх обробки супроводжується виділенням променевої теплоти, іскор та полум’я.

До категорії Д належать приміщення, в яких є неспалимі речовини та матеріали у холодному стані.

На розвиток пожежі у приміщеннях та спорудах значно впливає здатність окремих будівельних елементів чинити опір впливу тепла, тобто їх вогнестійкість.

Вогнестійкість – здатність будівельних конструкцій чинити опір дії високої температури, утворенню наскрізних тріщин та поширенню вогню в умовах пожежі і виконувати при цьому свої звичайні експлуатаційні функції.

Вогнестійкість конструкцій будівель характеризується межею вогнестійкості.

Межа вогнестійкості – це час, на протязі якого конструкція може витримати дію вогню, а потім вже починається деформація.

Всі будівлі і споруди за ступенем вогнестійкості за СНиП 2.01.02-85 поділяють на 5 ступеней.

Будинок може належати до того або іншого ступеня вогнестійкості, якщо значення меж вогнестійкості і меж поширення вогню усіх конструкцій не перевищує значень вимог СНіП 2.01.02-85.

**3.3.2 Пожежна профілактика електрообладнання.**

Електрична енергія певних умовах легко переходить у теплову і це може викликати пожежі і вибухи. Пожежна небезпека електрообладнання, електронних приладів, радіоелектронної апаратури, апаратури управління, електроприймачів пов’язана з використанням спалимих матеріалів: гуми, пластмас, лаків, олій.

Джерелами займання можуть бути електричні іскри, дуги, коротке замикання, струмові перевантаження, перегріті опірні поверхні, несправність обладнання. Окислювачем звичайно служить кисень. Але потужність і тривалість дії цих джерел займання порівняно малі, тому горіння, як правило, не розвивається. Виникнення пожежі в електронних пристроях можливо, якщо використовуються спалимі і важкоспалимі матеріали і вироби.

Кабельні лінії електроживлення виконані з спалимого ізоляційного матеріалу, тому є найбільш пожежонебезпечними елементами в конструкціях електрообладнання.

**3.4 Коротке замикання (КЗ).**

КЗ виникають в результаті порушення ізоляції частин обладнання, що проводять струм і зовнішніх механічних пошкоджень в електричних дротах, монтажних дротах, обмотках двигунів і апаратів. Ізоляція елементів, що проводять струм може пошкоджуватися при дії на неї високої температури або полум’я, інфрачервоного випромінювання, переходу напруги з первинної обмотки силового трансформатора на вторинну, при підвищених режимах навантаження (нагрів до високих температур, і як наслідок при охолодженні конденсується вода) та інш.

Сила струму КЗ може бути від одиниць до сотень кілоампер. Струми КЗ викликають термічну і електродинамічну дію і супроводжуються різким зниженням напруги в електромережі. Струми КЗ можуть перегріти частини, що проводять струм і розплавити дроти (температура до 20000(С). Протікання по провіднику тривалого допустимого струму силою (І) пов’язано з виділенням тепла Q (Дж), і кількісно визначається законом Ленца-Джоуля: [pic], I – сила тривалого припустимого струму, А; R – активний опір, Ом; ( - час, с. Час проходження струму КЗ не перевищує декількох секунд або навітьдолі секунди і залежить від дії апаратів захисту (плаких запобіжників, автоматичних виключателі, інш). При проходженні струму КЗ сила якого перевищує допустимий струм, температура нагріву дроту різко підвищується і може досягнути небезпечних значень.

Відомо, що два провідники, по яких проходить електричний струм, взаємодіють один з одним. Напрям сили взаємодії визначається напрямом струму в провідниках. При одинаковому напрямі струму електродинамічні сили притягують провідники, при різних – відштовхують. При КЗ в мережі можуть виникати струми, що в десятки і сотні раз перевищують номінальні, тому електродинамічні сили стараються деформувати провідники і ізолюючі частини, на яких вони кріпляться.

КЗ супроводжується різким зниженням напруги в електромережах. В результаті виникає частковий або повний розлад електропостачання споживачів.

Профілактика КЗ передбачає наступні заходи: правильний вибір, монтаж і експлуатація електричних мереж, електрообладнання правильний вибір конструкціїї електрообладнання, способу встановлення і класу ізоляції (опір ізоляції згідно з ПУЕ 500кОм) електричний захист електричних мереж, електрообладнання (швидкодіючі реле, автоматичні вимикачі, запобіжники).

Перевантаження.

При проходженні струму по провідниках виділяється тепло, яке нагріває їх до температур при яких посилюються окислювальні процеси, на дротах утворюються оксиди, які мають високий опір, збільшується опір контакту і, відповідно кількість тепла, що виділяється. А це спричиняє старіння або руйнування ізоляції. Наслідком цього може бути електричний пробій ізоляції і пошкодження пристрою, а при наявності спалимої ізоляції і пожежо- і вибухонебезпечного середовища – пожежа або вибух. Оскільки кожний провідник розрахований на певний струм, то збільшення його може призвести до перевантаження.

Причиною перевантаження може бути неправильний розрахунок при проектуванні мереж і схем (занижений переріз дротів, перевантаження радіоелементів, додаткове включення пристроїв до джерел живлення на які вони не розраховані), пониження напруги в мережі.

Профілактика пожеж від перевантажень: при проектуванні необхідно правильно вибирати переріз провідників мереж і схем за допустимою густиною струму, щоб Ідоп.>=Ір; в процесі експлуатації електричних мереж не можна включати додатково електроприймачі, якщо мережа на це не розрахована; для захисту електрообладнання від струмів перевантаження найбільш ефективні автоматичні і електронні схеми захисту, виключателі, теплові реле і плавкі запобіжники.

Перехідні опори.

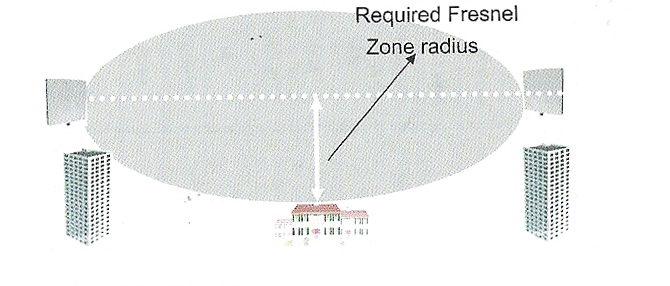
Причиною пожежі і аварій можуть бути великі перехідні опори, які виникають в місцях з’єднань та розгалужень провідників, в контактах пристроїв, або на клемах, якщо ці з’єднання зроблені неправильно або покрилися іржою.

При проходженні струму навантаження в такому контактному з’єднанні виділяється деяка кількість тепла, пропорційна квадратному струму і опору точок дійсного дотику. Вона може бути досить велика, що місця перехідних опорів сильно нагріваються. Якщо контакти будуть торкатися спалимих матеріалів, то ці матеріали можуть зайнятися, якщо ж є вибухонебезпечна суміш газів виникне вибух.

Профілактика пожеж від перехідних опорів: для збільшення площі дійсного дотику контактів необхідно використовувати пружні контакти або спеціальні стальні пружини; для відводу тепла від точок дотику і розсіювання його необхідно виготовляти контакти певної маси і поверхні охолодження; всі контактні з’єднання повинні бути доступні для огляду.

Головним засобом запобігання пожеж і вибухів від електрообладнання є правильний вибір і експлуатація обладнання у вибухо- і пожежоне

**Висновок**

Мета даного дипломного проекту полягала в огляді існуючих можливостей на базі сучасних і економічно доцільних технологій, розробці й розгортанні локальної мережі на основі технології Wi-Fi.