О.Г. Бєдняк, Ю.В. Савченко,
В.О. Воскобойник, А.В. Тіменко
Н.В. Кіцель, О.О. Шаповал

ОСНОВИ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

Монографія

Кременчук
NOVABOOK
ВИДАВНИЦТВО
2025

УДК 004.7:621.391
О 72

Друкується за рекомендацією вченої ради
Кременчуцького національного університету імені Михайла
Остроградського (протокол № 7 від 24.04.2025 р.)
Рецензенти:

КУХАР Володимир Валентинович – доктор технічних наук, професор, проректор з науково-дослідної роботи, ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА», м. Запоріжжя, Україна;
МАРКОВ Олег Євгенійович – доктор технічних наук, професор, завідувач кафедри автоматизації виробничих процесів, Донбаська державна машинобудівна академія, м. Тернопіль, Україна.

О 72 **Основи бездротових технологій** / О.Г. Бєдняк, Ю.В. Савченко, В.О. Воскобойник, А.В. Тіменко, Н.В. Кіцель, О.О. Шаповал. – Кременчук : Видавництво «НОВАБУК», 2025. – 300 с.
ISBN 978-617-639-525-6

Робота присвячена розгляду Wi-Fi – це технологія, що дозволяє різним стаціонарним і мобільним цифровим пристроям підключатися до інтернету без використання проводів. Для цього використовуються радіосигнали, які передаються через повітря. Метою даної монографії є сприяти підготовці фахівців галузі знань 12 «Інформаційні технології», спеціальностей 123 «Комп'ютерна інженерія», 125 «Кібербезпека та захист інформації»; галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону», спеціальності 256 «Національна безпека», а також усіх бажаючих, які мають знання за загальним принципом функціонування, стандартними протоколами та технологіями побудови комп'ютерних мереж. Основними компетенціями монографії є необхідність надати студентам знання про принципи побудови та функціонування комп'ютерних мереж, основні технології та обладнання передачі даних, протоколи інформаційного обміну та мережеві можливості операційних систем. Монографія складається з вступу, дванадцяти розділів, списку використаних джерел і додатків. Повний обсяг становить 300 сторінок, 141 рисунків, 15 таблиць, 7 додатків, список використаних джерел із 20 найменувань.

УДК 004.7:621.391

ISBN 978-617-639-525-6

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АМ – амплітудна модуляції
ОБС – одна бокова смуга
WDM (Wavelength Division Multiplexing) – ущільнення за довжинами хвиль
MFSK (Multiple FSK) – багаточастотна модуляція
CDM (Code Division Multiplexing) – Ущільнення з кодовим поділом
FDM (Frequency Division Multiplexing) – ущільнення з частотним поділом
OFDM (Orthogonal Frequency Division Multiplexing) – мультиплексування за допомогою ортогональних несучих частот
FEC (Forward Error Correction) – схеми прямої корекції помилок
ARQ (Automatic Repeat Request) – запит повторної передачі
CRC (Cyclic Redundancy Check) – циклічний надлишковий контроль
ARQ (Automatic Repeat Request) – автоматичний запит повторної передачі
FHSS – метод стрибкоподібної перебудови частоти
DSSS – метод прямої послідовності
DBPSK (Differential Binary Phase Shift Keying) – Двійкова відносна фазова модуляція
DQPSK (Differential Quadrature Phase Shift Key) – Квадратурна відносна фазова модуляція
ISO/OSI (The Open Systems Interconnection model) – м ережева модель стека (магазину) мережевих протоколів
LAN (Local Area Network) – локальна комп’ютерна мережа

ВСТУП

Комп'ютерні мережі сьогодні є звичним інструментом комунікацій, інформаційного обміну та виконання обчислень. Одночасно організація мереж, принципи їх функціонування та правила конфігурування не є простими і вимагають від фахівців, які виконують проектування, побудову та адміністрування комп'ютерних мереж, певних теоретичних знань та обов'язкового практичного досвіду.

Бездротова технологія Wi-Fi у тому приблизно вигляді, у якому вона існує сьогодні, була розроблена й стандартизована наприкінці 90-х років минулого сторіччя. Але історично її створення почалася на добрі 10 років раніше. В 1980-их відразу кілька груп учених з Америки й Об'єднаного Королівства займалися активною теоретичною та практичною розробкою технологій, які могли б забезпечити будівництво бездротових мереж передачі даних. А найперші випадки для передачі даних на короткі відстані з'явилися ще раніше – в 1970-ті.

1985 рік можна назвати проривним – саме в цей час був створений стандарт IEEE 802.11, який став основою для майбутніх бездротових комунікацій, гранично близьких до тих, які сьогодні ми називаємо технологією Wi-Fi. А розробка справжнього Wi-Fi почалася в 1989 році, коли компанія NCR Corporation і мережа лабораторій Intel спроєктували радіотехнологію Wavelan. Спочатку вона створювалася винятково для комерційної експлуатації в офісах і на виробничих підприємствах.

Після цього в 1991 році компанія AT&T розробила технологію Wavelan 802.11 у рамках проєкту «JANET». Але ця технологія не одержала широкого поширення через високу вартість устаткування й складності використання. І, нарешті, в 1997 році Wi-Fi був стандартизований і одержав свою нинішню назву в рамках проєкту IEEE 802.11. «Батьком» Wi-Fi світове телекомунікаційне товариство визнає Джона О'салливана з Австралії.

У цьому ж році була створена організація Wi-Fi Alliance, яка займається просуванням і стандартизацією технології Wi-Fi. З

тих пір стандарт постійно розбудовується й удосконалюється. У сучасному світі він належить до числа найвідоміших і найчастіше використовуваних.

Wi-Fi – це технологія, що дозволяє різним стаціонарним і мобільним цифровим пристроям підключатися до інтернету без використання проводів. Для цього використовуються радіосигнали, які передаються через повітря. Сьогодні людство досягло етапу, коли доступ до Інтернету та взаємодія через Wi-Fi стали реальністю не лише для традиційних обчислювальних пристроїв, а й для побутової техніки – зокрема, роботів-пилососів, електроінструментів. Не говорячи про комп'ютери й ноутбуки, планшети й смартфони, телефони й розумні годинники, аудіоколонки й цифрові мультимедійні станції. І навіть розетки й вимикачі, які одержують усе більшого поширення в hi-tech системах за назвою «Розумний будинок».

Як працює Wi-Fi? Wi-Fi передає дані від одного обладнання до іншого за допомогою радіохвиль у певному частотному діапазоні – 2,4; 5 або 6 ГГц.

Для створення мережі звичайно використовують роутери або маршрутизатори з бездротовими адаптерами. Їхня головна відмінність полягає в способі підключення до кабелю інтернет-провайдера: роутер – прямо, маршрутизатор – через модем.

На кожному із цих обладнань є антени для передачі сигналу. Вони можуть перебувати усередині корпусу модема або маршрутизатора, а можуть бути зовнішніми.

На обладнанні-одержувачі, наприклад ноутбуці або смартфоні, теж є антена, яка звичайно перебуває усередині корпусу. Її розмір і форма залежать від конкретного гаджета.

Якщо говорити просто, то передача даних за допомогою Wi-Fi працює в такий спосіб. На антени роутера або маршрутизатора подається струм, який використовується для генерації радіохвиль. Тут відбувається модулювання сигналу. Це означає, що його характеристики, такі як амплітуда, частота або фаза, змінюються відповідно до бітів інформації, які потрібно передати. Модуляція «упаковує» передані дані (набір нулів і одиниць) у форму радіохвилі, придатну для бездротової передачі.

На комп'ютері або іншому гаджеті приймач демодулює сигнал, переводячи радіохвилю у вихідні дані, тобто в набір нулів і одиниць, з якими здатні працювати обладнання.

Радіосигнали проходять через стіни й інші перешкоди – це забезпечує зв'язок усередині приміщень і на невеликих відстанях. Загальна зона покриття Wi-Fi – кілька десятків метрів усередині будинків і близько 100 метрів у вуличних точках доступу. Вона залежить від потужності роутера, діапазону частот і версії стандарту. Стіни, меблі, металеві об'єкти й інші перешкоди зменшують зону покриття.

Для бездротового зв'язку використовуються радіохвилі в діапазоні частот 2,4; 5 і 6 ГГц. Усередині діапазону є окремі канали для підключення:

– Для Wi-Fi із частотою 2,4 ГГц використовується три непересічні канали із шириною 20 МГц кожний.

– Для частоти 5 ГГц використовуються 33 каналу, 19 з яких не перетинаються. При цьому канали мають ширину 40 МГц, тобто у два рази більше, ніж у Wi-Fi із частотою 2,4.

– Для стандарту із частотою 6 ГГц використовується вже 59 каналів різної ширини. З'являються 14 додаткових каналів шириною 80 МГц і сім каналів шириною 160 МГц.

Звучить складно, але тут працює правило: чим більше непересічних каналів і чим більше їх ширина, тем менше перешкод буде виникати через одночасну роботу декількох мереж. Тому в багатоквартирних будинках або в бізнес-центрах, де одночасно існують десятки або сотні бездротових мереж, краще використовувати Wi-Fi із частотою 5 ГГц, а не 2,4 ГГц. В останньому випадку вони будуть перетинатися, знижуючи стабільність один одного.

Wi-Fi – технологія бездротового зв'язку, за допомогою якої комп'ютери, смартфони, планшети й інше обладнання обмінюються даними за допомогою ультракоротких радіохвиль.

В основі Wi-Fi лежить набір стандартів IEEE 802.11 – це правила, які використовуються для створення бездротової локальної мережі. Вони розробляються Інститутом інженерів електротехніки й електроніки (IEEE, Institute of Electrical and Electronics Engineers). Сьогодні IEEE 802.11 містять у собі кілька

стандартів, які різняться своїми характеристиками: 802.11b, 802.11ax та інші. Про них ми докладно поговоримо далі.

Стандарти IEEE 802.11 звичайно називають Wi-Fi. Цей бренд просуває Wi-Fi Alliance – некомерційна організація, що поєднує виробників бездротових технологій. Вона ж займається забезпеченням сумісності стандартів і розробкою їх нових версій.

Wi-Fi створює бездротову локальну мережу в обмеженій області: у межах будинку, офісу або іншого простору. Усередині мережі можуть перебувати комп'ютери, планшети, смартфони, принтери й інші обладнання.

У квартирі або офісі Wi-Fi часто використовують для бездротового підключення до інтернету. Але локальна мережа може існувати й без нього, забезпечуючи обмін даними між обладнаннями усередині цієї мережі.

Для чого потрібний Wi-Fi – бездротове підключення обладнань до інтернету. Wi-Fi використовують у квартирах, офісах і громадських місцях для створення бездротової точки доступу до інтернету. До неї можна під'єднати пристрої, що не потребують мережевого кабелю, зокрема смартфони, планшети та ноутбуки.

Створення локальної мережі для обміну даними й керування обладнаннями. За допомогою Wi-Fi можна об'єднати обладнання в локальну мережу. Вони зможуть передавати один одному файли й використовувати спільні ресурси: загальні теки і так далі.

Об'єднані обладнання можуть взаємодіяти один з одним без підключення через кабель. Наприклад, можна направити файл із комп'ютера на принтер для друку всередині локальної мережі.

Wi-Fi – один зі стандартів бездротового підключення, взаємодії й керування обладнаннями Iot: термостатами, лампочками, камерами відеоспостереження, замками, вимикачами й іншими гаджетами в розумних будинках.

Переваги і недоліки Wi-Fi. Wi-Fi – основний протокол бездротового зв'язку, який використовується у квартирах, офісах і на виробничих об'єктах. Його широке поширення пов'язане з перевагами стандарту: при переміщенні обладнання у просторі зберігається стабільність з'єднання й висока швидкість передачі даних.

Одна бездротова мережа може обслуговувати кілька десятків обладнань одночасно. Максимальна кількість гаджетів залежить від стандарту Wi-Fi, типу роутера й пропускної здатності мережі.

Можна підключати до Wi-Fi різноманітні розумні обладнання й датчики, створити мережу для керування розумним будинком, медіацентром, системою безпеки й іншими додатками Iot.

Wi-Fi можна використовувати для створення локальних бездротових мереж. Обладнання усередині будинку або офісу зможуть обмінюватися даними між собою без проводів і підключатися до загальних ресурсів: принтеру, сканеру тощо.

Можливість налаштування мережі з декількома маршрутизаторами. Вона забезпечує «безшовне» підключення обладнань до інтернету навіть у приміщеннях з більшою кількістю об'єктів, що екранують, – наприклад, з товстими стінами або промисловим устаткуванням.

Але є й недоліки, які варто враховувати при роботі з Wi-Fi. Сигнал обмежений межами певної зони покриття. Як правило, у приміщеннях це 50–70 метрів залежно від типу роутера або маршрутизатора. Стіни, особливо залізобетонні, масивні меблі й інші перешкоди погіршують якість сигналу. Цю проблему можна вирішити за допомогою репітера, але це вимагає додаткових витрат.

Стабільність з'єднання може погіршуватись через електромагнітні завади, що виникають від роботи інших бездротових пристроїв і електронного обладнання. До таких джерел інтерференції належать флуоресцентні лампи, електронагрівачі, вентилятори, мікрохвильові печі, бездротові телефони, Bluetooth-пристрої, охоронні системи та інші засоби, що працюють у тому самому частотному діапазоні, що й Wi-Fi – 2,4 ГГц. Одним із способів усунення цього негативного впливу є використання мережевого з'єднання у діапазоні 5 ГГц.

Той самий канал можуть використовувати мережі, розташовані поруч, що призводить до його перевантаження. Знижується стабільність з'єднання й швидкість передачі даних. Це варто враховувати при розташуванні квартири або офісу в щільно населених районах або місцях з високою концентрацією

бездротових обладнань. Упоратися з перевантаженням каналу допоможе використання мереж із частотним діапазоном 5 ГГц, тому що в них більше каналів з більшою шириною, які не перекриваються один одним.

Більш детально про це розглянуто в даній монографії. Матеріал структуровано за тематичними розділами.

Матеріал монографії охоплює канальний, мережевий та транспортний рівні моделі мережевої взаємодії (ДОДАТОК Ж), оскільки саме ці рівні в основному відповідають за організацію комп'ютерних мереж.

Метою даної монографії є сприяння підготовці фахівців галузі знань 12 «Інформаційні технології», спеціальностей 123 «Комп'ютерна інженерія», 125 «Кібербезпека та захист інформації», галузі знань: 25 «Воєнні науки, національна безпека, безпека державного кордону», спеціальності 256 «Національна безпека», а також усіх бажаючих, які мають знання за загальним принципом функціонування, стандартними протоколами та технологіями побудови комп'ютерних мереж.

Основними компетенціями монографії є необхідність надати студентам знання про принципи побудови та функціонування комп'ютерних мереж, основні технології та обладнання передачі даних, протоколи інформаційного обміну та мережеві можливості операційних систем.

Монографія складається з вступу, дванадцяти розділів, списку використаних джерел та додатків. Повний обсяг становить 306 сторінок, 141 рисунків, 15 таблиць, 7 додатків, список використаних джерел із 20 найменувань.

1. ОСНОВИ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

1.1. Що таке Wi-Fi?

WI-FI – це сучасна бездротова технологія з'єднання комп'ютерів у локальну *мережу* й підключення їх до *Internet*. Саме завдяки цій технології *Internet* стає мобільним і дає користувачеві волю переміщення не лише в межах кімнати, але й по усьому світу.

Уявіть собі таку картину: ви користуєтеся своїм комп'ютером, так само як мобільним телефоном; вам не потрібні кабелі, ви можете приєднати свій ноутбук у будь-яку точку доступу й увійти в *Internet* практично звідусіль. Це – найближче майбутнє.

Під абревіатурою «Wi-Fi» (від англійського словосполучення "*Wireless Fidelity*", яке можна дослівно перевести як «висока *ймовірність* бездротової передачі даних») наразі об'єднано ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах.

Зі збільшенням числа мобільних користувачів виникає гостра потреба в оперативному створенні комунікацій між ними, в обміні даними та у швидкому одержанні інформації. Тому природно відбувається інтенсивний розвиток технологій бездротових комунікацій. Особливо це актуально відносно бездротових мереж, або так званих Wlan-*Мереж* (*Wirelesslocal Area Network*). Мережі *Wireless LAN* – це бездротові мережі (замість звичайних проводів у них використовуються радіохвилі). Установка таких мереж рекомендується там, де *розгортання* кабельної системи неможливо або економічно недоцільно.

Бездротові мережі особливо ефективні на підприємствах, де співробітники активно переміщаються по території під час робочого дня з метою обслуговування клієнтів або збору інформації (великі склади, агентства, офіси продажів, служби охорони та безпеки, установи охорони здоров'я тощо).

Завдяки функції роумінгу між точками доступу користувачі можуть переміщатися по території покриття мережі Wi-Fi без розриву з'єднання.

Wlan-Мережі мають ряд переваг перед звичайними кабельними мережами:

– *Wlan-Мережу* можна дуже швидко розгорнути, що дуже зручно при проведенні презентацій або в умовах роботи поза офісом;

– користувачі мобільних пристроїв при підключенні до локальних бездротових мереж можуть легко переміщатися в межах покриття мережі;

– швидкість сучасних мереж досить висока, що дозволяє використовувати їх для вирішення дуже широкого спектра завдань;

– *Wlan-Мережа* може виявитися єдиним виходом, якщо неможлива прокладка кабелю для звичайної мережі.

Разом з тим необхідно пам'ятати про обмеження бездротових мереж. Це, як правило, все-таки менша швидкість, схильність впливу перешкод і більш складна схема забезпечення безпеки передачі інформації.

Сегмент Wi-Fi мережі може використовуватися як самостійна *мережа*, або в складі більш складної мережі, що містить як бездротові, так і звичайні дротові *сегменти*.

Wi-Fi *мережа* може використовуватися:

– для бездротового підключення користувачів до мережі;

– для об'єднання просторово рознесених підмереж в одну загальну мережу там, де кабельне з'єднання підмереж неможливо або небажане;

– для підключення до мереж провайдера Internet-послуги замість використання виділеної провідної лінії або звичайного модемного з'єднання.

1.1.1. Модуляція сигналів

Історично модуляція почала застосовуватися для аналогової інформації, і тільки потім – для дискретної. Необхідність у модуляції аналогової інформації виникає, коли потрібно передати низькочастотний (наприклад, голосовий) *аналоговий*

сигнал через канал, що перебуває у високочастотній області спектра.

Для вирішення цієї проблеми амплітуду високочастотного опорного сигналу змінюють (модулюють) відповідно до зміни низькочастотного сигналу.

У бездротовій технології в процесі модулювання залучена одна або декілька характеристик опорного сигналу: амплітуда, частота й фаза. Відповідно, існують три основні технології кодування або модуляції, що виконують перетворення цифрових даних в *аналоговий сигнал* (рис. 1.1):

- амплітудна модуляція (*Amplitude-Shift* Keying – ASK);
- частотна модуляція (Frequency-Shift Keying – *FSK*);
- фазова модуляція (*Phase-Shift* Keying – *PSK*).

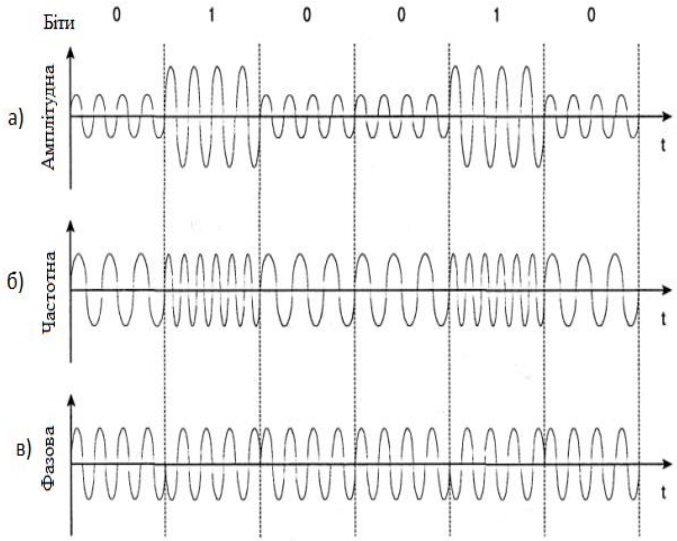


Рисунок 1.1 – Модуляція цифрових даних аналоговими сигналами

Слід відзначити, що у всіх перерахованих випадках підсумковий сигнал центрований на опорній частоті.

При *амплітудній модуляції* двійкові значення представляються сигналами опорної частоти із двома різними

амплітудами. Одна з амплітуд, як правило, вибирається рівною одиниці; тобто одне двійкове число представляється наявністю опорної частоти при постійній амплітуді, а інше – амплітудою іншої величини або її відсутністю (рис. 1.1а).

При амплітудній модуляції підсумковий сигнал рівний:

$$s(t) = \begin{cases} A\cos(2\pi f_c\, t) - \text{двійкова } 1 \\ 0 - \quad \text{двійковий } 0 \end{cases} \qquad (1.1)$$

де $A\cos(2\pi f_c\, t) -$ несучий сигнал.

Найпоширенішою формою *частотної модуляції* є бінарна: (Binary *FSK* – *BFSK*), у якій двійкові числа представляються сигналами двох різних частот, розташованих близько опорної (рис. 1.1б). Підсумковй сигнал буде рівний

$$s(t) = \begin{cases} A\cos(2\pi f_1\, t) & - \text{двійкова } 1 \\ A\cos(2\pi f_2\, t) & - \text{двійковий } 0 \end{cases} \qquad (1.2)$$

де f_1 і f_2 – частоти, зміщені від опорної частоти f_c на величини, рівні по модулю, але протилежні за знаком.

Бінарна частотна модуляція менш сприйнятлива до помилок, ніж амплітудна модуляція.

Більш ефективною, але водночас більш вразливою до помилок, є схема *багаточастотної модуляції* (Multiple *FSK* – *MFSK*), у якій використовується більш як дві частоти. У цьому випадку кожна сигнальна посилка представляє більше одного біта. Переданий сигнал *MFSK* (для одного періоду передачі сигнальної посилки) можна визначити в такий спосіб:

$$s_i = A\cos(2\pi f_i t), \quad 1 << i >> M \qquad (1.3)$$

В цьому виразі $f_i = f_c + (2i - 1 - M)f_d$,

де f_c – опорна частота; f_d – різниця частот; $M = 2^L$ - число різних сигнальних посилок; L – кількість бітів на одну сигнальну посилку.

На рис. 1.2 представлений приклад схеми *MFSK* з $M = 4$. Вхідний потік бітів кодується по два біти, після чого передається одна із чотирьох можливих двобітових комбінацій.

Для зменшення ширини смуги частот у модуляторах сигналів з фазовою модуляцією використовуються фільтри згладжування. Застосування фільтрів згладжування призводить до збільшення ефективності використання смуги, але водночас зменшується відстань між сусідніми сигналами, що викликає зниження завадостійкості.

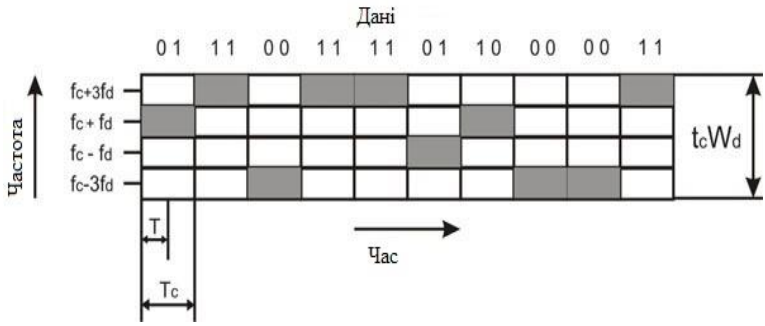


Рисунок 1.2 – Використання частоти схемою MFSK (M = 4)

При *фазовій модуляції* для представлення даних виконується зсув опорного сигналу. Найпростішою фазовою модуляцією є дворівнева модуляція (Binary *PSK, BPSK*), де для представлення двох двійкових цифр використовуються дві фази (рис. 1.1в). Отриманий сигнал має такий вигляд (для одного періоду передачі біта):

$$s(t)=\begin{cases} A\cos(2\pi f_c\, t) \\ A\cos(2\pi f_c\, t+\pi) \end{cases}=\begin{cases} A\cos(2\pi f_c\, t)-\text{двійкова } 1 \\ -A\cos(2\pi f_c\, t)-\text{ двійковий } 0 \end{cases} \qquad (1.4)$$

Альтернативною формою дворівневої PSK є диференціальна PSK (DPSK), приклад якої наведений на рис. 1.3. У даній системі двійковий 0 виражається сигнальним пакетом, фаза якого збігається з фазою попереднього посланого пакета, а двійкова 1 виражається сигнальним пакетом з фазою, протилежною фазі попереднього пакета. Така схема називається диференціальною, оскільки зрушення фаз здійснюється відносно попередньо

переданого біта, а не щодо якогось еталонного сигналу. При диференціальному кодуванні передана інформація відображається не сигнальними посилками, а змінами між послідовними сигнальними посилками. Схема DPSK робить зайвим суворе узгодження фази місцевому гетеродину приймача й передавача. Доти, поки попередня отримана фаза точна, точний і фазовий еталон.

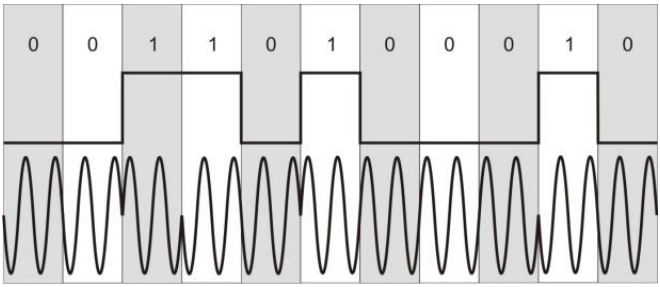


Рисунок 1.3 – Диференціальна фазова модуляція (DPSK)

Якщо кожною сигнальною посилкою представити більш одного біта, це дозволить ефективніше використовувати смугу сигналу. Наприклад, у розповсюдженому кодуванні, відомої як квадратурна фазова модуляція (Quadrature Phase-Shift Keying – QPSK), замість зсуву фази на 180^0, як у кодуванні BPSK, використовуються зсуви фаз, кратні π/2 (90^0).

При квадратурній фазовій модуляції:

$$s(t) = \begin{cases} A\cos(2\pi f_c\, t\frac{\pi}{4}) - 11 \\ A\cos(2\pi f_c\, t\frac{3\pi}{4}) - 10 \\ A\cos(2\pi f_c\, t\frac{5\pi}{4}) - 00 \\ A\cos(2\pi f_c\, t\frac{7\pi}{4}) - 01 \end{cases} \quad (1.5)$$

Таким чином, кожна сигнальна посилка містить не один біт, а два.

Описану схему можна розширити: передавати, наприклад, по три біти в кожний момент часу, використовуючи для цього вісім різних кутів зсуву фаз. Більше того, для кожного кута може використовуватися кілька амплітуд. Така модуляція називається багаторівневою фазовою модуляцією (Multiple PSK – MPSK).

Квадратурна амплітудна модуляція (Quadrature Amplitude Modulation – QAM) є популярним методом аналогової передачі сигналів, який використовується у деяких бездротових стандартах. Ця схема модуляції поєднує в собі амплітудну й фазову модуляції. У методі QAM використані переваги одночасної передачі двох різних сигналів на одній опорній частоті, але при цьому залучено дві копії опорної частоти, зсунуті відносно один одного на 90 градусів. При квадратурній амплітудній модуляції обидві опорні частоти є амплітудно-модульованими. Отже, два незалежні сигнали одночасно передаються через одне середовище. У приймачі ці сигнали демодулюються, а результати поєднуються з метою відновлення вихідного двійкового сигналу.

При використанні дворівневої квадратурної амплітудної модуляції (2QAM) кожний із двох потоків може перебувати в одному із двох станів, а об'єднаний потік – в одному з *2x2=4* станів. При використанні чотирирівневої модуляції (тобто чотирьох різних рівнів амплітуди, 4QAM) об'єднаний потік буде перебувати в одному з *4x4 = 16* станів. Уже реалізовані системи, які мають 64 або навіть 256 станів. Чим більше число станів, тим вище швидкість передачі даних, яка можлива при певній ширині смуги. Отже, як вказувалося раніше, чим більше число станів, тим вища потенційна частота виникнення помилок внаслідок перешкод або поглинання. Більш детальна інформація про квадратурну амплітудну модуляцію надана в Додаток Д.

1.2. Основні елементи мережі Wi-Fi

Для побудови бездротової мережі використовуються Wi-Fi адаптери та точка доступу.

Адаптер (рис1.4) – пристрій, який підключається через слот розширення PCI, PCMCIA, Compactflash. Існують також

адаптери з підключенням через порт USB 2.0, 3.0. Wi-Fi адаптер виконує ту ж функцію, що й мережева карта в дротовій мережі. Він служить для підключення комп'ютера користувача до бездротової мережі.

Рисунок 1.4 – Адаптери

Завдяки платформі Centrino усі сучасні ноутбуки мають вбудовані адаптери Wi-Fi, сумісні з багатьма сучасними стандартами. Wi-Fi адаптерами, як правило, забезпечуються й КПК (кишенькові персональні комп'ютери), що також дозволяє підключати їх до бездротових мереж.

Для доступу до бездротової мережі адаптер може встановлювати зв'язок безпосередньо з іншими адаптерами. Така *мережа* називається *бездротовою одноранговою мережею,* або *Ad Hoc* («до випадку»). *Адаптер* також може встановлювати зв'язок через спеціальний пристрій – точку доступу. Такий режим називається *інфраструктурою*.

Для вибору способу підключення адаптер повинен бути налаштований на використання або *Ad Hoc*, або *інфраструктурного* режиму.

Точка доступу (рис. 1.5) – автономний модуль із вбудованим мікрокомп'ютером і приймально-передавальним пристроєм.

Через точку доступу здійснюється взаємодія й обмін інформацією між бездротовими адаптерами, а також зв'язок із дротовим сегментом мережі. Таким чином, точка доступу виступає комутатором. Точка доступу має мережевий інтерфейс (*uplink port*), за допомогою якого вона може бути підключена до

звичайної дротової мережі. Через цей інтерфейс може здійснюватися й налаштування точки.

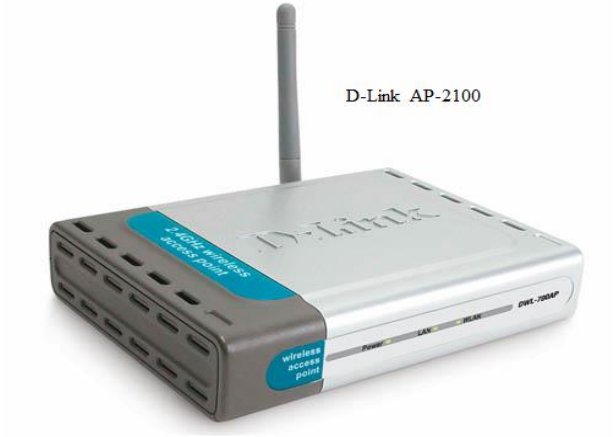


Рисунок 1.5 – Точка доступу

Опис бездротового устаткування можна знайти в Додатку А. Огляд бездротового устаткування D-Link .

Точка доступу може використовуватися як для підключення до неї клієнтів (базовий режим точки доступу), так і для взаємодії з іншими точками доступу з метою побудови розподіленої мережі (Wireless Distributed System – WDS). Це режими бездротового мосту «точка-точка» і «точка-багато точок», бездротовий клієнт і *повторювач*.

Доступ до мережі забезпечується шляхом передачі широкомовних сигналів через ефір. Приймальна станція може одержувати сигнали в діапазоні роботи декількох передавальних станцій. Станція-приймач використовує ідентифікатор зони обслуговування (Service Set Identifier – SSID) для фільтрації одержуваних сигналів і виділення того, який їй потрібен.

Зоною обслуговування (Service Set – SS) називаються логічно згруповані пристрої, що забезпечують підключення до бездротової мережі.

Базова зона обслуговування (Basic Service Set – BSS) – це група станцій, які зв’язуються одна з одною по бездротовому

зв'язку. Технологія BSS припускає наявність особливої станції, яка називається *точкою доступу (access point).*

Для більш повного розуміння роботи бездротових пристроїв слід розглянути наступний матеріал.

1.3. Основи передачі даних у бездротових мережах

1.3.1. Сигнали для передачі інформації

Якщо розглядати сигнал як функцію часу, то він може бути або аналоговим, або цифровим. *Аналоговим* називається сигнал, інтенсивність якого в часі змінюється поступово. Інакше кажучи, у сигналі не буває пауз або розривів. *Цифровим* називається сигнал, інтенсивність якого протягом деякого періоду підтримується на постійному рівні, а потім також змінюється на постійну величину (це визначення ідеалізоване). На рис. 1.6 наведені приклади сигналів обох типів. Аналоговий сигнал може представляти мову, а цифровий – набір двійкових одиниць і нулів.

Найпростішим типом сигналу є періодичний сигнал, у якому деяка структура періодично повторюється в часі.

На рис. 1.7 наведений приклад періодичного аналогового сигналу (синусоїда) і періодичного цифрового сигналу (прямокутний сигнал, або *меандр*).

Математичне визначення: сигнал s(t) є періодичним тоді й тільки тоді, коли

$$\mathrm{s(t+T)} = s(t), \text{при}, -\infty < t < +\infty, \qquad (1.6)$$

де: постійна T є періодом сигналу (T – найменша величина, що задовольняє цьому рівнянню).

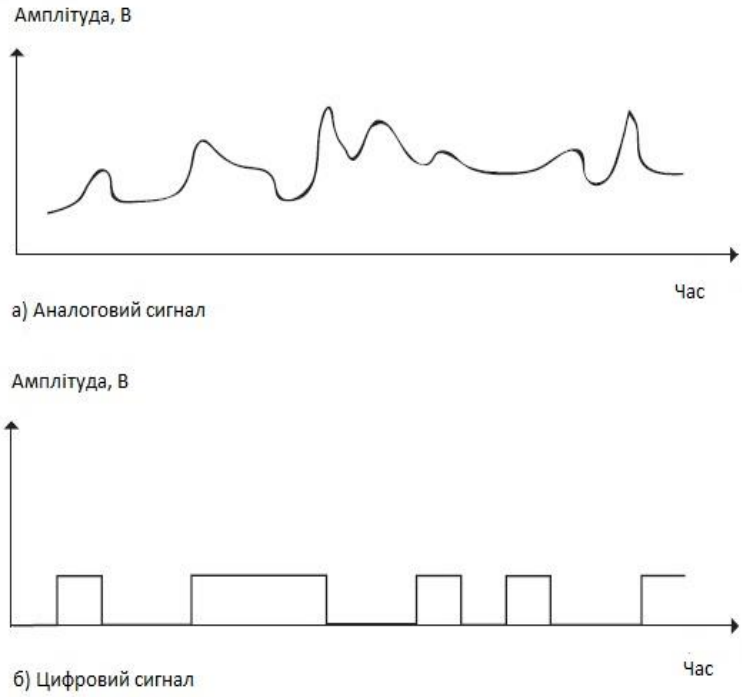


Рисунок 1.6 – Аналоговий і цифровий сигнали

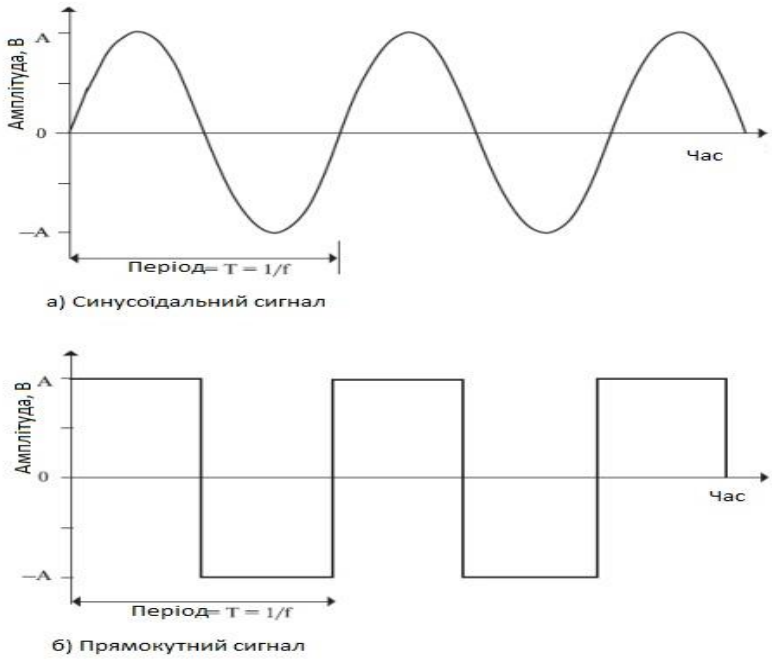


Рисунок 1.7 – Періодичні сигнали

Фундаментальним аналоговим сигналом є синусоїда. У загальному випадку такий сигнал можна визначити трьома параметрами: максимальною амплітудою *A*, частотою *f* та фазою *Ф*. *Максимальна амплітуда* – максимальне значення або інтенсивність сигналу в часі. Виміряється максимальна амплітуда, як правило, у вольтах. *Частотою* називається темп повторення сигналів (у періодах за секунду, або в герцах). *Еквівалентним параметром* є період сигналу *T*, який визначається як час, за який відбувається повторення сигналу; отже, *T=1/f*. *Фаза* є мірою відносного зрушення за часом у межах окремого періоду сигналу (даний термін буде розглянуто нижче).

У загальному випадку синусоїдальний сигнал можна представити в наступному вигляді:

$$s(t) = \mathrm{A}\sin(2\pi f t + \varphi)\,, \qquad (1.7)$$

Існує співвідношення між двома синусоїдальними сигналами, один з яких змінюється в часі, а інший – у просторі. Визначимо довжину хвилі сигналу λ як відстань, займану одним періодом або, іншими словами, як відстань між двома точками рівних фаз двох послідовних циклів. Припустимо, що сигнал поширюється зі швидкістю v. Тоді довжина хвилі пов'язана з наступним періодом співвідношенням: $\lambda = vT$, що рівносильне $\lambda f = v$. Особливе значення для нашого викладу має випадок, де $v = c$, де c – швидкість світла у вакуумі, яка приблизно рівна $3*10^8$ м/с. Застосувавши аналіз Фур'є, тобто склавши разом достатню кількість синусоїдальних сигналів з відповідними амплітудами, частотами й фазами, можна одержати електромагнітний сигнал будь-якої форми. Аналогічно, будь-який електромагнітний сигнал слід розглядати як сукупність періодичних аналогових (синусоїдальних) сигналів з різними амплітудами, частотами й фазами.

Спектром сигналу називається область частот, що становлять даний сигнал.

Цифровий сигнал можна виразити в такий спосіб:

$$s = \mathrm{A} \times \frac{4}{\pi} \sum_{k=1,3,5\ldots}^{\infty} \frac{\sin(2\pi k f t)}{\mathrm{k}}\,, \qquad (1.8)$$

де A – амплітуда, k – 1,3,5,…

Цей сигнал містить нескінченне число частотних компонент і, отже, має нескінченну ширину смуги.

Таким чином, можна зробити наступний висновок: у загальному випадку будь-який цифровий сигнал має нескінченну ширину смуги.

Якщо ми спробуємо передати цей сигнал через якесь середовище, передавальна система, накладе обмеження на ширину смуги, яку можна передати. Мало того, для кожного конкретного середовища справедливо наступне: чим більша передавальна смуга, тим більша вартість передачі. Тому, з одного боку, з економічних і практичних міркувань слід апроксимувати цифрову інформацію сигналом з обмеженою шириною смуги. З

іншого боку, при обмеженні ширини смуги виникають викривлення, що ускладнюють інтерпретацію прийнятого сигналу. Чим більше обмежена смуга, тим сильніше викривлення сигналу й тим більша потенційна можливість виникнення помилок при прийманні.

1.3.2. Передача даних

Будемо розуміти, що *дані* – це об'єкти, що передають зміст, або інформацію. *Сигнали* – це електромагнітне відображення даних. *Передача* – процес переміщення даних шляхом поширення сигналів по передавальному середовищу і їх обробки.

Поняття «аналогові дані» і «цифрові дані» досить прості. Аналогові дані приймають безперервні значення в межах певного діапазону. Наприклад, звукові та відеосигнали є безперервними змінними величинами. Цифрові дані, навпаки, приймають тільки дискретні значення; приклади – текст і цілі числа.

У системі зв'язку інформація поширюється від однієї точки до іншої за допомогою електричних сигналів. *Аналоговий сигнал* – безперервна мінлива електромагнітна хвиля, яка може поширюватися через безліч середовищ, залежно від частоти; як приклад таких середовищ можна назвати кабельні лінії, такі як: кручена пара й коаксіальний кабель, оптоволокно. Цей сигнал також може поширюватися через атмосферу або космічний простір. *Цифровий сигнал* являє собою послідовність імпульсів напруги, які можуть передаватися по дротовій лінії, при цьому постійний позитивний рівень напруги може використовуватися як двійкова одиниця, а постійний негативний рівень – двійковий нуль.

У бездротових технологіях використовуються як цифрові дані, так і аналогові сигнали, оскільки цифрові сигнали зазнають більшого загасання порівняно з аналоговими. Наприклад: Мова являє собою звукові хвилі й містить частотні компоненти в межах 70 Гц – 7,2 кГц. Однак, більша частина енергії мови перебуває в набагато вужчому діапазоні. Стандартний спектр мовних сигналів від 300 Гц до 3400 Гц, і цього діапазону цілком вистачає для розбірливої й чіткої передачі мови. Саме такий діапазон обробляє телефонний апарат. Усі звукові коливання в діапазоні

300-3400 Гц перетворяться в електромагнітний сигнал з подібними амплітудами й частотами. В іншому апараті виконується зворотний процес: електромагнітна енергія перетвориться у звук.

Цифрові дані можна представити аналоговими сигналами, застосувавши із цією метою модем (модулятор/демодулятор). Модем, або бездротовий адаптер перетворить послідовність двійкових (що мають два значення) імпульсів напруги в аналоговий сигнал, модулюючи їх опорною частотою. Отриманий сигнал займає певний спектр частот із центром на опорній частоті й може поширюватися в навколишнє середовище. На іншому кінці лінії інший модем або бездротовий адаптер демодулює сигнал і відновлює вихідні дані.

1.3.3. Пропускна здатність каналу

Існує безліч факторів, здатних спотворити або ушкодити сигнал. Найпоширеніші з них – перешкоди або шуми, що являти собою будь-який небажаний сигнал, який змішується із сигналом, призначеним для передачі або приймання, і спотворює його. Для цифрових даних виникає питання: наскільки ці викривлення обмежують можливу швидкість передачі даних? Максимально можлива за певних умов швидкість, при якій інформація може передаватися по конкретному тракту зв'язку, або каналу, називається *пропускною здатністю* каналу.

Існує чотири поняття, які ми спробуємо зв'язати воєдино:

– *швидкість передачі даних* – швидкість у бітах у секунду (біт/с), з якої можуть передаватися дані;

– *ширина смуги* – ширина смуги переданого сигналу, що обмежується передавачем і природою передавального середовища. Виражається в періодах у секунду, або герцах (Гц);

– *шум* – середній рівень шуму в каналі зв'язку;

– *рівень помилок* – частота появи помилок. Помилкою вважається приймання 1 при переданому 0 і навпаки.

Проблема полягає в наступному: засоби зв'язку недешеві й, у загальному випадку, чим ширша їх смуга, тем дорожче вони коштують. Мало того, всі канали передачі, що представляють практичний інтерес, мають обмежену ширину смуги. Обмеження

обумовлені фізичними властивостями передавального середовища або навмисними обмеженнями ширини смуги в самому передавачі, зробленими для запобігання інтерференції з іншими джерелами. Природно, є бажання максимально ефективно використовувати наявну смугу. Для цифрових даних це означає, що для певної смуги бажано одержати максимально можливу при наявному рівні помилок швидкість передачі даних. Але, на жаль, головним обмеженням при досягненні такої ефективності є перешкоди.

1.3.4. Методи доступу до середовища в бездротових мережах

Одна з основних проблем побудови бездротових систем – це розв'язання завдання доступу багатьох користувачів до обмеженого ресурсу середовища передачі. Існує декілька базових методів доступу (їх ще називають методами ущільнення або мультиплексування), заснованих на поділі між станціями таких параметрів, як простір, час, частота та код. Завдання ущільнення – виділити кожному каналу зв'язку простір, час, частоту й/або код з мінімумом взаємних перешкод і максимальним використанням характеристик передавального середовища.

Ущільнення із просторовим поділом засноване на поділі сигналів у просторі, коли передавач посилає сигнал, використовуючи код c, час t і частоту f області si. Тобто кожний бездротовий пристрій може вести передачу даних тільки в границях певної території, на якій будь-якому іншому пристрою заборонено передавати свої повідомлення.

Наприклад: якщо радіостанція віщає на строго певній частоті на закріпленій за нею територією, а яка-небудь інша станція в цій же місцевості також почне віщати на тій же частоті, слухачі радіопередач не зможуть одержати «чистий» сигнал ні від однієї із цих станцій. Інша справа, якщо радіостанції працюють на одній частоті в різних містах. Викривлень сигналів кожної радіостанції не буде у зв'язку з обмеженою дальністю поширення сигналів цих станцій, що виключає їхнє накладення один на одного.

Характерний приклад – системи стільникового зв'язку де присутнє ущільнення із частотним поділом (Frequency Division

Multiplexing – FDM). Кожний пристрій працює на певній частоті, завдяки чому кілька пристроїв можуть вести передачу даних на одній території (рис. 1.8). Це один з найбільш відомих методів, так чи інакше, використовуваний у найсучасніших системах бездротового зв'язку.

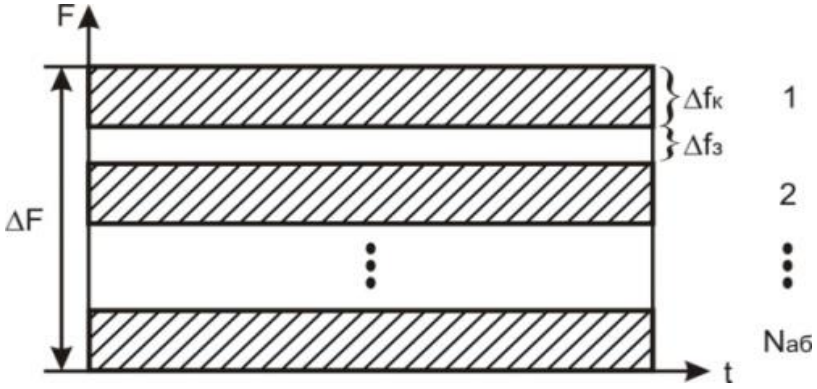


Рисунок 1.8 – Принцип частотного поділу каналів

Наочна ілюстрація схеми *частотного ущільнення* – функціонування в одному місті декількох радіостанцій, що працюють на різних частотах. Для надійної відстрочки однієї від другої їх робочі частоти повинні бути розділені захисним частотним інтервалом, який дозволяє виключити взаємні перешкоди.

Ця схема, хоча й дозволяє використовувати безліч пристроїв на певній території, але сама по собі призводить до невиправданого марнотратства звичайно вбогих частотних ресурсів, оскільки вимагає виділення своєї частоти для кожного бездротового пристрою.

Слід звернути увагу на ущільнення з тимчасовим поділом (Time Division Multiplexing – TDM). У даній схемі розподіл каналів іде за часом, тобто кожний передавач транслює сигнал на одній і тій же частоті f області s, але в різні проміжки часу t_i (як правило, що циклічно повторюються) при суворих вимогах до *синхронізації процесу* передачі (рис. 1.9).

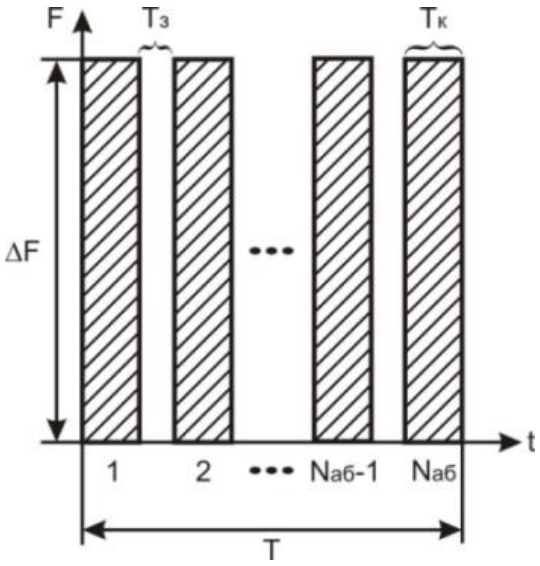


Рисунок 1.9 – Принцип часового розподілу каналів

Подібна схема досить зручна, тому що тимчасові інтервали можуть динамічно перерозподілятися між пристроями мережі. Пристроям з більшим трафіком призначаються більш тривалі інтервали, чим пристроям з меншим обсягом трафіка.

Основний недолік систем з тимчасовим ущільненням – це миттєва втрата інформації при зриві синхронізації в каналі, наприклад через сильні перешкоди, випадкові або навмисні. Проте, успішний досвід експлуатації таких знаменитих *TDM-систем*, як стільникові телефонні мережі стандарту *GSM*, свідчить про достатню надійність механізму тимчасового ущільнення.

Ущільнення з кодовим поділом (Code Division Multiplexing – CDM) передбачає, що у даній схемі всі передавачі транслюють сигнали на одній і тій же частоті f в області s і під час t, але з різними кодами заснованого на CDM механізмі поділу каналів (CDMA – CDM Access), навіть названий стандарт стільникового телефонного зв'язку IS-95a, а також ряд стандартів третього

покоління стільникових систем зв'язку (CDMA 2000, WCDMA та ін.).

У схемі CDM кожний передавач заміняє кожний біт вихідного потоку даних на *CDM – символ* – кодову послідовність довжиною в 11, 16, 32, 64 і т.п. біт (їх називають *чипами*). Кодова послідовність унікальна для кожного передавача. Як правило, якщо для заміни «1» у вихідному потоці даних використовують якийсь *CDM – код*, то для заміни «0» застосовують той же код, але інвертований.

Приймач знає *CDM – код* передавача, сигнали якого повинен сприймати. Він постійно сприймає всі сигнали й зацифровує їх. Потім у спеціальному пристрої (кореляторі) проводиться операція згортки (множення з нагромадженням) вхідного зацифрованого сигналу з відомим йому *CDM–кодом* і його інверсією. У трохи спрощеному вигляді – це операція *скалярного добутку вектора* вхідного сигналу й вектора з *CDM–кодом.* Якщо сигнал на виході корелятора перевищує якийсь установлений граничний рівень, приймач уважає, що прийняв 1 або 0. Для збільшення ймовірності приймання передавач повинен повторювати посилку кожного біта кілька раз. При цьому сигнали інших передавачів з іншими *CDM–кодами* приймач сприймає як адитивний шум. Мало того, завдяки великій надмірності (кожний біт заміняється десятками чипів), потужність прийнятого сигналу може бути порівнянна з інтегральною потужністю шуму. Подібності *CDM–сигналів* з випадковим (гауссовим) шумом домагаються, використовуючи *CDM–коди*, породжені генератором *псевдовипадкових послідовностей*. Тому даний метод ще називають *методом розширення спектра сигналу* за допомогою прямої послідовності (*DSSS* – Direct Sequence *Spread Spectrum*). Про розширення спектра буде розглянуто далі.

Найбільш потужна сторона даного ущільнення полягає в підвищеній захищеності й *прихованості* передачі даних: не знаючи коду, неможливо одержати сигнал, а в ряді випадків – і виявити його присутність. Крім того, кодовий простір незрівнянно більш значний в порівнянні із частотною схемою ущільнення, що дозволяє без особливих проблем привласнювати

кожному передавачу свій індивідуальний код. Основною ж проблемою кодового ущільнення донедавна була складність технічної реалізації приймачів і необхідність забезпечення точної синхронізації передавача й приймача для гарантованого одержання пакета.

Для подальшого розуміння методів доступу слід зупинитися на механізмі мультиплексування за допомогою ортогональних опорних частот (Orthogonal Frequency Division Multiplexing – OFDM). Суть цього механізму: увесь доступний частотний діапазон розбивається на досить багато підопорних частот (від кількох сотень до тисяч). Одному каналу зв'язку (приймачу й передавачу) призначають для передачі трохи таких опорних, обраних з безлічі за певним законом. Передача ведеться одночасно по всім підопорним частотам, тобто в кожному передавачу вихідний потік даних розбивається на N субпотоків, де N – число підопорних частот, що призначені даному передавачу.

Розподіл, підопорних частот у ході роботи може динамічно змінюватися, що робить даний механізм не менш гнучким, ніж метод часового ущільнення.

Схема OFDM має кілька переваг. По-перше, селективному завмиранню будуть піддані тільки деякі підканали, а не весь сигнал. Якщо потік даних захищений кодом прямого виправлення помилок, то із цим завмиранням легко боротися. По-друге, що більш важливо, OFDM дозволяє придушити міжсимвольну інтерференцію. Міжсимвольна інтерференція значно впливає при високих швидкостях передачі даних, тому що відстань між бітами (або символами) мала. У схемі OFDM швидкість передачі даних зменшується в N раз, що дозволяє побільшати час передачі символу в N раз. Таким чином, якщо час передачі символу для вихідного потоку становить Ts, де період сигналу *OFDM* буде рівний NTs. Це дозволяє суттєво знизити вплив міжсимвольних перешкод. При проєктуванні системи N вибирається таким чином, щоб величина NTs значно перевищувала середньоквадратичний розкид затримок каналу. Алгоритм формування сигналу OFDM див. у Додатку Е.

1.4. Технологія розширеного спектра

Споконвічно метод розширеного спектра створювався для розвідувальних і військових цілей. Основна ідея методу полягає в тому, щоб розподілити інформаційний сигнал по широкій смузі радіодіапазону, що в підсумку дозволить значно ускладнити придушення або перехоплення сигналу. Перша розроблена схема розширеного спектра відома як метод перебудови частоти. Більш сучасною схемою розширеного спектра є метод прямого послідовного розширення. Обидва методи використовуються в різних стандартах і продуктах бездротовому зв'язку.

Розширення спектра стрибкоподібною перебудовою частоти (Frequency Hopping Spread Spectrum – FHSS). Для того, щоб радіообмін не можна було перехопити або придушити вузькополосним шумом, було запропоновано звістки передачу з постійною зміною опорної в межах широкого діапазону частот. У результаті потужність сигналу розподілялася по всьому діапазону, і прослуховування якоїсь певної частоти давало тільки невеликий шум. Послідовність опорних частот була псевдовипадкової, відомої тільки передавачу й приймачу. Спроба придушення сигналу в якомусь вузькому діапазоні також не занадто погіршувала сигнал, тому що пригнічувалася тільки невелика частина інформації.

Ідею цього методу ілюструє рис. 1.10.

Протягом фіксованого інтервалу часу передача ведеться на незмінній опорній частоті. На кожній опорній частоті для передачі дискретної інформації застосовуються стандартні *методи модуляції*, такі як *FSK* або *PSK*. Для того, щоб приймач синхронізувався з передавачем, для позначення початку кожного періоду передачі протягом деякого часу передаються синхробіти. Так, що корисна швидкість цього методу кодування виявляється менша через постійні накладні витрати на синхронізацію.

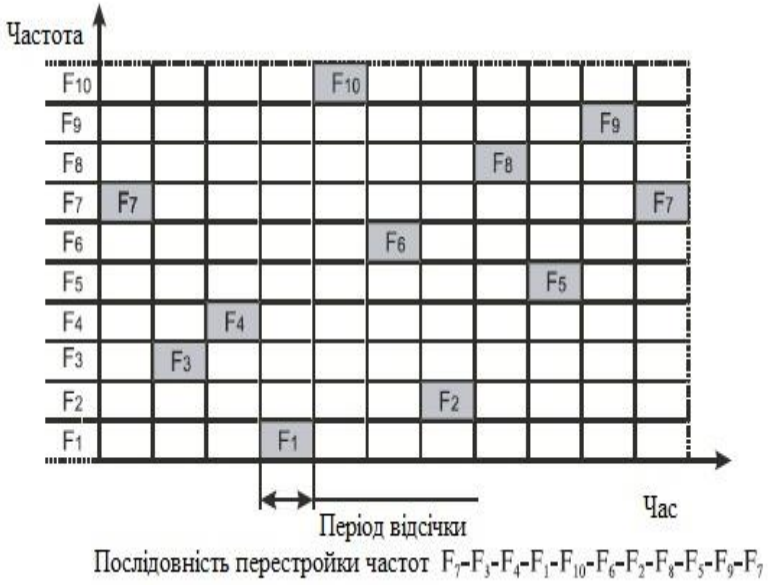


Рисунок 1.10 – Розширення спектра стрибкоподібною перебудовою частоти.

Опорна частота міняється відповідно до номерів частотних підканалів, вироблюваних алгоритмом псевдовипадкових чисел. Псевдовипадкова послідовність залежить від деякого параметра, який називають початковим числом. Якщо приймачу й передавачу відомі алгоритм і значення початкового числа, то вони міняють частоти в однаковій послідовності, яка називається послідовністю псевдовипадкової перебудови частоти.

Якщо частота зміни підканалів нижче, ніж швидкість передачі даних у каналі, то такий режим називають *повільним розширенням спектра* (рис. 1.11а); а якщо ні, то ми маємо справу зі *швидким розширенням спектра* (рис. 1.11б).

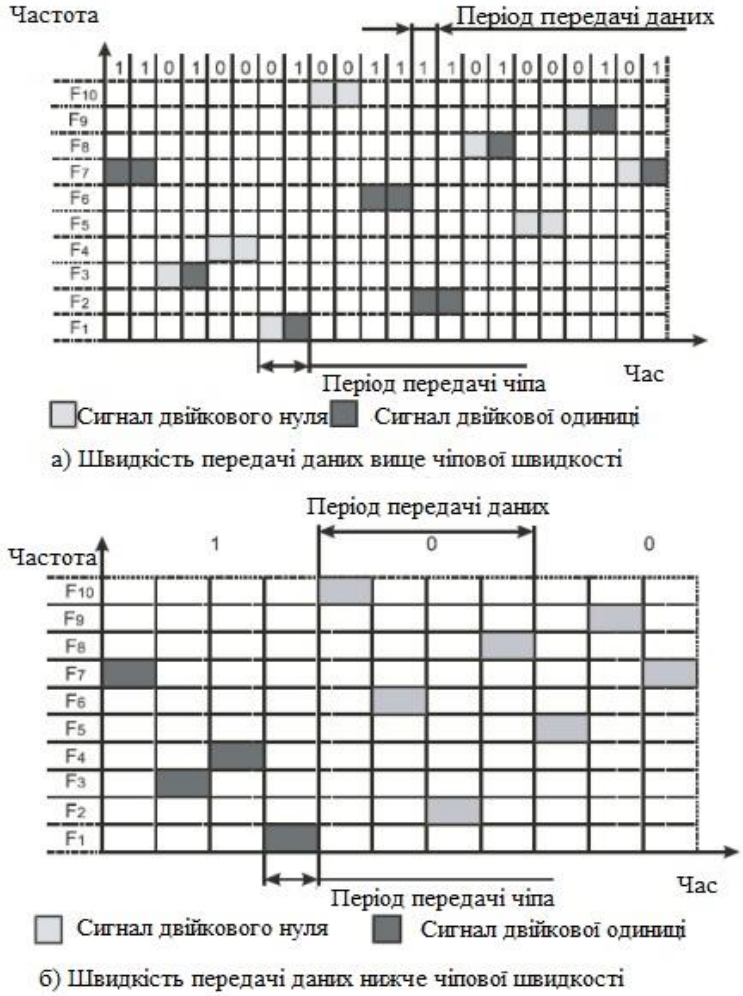


Рисунок 1.11 – Співвідношення між швидкістю передачі даних і частотою зміни підканалів

Метод швидкого розширення спектра більш стійкий до перешкод, оскільки вузькополосна перешкода, яка пригнічує сигнал у певному підканалі, не приводить до втрати біта, тому що його значення повторюється кілька раз у різних частотних

підканалах. У цьому режимі не проявляється ефект міжсимвольної інтерференції, тому що вчасно приходу затриманого уздовж одного зі шляхів сигналу система встигає перейти на іншу частоту.

Метод повільного розширення спектра такої властивістю не має, але він простіше в реалізації й сполучений з меншими накладними витратами.

В бездротових технологіях *IEEE 802.11* і *Bluetooth* використовуються Методи *FHSS*. У *FHSS* підхід до використання частотного діапазону не такий, як в інших методах кодування – замість ощадливої витрати вузької смуги робиться спроба зайняти весь доступний діапазон. На перший погляд, це може здаватися не дуже ефективним – адже в кожний момент часу в діапазоні працює тільки один канал. Однак останнє твердження не завжди слушне – коди розширеного спектра можна використовувати й для мультиплексування декількох каналів у широкому діапазоні. Зокрема, методи *FHSS* дозволяють організувати одночасну роботу декількох каналів шляхом вибору для кожного каналу таких *псевдовипадкових послідовностей*, щоб у кожний момент часу кожний канал працював на своїй частоті (звичайно, це можна зробити, тільки якщо число каналів не перевищує числа частотних підканалів).

У методі прямого послідовного розширення спектра (Direct Sequence Spread Spectrum – DSSS) також використовується весь частотний діапазон, виділений для однієї бездротової лінії зв'язку. На відміну від методу *FHSS*, увесь частотний діапазон займається не шляхом постійних перемикань із частоти на частоту, а шляхом того, що кожний біт інформації заміняється N-Бітами, так що тактова швидкість передачі сигналів збільшується в N раз. А це, своєю чергою, означає, що спектр сигналу також розширюється в N раз. Досить відповідним чином вибрати швидкість передачі даних і значення N, щоб спектр сигналу заповнив увесь діапазон.

Ціль кодування методом *DSSS* та ж, що й методом *FHSS*, – підвищення стійкості до перешкод. Вузькополосна перешкода буде спотворювати тільки певні частоти спектра сигналу, так що

приймач із великим ступенем імовірності зможе правильно розпізнати передану інформацію.

Код, яким заміняється двійкова одиниця вихідної інформації, називається *розширювальною послідовністю*, а кожний біт такої послідовності – чипом.

Відповідно, швидкість передачі результівний код називають *чіповою* швидкістю. Двійковий нуль кодується інверсним значенням розширювальної послідовності. Приймачі повинні знати розширювальну послідовність, яку використовує передавач, щоб зрозуміти передану інформацію.

Кількість бітів у розширювальній послідовності визначає коефіцієнт розширення вихідного коду. Як і у випадку *FHSS*, для кодування бітів результативного коду може використовуватися будь-який вид модуляції, наприклад *BFSK*.

Чим більше коефіцієнт розширення, тем ширше спектр результативного сигналу й вище ступінь придушення перешкод. Але, при цьому росте займаний каналом діапазон спектра. Звичайно коефіцієнт розширення має значення від 10 до 100.

Дуже часто в якості значення розширювальної послідовності беруть послідовність Баркера (Barker), яка складається з 11 біт: 10110111000. Якщо передавач використовує цю послідовність, то передача трьох бітів 110 веде до передачі наступних бітів:

10110111000 10110111000 01001000111.

Послідовність Баркера дозволяє приймачу швидко синхронізуватися з передавачем, тобто надійно виявляти початок послідовності. Приймач визначає таку подія, по черзі порівнюючи одержувані біти зі зразком послідовності. Дійсно, якщо зрівняти послідовність Баркера з такою ж послідовністю, але зрушеної на один біт уліво або вправо, ми одержимо менше половини збігів значень бітів. Виходить, навіть при викривленні декількох бітів з великою часткою ймовірності приймач правильно визначить початок послідовності, а виходить, зможе правильно інтерпретувати одержувану інформацію.

Метод *DSSS* меншою мірою захищений від перешкод, ніж метод швидкого розширення спектра, тому що потужна вузькополосна перешкода впливає на частину спектра, а

виходить, і на результат розпізнавання одиниць або нулів (рис. 1.12).

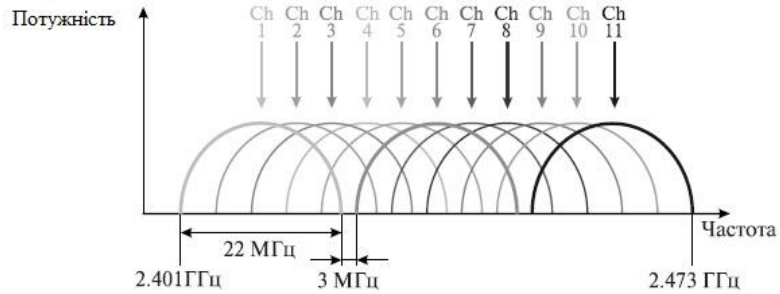


Рисунок 1.12 – Канали, використовувані в технології DSSS

Бездротові локальні мережі *DSSS* використовують канали шириною 22 МГц, завдяки чому багато *WLAN* можуть працювати в одній і тій же зоні покриття. У Північній Америці й більш частин Європи, у тому числі й у Росії, канал шириною 22 МГц дозволяє створи у діапазон 2,4–2,473 ГГц, канали, що не перекриваються. Ці канали показані на рис. 1.12.

1.5. Кодування й захист від помилок

Існує три найпоширеніші знаряддя боротьби з помилками в процесі передачі даних:

- коди виявлення помилок;
- коди з корекцією помилок, називані також схемами прямої корекції помилок (Forward *Error Correction – FEC*);
- протоколи з автоматичним запитом повторної передачі (*Automatic Repeat Request – ARQ*).

Код виявлення помилок дозволяє досить легко встановити наявність помилки. Як правило, подібні коди використовуються разом з певними протоколами канального або транспортного рівнів, що мають схему *ARQ*. У схемі *ARQ* приймач попросту відхиляє блок даних, у якому була виявлена помилка, після чого

передавач передає цей блок повторно. Коди із прямою корекцією помилок дозволяють не тільки виявити помилки, але й виправити їх, не прибігаючи до повторної передачі. Схеми *FEC* часто використовуються в бездротовій передачі, де повторна передача вкрай неефективна, а рівень помилок досить високий.

1) Методи виявлення помилок

Методи виявлення помилок засновані на передачі в складі блоку даних надлишкової службової інформації, по якій можна судити з деяким ступенем імовірності про вірогідність прийнятих даних.

Надлишкову службову інформацію заведено називати контрольною сумою, або контрольною послідовністю кадра (*Frame Check Sequence – FCS*). Контрольна сума обчислюється як функція від основної інформації, причому не обов'язково шляхом підсумовування. Сторона, що ухвалює, повторно обчислює контрольну суму кадра по відомому алгоритму й у випадку її збігу з контрольною сумою, обчисленою передавальною стороною, робить висновок про те, що дані були передані через мережу коректно. Розглянемо кілька розповсюджених алгоритмів обчислення контрольної суми, що відрізняються обчислювальною складністю й здатністю виявляти помилки в даних.

Контроль по паритету являє собою найбільш простий метод контролю даних. Водночас, це найменш потужний алгоритм контролю, тому що з його допомогою можна виявити тільки одиничні помилки в даних, що перевіряються. Метод полягає в підсумовуванні по модулю 2 усіх бітів контрольованої інформації. Неважко помітити, що для інформації, що полягає з непарного числа одиниць, контрольна сума завжди рівна 1, а при парному числі одиниць – 0. Наприклад, для даних 100101011 результатом контрольного підсумовування буде значення 1. Результат підсумовування також являє собою один додатковий біт даних, який пересилається разом з контрольованою інформацією. При викривленні в процесі пересилання будь-якого біта вихідних даних (або контрольного розряду) результат підсумовування буде відрізнятися від прийнятого контрольного розряду, що говорить про помилку. Однак подвійна помилка,

наприклад 110101010, буде невірно прийнята за коректні дані. Тому контроль по паритету застосовується до невеликих порцій даних, як правило, до кожного байта, що дає коефіцієнт надмірності для цього методу 1/8. Метод рідко застосовується в комп'ютерних мережах через значну надмірність і невисоку діагностичну здатність.

Вертикальний і горизонтальний контроль по паритету являє собою модифікацію описаного вище методу. Його відмінність полягає в тому, що вихідні дані розглядаються у вигляді матриці, рядка якої становлять байти даних. Контрольний розряд підраховується окремо для кожного рядка й для кожного стовпця матриці. Цей метод виявляє значну частину подвійних помилок, однак має ще більшу надмірність. Він зараз також майже не застосовується при передачі інформації з мережі.

Циклічний надлишковий контроль (*Cyclic Redundancy Check – CRC*) є в цей час найбільш популярним методом контролю в обчислювальних мережах (і не тільки в мережах; зокрема, цей метод широко застосовується при записі даних на гнучкі й жорсткі диски). Метод заснований на розгляді вихідних даних у вигляді одного багаторозрядного двійкового числа. Наприклад, кадр стандарту Ethernet, що полягає з 1024 байт, буде розглядатися як одне число, що полягає з 8192 біт. Контрольною інформацією вважається залишок від розподілу цього числа на відомий дільник R. Звичайно в якості дільника вибирається сімнадцяти або трдцятитрьохрозрядне число, щоб залишок від розподілу мав довжину 16 розрядів (2 байта) або 32 розряду (4 байта). При одержанні кадра даних знову обчислюється залишок від розподілу на той же дільник R, але при цьому до даних кадра додається контрольна сума, що й утримується в ньому. Якщо залишок від розподілу на R дорівнює нулю, то робиться висновок про відсутність помилок в отриманому кадрові, а якщо ні, то кадр уважається перекрученим.

Цей метод має більш високу обчислювальну складність, але його діагностичні можливості набагато ширше, чим у методів контролю по паритету. Метод *CRC* виявляє всі одиничні помилки, подвійні помилки й помилки в непарному числі бітів. Метод також має невисокий ступінь надмірності. Наприклад, для

кадра Ethernet розміром 1024 байти контрольна інформація довжиною 4 байти становить тільки 0,4 %.

2) Методи корекції помилок

Техніка кодування, яка дозволяє приймачу не тільки зрозуміти, що прислані дані містять помилки, але й виправити їх, називається прямою корекцією помилок (Forward *Error Correction – FEC*). Коди, що забезпечують пряму корекцію помилок, вимагають уведення більшої надмірності в передані дані, чому коди, які тільки виявляють помилки.

При застосуванні будь-якого надлишкового коду не всі комбінації кодів є дозволеними. Наприклад, контроль по паритету робить дозволеними тільки половину кодів. Якщо ми контролюємо три інформаційні біти, то дозволеними 4-бітними кодами з доповненням до непарної кількості одиниць будуть:

000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0, тобто всього 8 кодів з 16 можливих.

Для того, щоб оцінити кількість додаткових бітів, необхідних для виправлення помилок, потрібно знати так звану відстань Хемминга між дозволеними комбінаціями коду. Відстанню Хемминга називається мінімальне число бітових розрядів, у яких відрізняється будь-яка пара дозволених кодів. Для схем контролю по паритету відстань Хемминга дорівнює 2.

Можна довести, що якщо ми сконструювали надлишковий код з відстанню Хемминга, рівним n, такий код може розпізнавати (n-1)-кратні помилки й виправляти (n-1)/2-кратні помилки. Тому що коди з контролем по паритету мають відстань Хемминга, рівне 2, вони можуть тільки виявляти однократні помилки й не можуть виправляти їх.

Коди Хемминга ефективно виявляють і виправляють ізольовані помилки, тобто окремі перекручені біти, які розділені більшою кількістю коректних бітів. Однак з появою довгої послідовності перекручених бітів (пульсації помилок) коди Хемминга не працюють.

Найбільше часто в сучасних системах зв’язку застосовується тип кодування, реалізований надточним пристроєм, що кодує (*Convolutional* coder), тому що таке кодування нескладне реалізувати апаратно з використанням ліній затримки *(*delay) і

суматорів. На відміну від розглянутого вище коду, який ставиться до блокових код без пам'яті, згорткове кодування ставиться до коду з кінцевою пам'яттю (*Finite* memory code); це означає, що вихідна послідовність *кодера* є функцією не тільки поточного вхідного сигналу, але також декількох з-поміж останніх попередніх бітів. Довжина кодового обмеження (*Constraintlength* of a code) показує, як багато вихідних елементів виходить із системи в перерахуванні на один вхідний. Коди часто характеризуються їхнім ефективним ступенем (або коефіцієнтом) кодування (Code rate). Вам може зустрітися згортковий код з коефіцієнтом кодування 1/2. Цей коефіцієнт указує, що на кожний вхідний біт доводиться два вихідні. Порівнюючи коди звертайте увагу на те, що, хоча коди з більш високим ефективним ступенем кодування дозволяють передавати дані з більш високою швидкістю, вони, відповідно, більш чутливі до шуму.

У бездротових системах із блоковими кодами широко використовується метод чергування блоків. Перевага чергування полягає в тому, що приймач розподіляє пакет помилок, що спотворив деяку послідовність бітів, по великій кількості блоків, завдяки чому стає можливим виправлення помилок. Чергування виконується за допомогою читання й записи даних у різному порядку. Якщо під час передачі пакет перешкод впливає на деяку послідовність бітів, то всі ці біти виявляються рознесеними по різних блоках. Отже, від будь-якої контрольної послідовності потрібна можливість виправити лише невелику частину від загальної кількості інвертованих бітів.

3) Методи автоматичного запиту повторної передачі

У найпростішому випадку захист від помилок полягає тільки в їхнім виявленні. Система повинна попередити передавач про виявлення помилки й необхідності повторної передачі. Такі процедури захисту від помилок відомі як методи автоматичного запиту повторної передачі (*Automatic Repeat Request – ARQ*). У бездротових локальних мережах застосовується процедура «запит *ARQ* із зупинками» (stop-and-wait *ARQ*).

У цьому випадку джерело, що послало кадр, очікує одержання підтвердження (Acknowledgement – ACK), або, як ще

його називають, квитанції, від приймача й тільки після цього посилає наступний кадр. Якщо ж підтвердження не приходить протягом тайм-ауту, то кадр (або підтвердження) вважається загубленим і його передача повторюється. На рис. 1.13 видно, що в цьому випадку продуктивність обміну даними нижче потенційно можливої, хоча передавач і міг би послати наступний кадр відразу ж після відправлення попереднього, він зобов'язаний чекати приходу підтвердження.

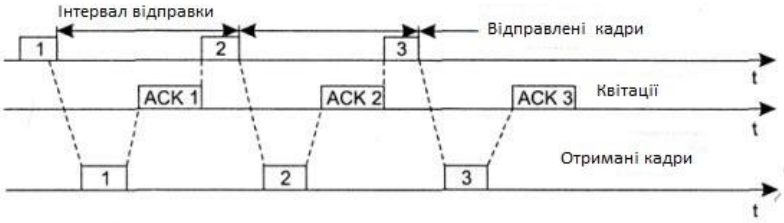


Рисунок 1.13 – Процедура запит ARQ із зупинками

2. АРХІТЕКТУРА IEEE 802.11

Інститут інженерів по електротехніці й електроніці IEEE (Institute of Electrical and Electronics Engineers) сформував робочу групу по стандартах для бездротових локальних мереж 802.11 в 1990 році. Ця група зайнялася розробкою загального стандарту для радіоустаткування й мереж, що працюють на частоті 2,4 ГГц, зі швидкостями доступу 1 і 2 Мбит/с. Роботи зі створення стандарту були завершені через 7 років, і в червні 1997 року була ратифікована перша специфікація 802.11.

Стандарт IEEE 802.11 був першим стандартом для продуктів WLAN від незалежної міжнародної організації, що розробляє більшість стандартів для провідних мереж.

У цьому підрозділі буде розглянута архітектура самого популярного стандарту бездротових локальних мереж – *IEEE 802.11*, а в наступному підрозділі мова піде про найбільш популярні стандарти: *IEEE 802.11a, IEEE 802.11b* і *IEEE 802.11g*.

2.1. Стек протоколів IEEE 802.11

Природно, стек протоколів стандарту *IEEE 802.11* відповідає загальній структурі стандартів комітету 802, тобто складається з фізичного рівня й канального рівня з підрівнями керування доступом до середовища MAC (*Media Access Control*) і логічної передачі даних *LLC* (*Logical Link Control*). Як і у всіх технологій сімейства 802, технологія 802.11 визначається двома нижніми рівнями, тобто фізичним рівнем і рівнем MAC, а рівень *LLC* виконує свої стандартні загальні для всіх технологій LAN функції (рис. 2.1).

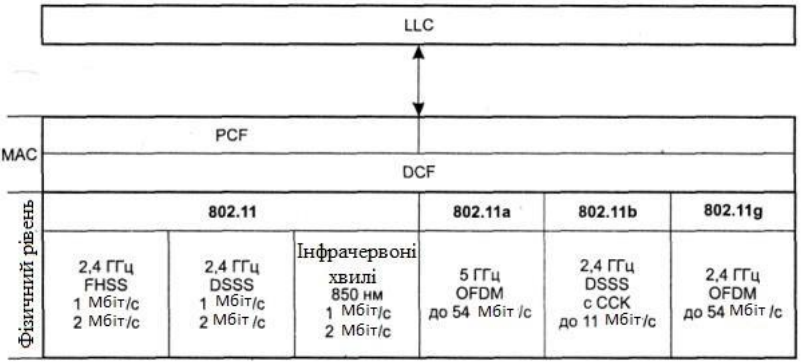


Рисунок 2.1 – Стек протоколів IEEE 802.11

На фізичному рівні існує кілька варіантів специфікацій, які відрізняються використовуваним частотним діапазоном, методом кодування і як наслідок – швидкістю передачі даних. Усі варіанти фізичного рівня працюють із тим самим алгоритмом рівня MAC, але деякі тимчасові параметри рівня MAC залежать від використовуваного фізичного рівня.

2.2. Рівень доступу до середовища стандарту 802.11

У мережах 802.11 рівень MAC забезпечує два режими доступу до *поділюваного середовища* (рис. 2.1):

- розподілений режим *DCF* (Distributed Coordination Function);
- централізований режим PCF (Point Coordination Function).

2.2.1. Розподілений режим доступу DCF

Розглянемо спочатку, як забезпечується доступ у розподіленому режимі *DCF*. У цьому режимі реалізується метод *множинного доступу з контролем опорної частоти й запобіганням колізій* (*Carrier Sense Multiple Access* with *Collision Avoidance* – *CSMA*/CA). Замість неефективного в бездротових мережах прямого розпізнавання колізій по методу *CSMA*/CD тут використовується їхнє непряме виявлення. Для цього кожний

переданий кадр повинен підтверджуватися кадром позитивної квитанції, що посилають станцією призначення. Якщо ж після закінчення застереженого тайм-ауту квитанція не надходить, станція-відправник вважає, що відбулася колізія.

Режим доступу DCF вимагає синхронізації станцій. У специфікації 802.11 ця проблема вирішується досить елегантно - тимчасові інтервали починають відлічуватися від моменту закінчення передачі чергового кадра (рис. 2.2).

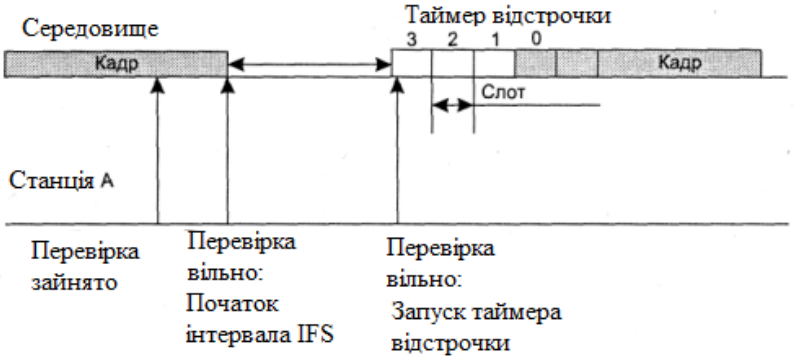


Рисунок 2.2 – Режим доступу DCF

Це не вимагає передачі яких-небудь спеціальних синхронувальних сигналів і не обмежує *розмір пакета* розміром слота, тому що слоти беруться до уваги тільки при ухваленні рішення про початок передачі кадра.

Станція, яка прагне передати кадр, зобов'язана попередньо прослухати середовище. Стандарт *IEEE 802.11* передбачає два механізми контролів активності в каналі (виявлення опорної): *фізичний і віртуальний*. Перший механізм реалізований на фізичному рівні й зводиться до визначення рівня сигналу в антені й порівнянню його із граничною величиною. Віртуальний механізм виявлення опорної заснований на тому, що в переданих кадрах даних, а також у керуючих кадрах ACK і *RTS*/*CTS* присутня інформація про час, необхідний для передачі пакета (або групи пакетів) і отримання підтвердження. Усі пристрої мережі одержують інформацію про поточну передачу й можуть

визначити, скільки часу канал буде зайнятий, тобто пристрій при встановленні зв'язку повідомляє всім, на який час воно резервує канал. Як тільки станція фіксує закінчення передачі кадра, вона зобов'язана відрахувати інтервал часу, рівний міжкадровому інтервалу (IFS). Якщо після витікання IFS середовище усе ще вільне, починається відлік слотів фіксованої тривалості. Кадр можна передавати тільки на початку якого-небудь зі слотів за умови, що середовище вільне. Станція вибирає для передачі слот на підставі усіченого експонентного двійкового алгоритму відстрочки, аналогічного використовуваному в методі *CSMA*/CD. Номер слота вибирається як випадкове ціле число, рівномірно розподілене в інтервалі [0, CW], де «CW» означає «Competition Window» (конкурентне вікно).

Розглянемо цей досить непростий метод доступу на прикладі Рисунка 2.3 Нехай станція А вибрала для передачі на підставі усіченого експонентного двійкового алгоритму відстрочки слот 3. При цьому вона привласнює таймеру відстрочки (призначення якого буде ясно з подальшого опису) значення 3 і починає перевіряти стан середовища на початку кожного слота. Якщо середовище вільне, то зі значення таймера відстрочки віднімається 1, і якщо результат дорівнює нулю, починається передача кадра.

Таким чином, забезпечується умова незайнятості всіх слотів, включаючи обраний. Ця умова є необхідною для початку передачі.

Якщо ж на початку якого-небудь слота середовище виявляється зайнятий, то вирахування одиниці не відбувається, і таймер «заморожується». У цьому випадку станція починає новий цикл доступу до середовища, змінюючи тільки алгоритм вибору слота для передачі. Як і в попередньому циклі, станція стежить за середовищем і при її звільненні робить паузу протягом міжкадрового інтервалу. Якщо середовище залишилося вільної, то станція використовує значення «замороженого» таймера як номера слота й виконує описану вище процедуру перевірки вільних слотів з вирахуванням одиниць, починаючи із замороженого значення таймера відстрочки.

Розмір слота залежить від способу кодування сигналу; так, для методу *FHSS* розмір слота рівний 28 мкс, а для методу *DSSS* – 1 мкс. Розмір слота вибирається таким чином, щоб він перевершував час поширення сигналу між будь-якими двома станціями мережі плюс час, затрачуване станцією на розпізнавання зайнятості середовища. Якщо така умова дотримується, то кожна станція мережі зуміє правильно розпізнати початок передачі кадра при прослуховуванні слотів, що передують обраному нею для передачі слота. Це, своєю чергою, означає наступне.

Колізія може мати місце тільки в тому випадку, коли кілька станцій вибирають той самий слот для передачі.

У цьому випадках кадри спотворюються, і квитанції від станцій призначення не приходять. Не одержавши протягом певного часу квитанцію, відправники фіксують факт колізії й намагаються передати свої кадри знову. При кожній повторній невдалій спробі передачі кадра інтервал [0, CW], з якого вибирається номер слота, подвоюється. Якщо, наприклад, початковий розмір вікна обраний рівним 8 (тобто CW = 7), те після першої колізії розмір вікна повинен бути рівний 16 (CW = 15), після другої послідовної колізії - 32 і т.д. Початкове значення CW, відповідно достандарту 802.11, повинне вибиратися залежно від типу фізичного рівня, використовуваного в бездротовій локальній мережі.

Як і в методі *CSMA*/CD, у даному методі кількість невдалих спроб передачі одного кадра обмежене, але стандарт 802.11 не дає точного значення цієї верхньої межі. Коли верхня межа в N спроб досягнута, кадр відкидається, а лічильник послідовних колізій установлюється в нуль. Цей лічильник також установлюється в нуль, якщо кадр після деякої кількості невдалих спроб все-таки передається успішно.

У бездротових мережах можлива ситуація, коли два пристрої (А й В) вилучені й не чують один одного, однак обоє попадають у зону обхвату третього пристрою З (рис. 2.3) – так звана проблема схованого термінала. Якщо обоє пристрою А й В почнуть передачу, то вони принципово не зможуть виявити конфліктну ситуацію й визначити, чому пакети не проходять.

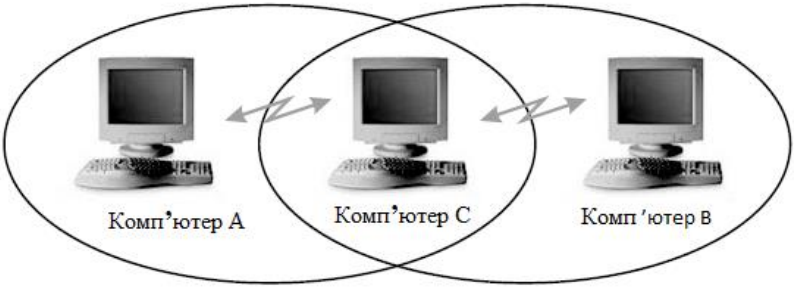


Рисунок 2.3 – Проблема схованого термінала

У режимі доступу *DCF* застосовуються заходом для усунення ефекту схованого термінала. Для цього станція, яка прагне захопити середовище й відповідно до описаного алгоритму починає передачу кадра в певному слоту, замість кадра даних спочатку посилає станції призначення короткий службовий кадр *RTS* (Request To Send – запит на передачу). На цей запит станція призначення повинна відповісти службовим кадром *CTS* (Clear To Send – вільна для передачі), після чого станція-відправник посилає кадра даних. Кадр *CTS* повинен сповістити про захоплення середовища ті станції, які перебувають поза зоною сигналу станції-відправника, але в зоні досяжності станції-одержувача, тобто є схованими терміналами для станції-відправника.

Максимальна довжина кадра даних 802.11 рівна 2346 байтів, довжина Rts-*Кадра* – 20 байтів, Cts-*Кадра* – 14 байтів. Тому, що *RTS*- і Cts-*Кадри* набагато коротше, ніж кадр даних, втрати даних у результаті колізії *RTS*- або Cts-*Кадрів* набагато менше, чим при колізії кадрів даних. Процедура обміну *RTS*- і Cts-*Кадрами* не обов'язкова. Від неї можна відмовитися при невеликому навантаженні мережі, оскільки в такій ситуації колізії трапляються рідко, а виходить, не варто витрачати додатковий час на виконання процедури обміну *RTS*- і Cts-*Кадрами*.

При перешкодах іноді трапляється, що губляться більші фрейми даних, тому можна зменшити довжину цих фреймів шляхом *фрагментації*. Фрагментація фрейму – це виконувана на

рівні MAC функція, призначення якої – підвищити надійність передачі фреймів через бездротове середовище. Під фрагментацією розуміється дроблення фрейму на менші фрагменти й передача кожного з них окремо (рис. 2.4).

Передбачається, що ймовірність успішної передачі меншого фрагмента через зашумлене бездротове середовище вище. Одержання кожного фрагмента фрейму підтверджується окремо; отже, якщо який-небудь фрагмент фрейму буде переданий з помилкою або вступить у колізію, передавати повторно прийде тільки його, а не весь фрейм. Це збільшує пропускну здатність середовища.

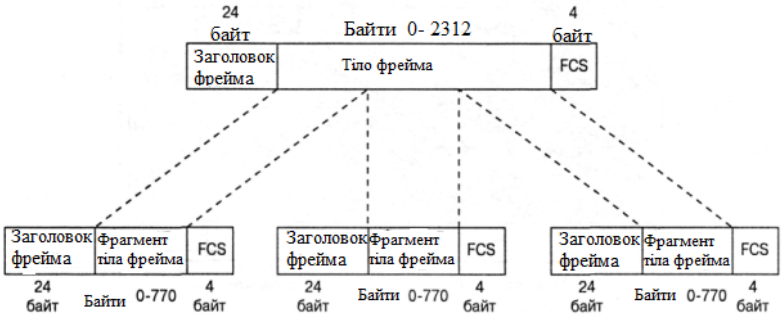


Рисунок 2.4 – Фрагментація фрейму

Розмір фрагмента може задавати адміністратор мережі. Фрагментації зазнають тільки одноадресні фрейми. Широкомовні, або багатоадресні, фрейми передаються цілком. Крім того, фрагменти фрейму передаються пакетом, з використанням тільки однієї ітерації механізму доступу до середовища *DCF*.

Хоча внаслідок фрагментації можна підвищити надійність передачі фреймів у бездротових локальних мережах, вона приводить до збільшення «накладних витрат» MAC-Протоколу стандарту 802.11. Кожний фрагмент фрейму включає інформацію, що втримується в заголовку 802.11 MAC, а також вимагає передачі відповідного фрейму підтвердження. Це збільшує число службових сигналів MAC-Протоколу й знижує реальну продуктивність бездротової станції. Фрагментація – це

баланс між надійністю й непродуктивним завантаженням середовища.

2.2.2. Централізований режим доступу PCF

У тому випадку, коли в мережі є станція, що виконує функції точка доступу, може також застосовуватися централізований режим доступу PCF, що забезпечує пріоритетне обслуговування трафіка. У цьому випадку говорять, що точка доступу відіграє роль арбітра середовища.

Режим доступу PCF у мережах 802.11 співіснує з режимом DCF. Обоє режимів координуються за допомогою трьох типів міжкадрових інтервалів (рис. 2.5).

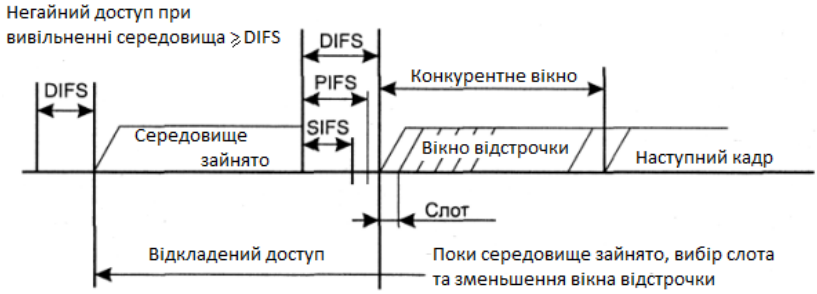


Рисунок 2.5 – Співіснування режимів PCF і DCF

Після звільнення середовища кожна станція відраховує час простою середовища, порівнюючи його із трьома значеннями:

- короткий міжкадровий інтервал (Short IFS – *SIFS*);
- міжкадровий інтервал режиму PCF (*PIFS*);
- міжкадровий інтервал режиму *DCF* (*DIFS*).

Захват середовища за допомогою розподіленої процедури *DCF* можливий тільки в тому випадку, коли середовище вільне протягом часу, рівного або більшого, ніж *DIFS*. Тобто в якості IFS у режимі *DCF* потрібно використовувати інтервал *DIFS* – самий тривалий період із трьох можливих, що дає цьому режиму найнижчий пріоритет.

Міжкадровий інтервал *SIFS* має найменше значення, він служить для першочергового захвата середовища відповідними Cts-*Кадрами* або квитанціями, які продовжують або завершують передачу, що вже почався, кадра.

Значення між кадрового інтервалу *PIFS* більше, чим *SIFS,* але менше, чим *DIFS*. Проміжком часу між завершенням *PIFS* і *DIFS* використовується арбітр середовища. У цьому проміжку він може передати спеціальний кадр, який говорить усім станціям, що починається контрольований період. Одержавши цей кадр, станції, які прагнули б скористатися алгоритмом *DCF* для захвату середовища, уже не можуть цього зробити, вони повинні чекати закінчення контрольованого періоду. Його тривалість оголошується в спеціальному кадрові, але цей період може закінчитися й раніше, якщо в станцій немає чутливого до затримок трафіка. У цьому випадку арбітр передає службовий кадр, після якого після закінчення інтервалу *DIFS* починає працювати режим *DCF*.

На керованому інтервалі реалізується *централізований метод* доступу PCF. Арбітр виконує процедуру опитування, щоб по черзі надати кожної такій станції право на використання середовища, направляючи їй спеціальний кадр. Станція, одержавши такого кадра, може відповісти іншим кадром, який підтверджує приймання спеціального кадра й одночасно передає дані (або за адресою арбітра для транзитної передачі, або безпосередньо станції).

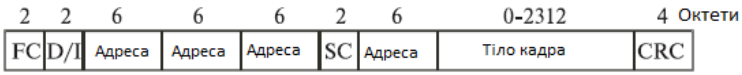
Для того, щоб якась частка середовища завжди діставалася асинхронному трафіку, тривалість контрольованого періоду обмежена. Після його закінчення арбітр передає відповідний кадр й починається неконтрольований період.

Кожна станція може працювати в режимі PCF, для цього вона повинна підписатися на дану послугу при приєднанні до мережі.

2.3. Кадр MAC-підрівня

На рис. 2.6 зображений формат кадра 802.11. Наведена загальна структура застосовується для всіх інформаційних і

керуючих кадрів, хоча не всі поля використовуються у всіх випадках.



FC — Управління кадром
D/I — Ідентифікатор довжини / з'єднання
SC — Керування чергою

Рисунок 2.6 – Формат кадра MAC IEEE 802.11

Перелічимо поля загального кадра:

- Керування кадром. Вказується тип кадра й надається керуюча інформація (пояснюється нижче).
- Ідентифікатор тривалості/з'єднання. Якщо використовується поле тривалості, вказується час (у мікросекундах), на який потрібно виділити канал для успішної передачі кадра MAC. У деяких кадрах керування в цім полі вказується ідентифікатор асоціації або з'єднання.
- Адреси. Число й значення полів адреси залежить від контексту. Можливі наступні типи адреси: джерела, призначення станції, що передає, ухвалює станції.
- Керування черговістю. Містить 4-бітове Підполе номера фрагмента, використовуване для фрагментації й повторного складання, і 12-бітовий порядковий номер, використовуваний для нумерації кадрів, переданих між приймачем і передавачем.
- Тіло кадра. Містить модуль даних протоколу LLC або керуючу інформацію MAC.
- Контрольна послідовність кадр а. 32-бітова перевірка парності з надмірністю.

Поле керування кадром, показане на рис. 2.7, складається з наступних полів:

- Версія протоколу. Версія 802.11 версія, що тече, – 0.

Таблиця 2.1 – Дозволені комбінації типу й підтипу

Значення типу	Опис типу	Значення підтипу	Опис підтипу
00	Керування	0000	Запит асоціації
00	Керування	0001	Відповідь на запит асоціації
00	Керування	0010	Запит повторної асоціації
00	Керування	0011	Відповідь на запит повторної асоціації
00	Керування	0100	Пробний запит
00	Керування	0101	Відповідь на пробний запит
00	Керування	1000	Сигнальний кадр
00	Керування	1001	Оголошення наявності трафіка
00	Керування	1010	Розрив асоціації
00	Керування	1011	Автентифікація
00	Керування	1100	Скасування автентифікації
01	Контроль	1010	Ps-запит
01	Контроль	1011	Запит передачі
01	Контроль	1100	«Готовий до передачі»
01	Контроль	1101	Підтвердження
01	Контроль	1110	Без змагання (CF)-кінець
01	Контроль	1111	Cf-кінець + Cf-підтвердження
10	Дані	0000	Дані
10	Дані	0001	Дані + Cf-підтвердження
10	Дані	0010	Дані + Cf-запит
10	Дані	0011	Дані + Cf-підтвердження + Cf-опитування
10	Дані	0100	Нульова функція (без даних)
10	Дані	0101	Дані + Cf-підтвердження
10	Дані	0110	Дані + Cf-запит
10	Дані	0111	Дані + Cf-підтвердження + Cf-запит

- Тип. Визначимо тип кадра: контроль, керування або дані.
- Підтип. Подальша ідентифікація функцій кадра. Дозволені комбінації типів і підтипів перераховано в таблиці 2.1.

– ДО DS. Координаційна функція MAC привласнює цьому біту значення 1, якщо кадр призначений розподільній системі.

– Від DS. Координаційна функція MAC привласнює цьому біту значення 0, якщо кадр виходить від розподільної системи.

– Більше фрагментів. 1, якщо за даним фрагментом випливає ще трохи.

– Повтор. 1, якщо даний кадр є повторною передачею попереднього.

– Керування потужністю. 1, якщо передавальна станція перебуває в режимі очікування.

– Більше даних. Указує, що станція передала не всі дані. Кожний блок даних може передаватися як один кадр або як група фрагментів у декількох кадрах.

– WEP. 1, якщо реалізований алгоритм конфіденційності провідного еквівалента (Wired Equivalent Privacy – WEP). Протокол WEP використовується для обміну ключами шифрування при безпечному обміні даними.

– Порядок. 1, якщо використовується послуга строгого впорядкування, що вказує адресатові, що кадри повинні оброблятися строго один по одному.

Рисунок 2.7 – Поле керування кадром

2.4. Типи кадрів MAC

2.4.1. Контрольні кадри

Контрольні кадри сприяють надійному доставленню інформаційних кадрів. Існує шість підтипів контрольних кадрів:

– *Опитування після виходу з економічного режиму (Ps-запит)*. Даний кадр передається будь-якою станцією станції, що включає крапку доступу. У кадрові запитується передача кадра, що прибув, коли станція перебувала в режимі енергоощадження, і в цей момент розміщеного в буфері точка доступу.

– *Запит передачі (RTS)*. Даний кадр є першим із четвірки, використовуваної для забезпечення надійної передачі даних. Станція, що послала це повідомлення, попереджає адресата й інші станції, здатні прийняти дане повідомлення, про свою спробу передати адресатові інформаційний кадр.

– *Готовий до передачі (CTS)*. Другий кадр чотирикадрової схеми. Передається станцією-адресатом станції-джерелу й надає право відправлення інформаційного кадра.

– *Підтвердження (ACK)*. Підтвердження успішного приймання попередніх даних, кадра керування або кадра «Ps-запит».

– *Без змагання (Cf-кінець)*. Повідомляє кінець періоду без змагання; частина стратегії використання розподіленого режиму доступу.

– *Cf-кінець + Cf-підтвердження*. Підтверджує кадр «Cf-кінець». Даний кадр завершує період без змагання й звільняє станції від обмежень, пов'язаних із цим періодом.

2.4.2. Інформаційні кадри

Існує вісім підтипів інформаційних кадрів, зібраних у дві групи. Перші чотири підтипи визначають кадри, що переносять дані вищих рівнів від вихідної станції до станції-адресата. Перелічимо ці кадри:

– *Дані*. Просто інформаційний кадр. Може використовуватися як у період змагання, так і в період без змагання.

– *Дані + Cf-підтвердження*. Може передаватися тільки в період без змагання. Крім даних, у цьому кадрові є підтвердження отриманої раніше інформації.

– *Дані + Cf-запит*. Використовується крапковим *координатором* для доставлення даних до мобільної станції й для запиту в мобільної станції інформаційного кадра, який перебуває в її буфері.

– *Дані + Cf-підтвердження + Cf-запит*. Поєднує в одному кадрові функції двох описаних вище кадрів.

Інші чотири підтипи інформаційних кадрів фактично не переносять дані користувача. Інформаційний кадр «нульова функція» не переносить ні даних, ні запитів, ні підтверджень. Він використовується тільки для передачі крапці доступу біта керування живленням у поле керування кадром, указуючи, що станція перейшла в режим роботи зі зниженим енергоспоживанням. Три кадри, що залишилися (Cf-підтвердження, Cf-запит, Cf-підтвердження + Cf-запит) мають ті ж функції, що й описані вище підтипи кадрів (дані + Cf-підтвердження, дані + Cf-запит, дані + Cf-підтвердження + Cf-запит), але не несуть користувацьких даних.

2.4.3. Кадри керування

Кадри керування використовуються для керування зв’язком станцій і точок доступу. Можливі наступні підтипи:

- *Запит асоціації*. Посилає станція до точки доступу з метою запиту асоціації з даною мережею з базовим набором послуг (Basic Service Set – *BSS*). Кадр включає інформацію про можливості, наприклад, чи буде використовуватися шифрування, або чи здатна станція відповідати при опитуванні.
- *Відповідь на запит асоціації*. Вертається точкою доступу й указує, що запит асоціації прийнятий.
- *Запит повторної асоціації*. Посилає станцією при переході між *BSS*, коли потрібно встановити асоціацію із точкою доступу в новому *BSS*. Використання повторної асоціації, а не просто асоціації, дозволяє новій крапці доступу домовлятися зі старої про передачу інформаційних кадрів по новій адресі.

- *Відповідь на запит повторної асоціації*. Вертається точкою доступу й указує, що запит повторної асоціації прийнятий.
- *Пробний запит*. Використовується станцією для одержання інформації від іншої станції або точка доступу. Кадр використовується для локалізації *BSS* стандарту *IEEE 802.11*.
- *Відповідь на пробний запит*. Відгук на пробний запит.
- *Сигнальний кадр*. Передається періодично, дозволяє мобільним станціям локалізувати й ідентифікувати *BSS*.
- *Оголошення наявності трафіка*. Посилає мобільною станцією з метою повідомлення інших (які можуть перебувати в режимі зниженого енергоспоживання), що в *буфері даної* станції перебувають кадри, адресовані іншим.
- *Розрив асоціації*. Використовується станцією для *анулювання* асоціації.
- *Автентифікація*. Для автентифікації станцій використовуються множинні кадри.
- *Скасування автентифікації*. Передається для припинення безпечного з'єднання.

2.5. Стандарти IEEE 802.11

З усіх чинних стандартів бездротової передачі даних *IEEE 802.11* на практиці найчастіше використовуються всього три стандарти, певні Інженерним інститутом електротехніки й радіоелектроніки (*IEEE): 802.11b, 802.11a* і *802.11g.*

У стандарті *IEEE 802.11b* завдяки високій швидкості передачі даних (до 11 Мбит/с), практично еквівалентної пропускної здатності звичайних провідних локальних мереж *Ethernet*, а також орієнтації на *діапазон* 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників устаткування для бездротових мереж.

Оскільки встаткування, що працює на максимальній швидкості 11 Мбіт/с, має менший *радіус* дії, тому на нижчих швидкостях, стандартом *802.11b* передбачене автоматичне зниження швидкості при погіршенні якості сигналу.

Стандарт *IEEE 802.11a* має більшу ширину смуги із сімейства стандартів *802.11* при швидкості передачі даних до 54 Мбіт/с.

На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями *802.11a* передбачена робота в діапазоні 5 ГГц. Методом *модуляції* сигналу обране ортогональне частотне *мультиплексування* (*OFDM*).

До недоліків *802.11a* ставляться вища споживана *потужність* радіопередавачів для частот 5 ГГц, а також менший радіус дії.

Стандарт *IEEE 802.11g* є логічним розвитком *802.11b* і припускає передачу даних у тому ж частотному діапазоні. Крім того, стандарт *802.11g* повністю сполучимо з *802.11b*, тобто будь-який пристрій *802.11g* повинне підтримувати роботу із пристроями *802.11b*. Максимальна *швидкість передачі* в стандарті *802.11g* становить 54 Мбіт/с, тому на сьогодні це найбільш перспективний стандарт бездротового зв'язку.

При розробці стандарту *802.11g* розглядалися дві технології: метод ортогонального частотного поділу *OFDM* і метод двійкового пакетного зверткового кодування *PBCC*, опціонально реалізований у стандарті *802.11b*. У результаті стандарт *802.11g* містить компромісний розв'язок: як базові застосовуються технології *OFDM* і *CCK*, а опціонально передбачено використання технології *PBCC*. Про технології *CCK* і *OFDM* ми розповімо трохи пізніше.

Набір стандартів *802.11* визначає *цілий* ряд технологій реалізації фізичного рівня (*Physical Layer Protocol – PHY)*, які можуть бути використані підрівнем *802.11 MAC*. У цій главі розглядається кожний з рівнів *PHY*:

– Рівень *PHY* стандарту *802.11* зі стрибкоподібною перебудовою частоти (*FHSS*) у діапазоні 2,4 ГГц.

– Рівень *PHY* стандарту *802.11* з розширенням спектра методом прямої послідовності (*DSSS*) у діапазоні 2,4 ГГц.

– Рівень *PHY* стандарту *802.11b* з комплементарним кодуванням у діапазоні 2,4 ГГц.

– Рівень *PHY* стандарту 802.11a з ортогональним частотним мультиплексуванням (*OFDM*) у діапазоні 5 ГГц.

– Розширений *фізичний рівень* (Extended Rate *Physical Layer* – ERP) стандарту *802.11g* у діапазоні 2,4 ГГц.

Основне призначення фізичних рівнів стандарту *802.11* – забезпечити *механізми* бездротової передачі для підрівня *MAC*, а також підтримувати виконання вторинних функцій, таких як оцінка стану бездротового середовища й повідомлення про нього підрівню *MAC*. Рівні MAC і *PHY* розроблялися так, щоб вони були незалежними. Саме незалежність між *MAC* і підрівнем *PHY* і дозволила використовувати додаткові високошвидкісні фізичні рівні, описані в стандартах *802.11b*, 802.11a й *802.11g*.

Кожний з фізичних рівнів стандарту *802.11* має два підрівні:

– *Physical Layer Convergence* Procedure (PLCP). Процедура визначення стану фізичного рівня.

– *Physical Medium Dependent* (*PMD*). Підрівень фізичного рівня, що залежить від середовища передачі.

На рис. 2.8 показано, як ці підрівні співвідносяться між собою й з вищими рівнями в *моделі взаємодії відкритих систем* (*Open System Interconnection – OSI*).

Рисунок 2.8 – Підрівні рівня PHY

Підрівень PLCP по суті є рівнем забезпечення взаємодії, на якому здійснюється переміщення елементів даних протоколу *MAC* (*MAC Protocol Data Units* – MPDU) між MAC-Станціями з

використанням підрівня *PMD*, на якому реалізується той або інший метод передачі й приймання даних через бездротове середовище. Підрівні PLCP і *PMD* відрізняються для різних варіантів стандарту *802.11*.

Перед тем як приступитися до вивчення фізичних рівнів, розглянемо одну зі складових фізичного рівня, дотепер не згадану, а саме – зкремблювання.

Одна з особливостей, що лежать в основі сучасних передавачів, завдяки якій дані можна передавати з високою швидкістю, – це припущення про те, що дані, які пропонуються для передачі, надходять, з погляду передавача, випадковим чином. Без цього припущення багато переваг, одержувані шляхом застосування інших складових фізичного рівня, залишилися б нереалізованими.

Однак буває, що прийняті дані не цілком випадкові й насправді можуть містити повторювані набори й довгі послідовності нулів і одиниць.

Зкремблювання (*перестановка* елементів) – це метод, за допомогою якого прийняті дані робляться більш схожими на випадкові; досягається це шляхом перестановки бітів послідовності таким чином, щоб перетворити її зі структурованої в схожу на випадкову. Цю процедуру іноді називають «відбілюванням потоку даних». Дезкремблер приймача потім виконує *зворотне перетворення* цієї випадкової послідовності з метою одержання вихідної структурованої послідовності. Більшість способів зкремблювання належить до самосинхронізуючих; це означає, що дезкремблер здатний самостійно синхронізуватися зі зкремблером.

Стандарт *802.11* визначає три методи передачі на фізичному рівні:

- Передача в діапазоні інфрачервоних хвиль.
- Технологія розширення спектра шляхом стрибкоподібної перебудови частоти (*FHSS*) у діапазоні 2,4 ГГц.
- Технологія широкосмугової модуляції з розширенням спектра методом прямої послідовності (*DSSS*) у діапазоні 2,4 ГГц.

2.5.1. Передача в діапазоні інфрачервоних хвиль

Середовищем передачі є інфрачервоні хвилі діапазону 850 нм, які генеруються або напівпровідниковим лазерним *діодом*, або світлодіодним (*LED*). Тому що інфрачервоні хвилі не проникають через стіни, область покриття LAN обмежується зоною прямої видимості. Стандарт передбачає три варіанти поширення випромінювання: *ненаправлену антену*, відбиття від стелі й фокусне спрямоване випромінювання. У першому випадку вузький промінь розсіюється за допомогою системи лінз. Фокусне спрямоване випромінювання призначене для організації двоточкового зв'язку, наприклад між двома будинками.

2.5.2. Бездротові локальні мережі зі стрибкоподібною перебудовою частоти (FHSS)

Бездротові локальні мережі *FHSS* підтримують швидкості передачі 1 і 2 Мбіт/с. Пристрої *FHSS* ділить призначені для їхньої роботи смугу частот від 2,402 до 2,480 ГГц на 79 каналів, що не перекриваються. Ширина кожного з 79 каналів становить 1 МГц, тому бездротові локальні мережі *FHSS* використовують відносно високу швидкість передачі символів – 1 МГц – і набагато меншу швидкість перебудови з каналу на канал.

Послідовність перебудови частоти повинна мати наступні параметри: частота перескоків не менш 2,5 рази за секунду як мінімум між шістьома (6 МГц) каналами. Щоб мінімізувати число колізій між зонами, що перекриваються, покриття, можливі послідовності перескоків повинні бути розбиті на три набори послідовностей, довжина яких для Північної Америки й більшої частини Європи становить 26. У таблиці 2.2 представлені схеми стрибкоподібної перебудови частоти, що забезпечують мінімальне перекриття.

По суті, схема стрибкоподібної перебудови частоти забезпечує неквапливий перехід з одного можливого каналу на інший таким чином, що після кожного стрибка покривається смуга частот, рівна як мінімум 6 МГц, завдяки чому в багатостільникових мережах мінімізується можливість виникнення колізій.

Таблиця 2.2 – Схема *FHSS* для Північної Америки і Європи

Набір	Схема стрибкоподібної перебудови частоти
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

Після того як рівень MAC пропускає MAC-Фрейм, який у локальних бездротових мережах *FHSS* називається також службовим елементом даних PLCP, або PSDU (PLCP Service Data Unit), підрівень PLCP додає два поля в початок фрейму, щоб сформувати в такий спосіб фрейм PPDU (PPDU – елемент даних протоколу PLCP). На рис. 2.9 представлений формат фрейму *FHSS* підрівня PLCP.

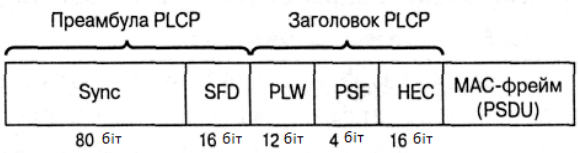


Рисунок 2.9 – Формат фрейму FHSS підрівня PLCP

Преамбула PLCP складається із двох підполів:

– Підполе *Sync розміром 80 біт*. Рядок, що полягає з, що чергуються 0 і 1, починається з 0. Приймальна станція використовує це поле, щоб ухвалити рішення щодо вибору антени при наявності такої можливості, відкоригувати відхід частоти (frequency offset) і синхронізувати розподіл пакетів (packet timing).

– Підполе *мітки початку фрейму (Start of Frame Delimiter, SFD) розміром 16 біт*. Складається зі специфічного рядка (0000 1100 1011 1101, крайній ліворуч біт перший) у забезпечення синхронізації фреймів (frame timing) для приймальної станції.

Заголовок фрейму PLCP складається із трьох підполів:

Слово довжини службового елемента даних PLCP (PSDU), PSDU Length Word (PLW) розміром 12 біт. Указує розмір фрейму MAC (PSDU) в *октетах*.

– *Сигнальне поле PLCP (Signaling Field PLCP – PSF) розміром 4 біт*. Указує швидкість передачі даних конкретного фрейму.

– *HEC (Header Error Check)*. Контрольна сума фрейму.

Службовий елемент даних PLCP (PSDU) проходить через операцію зкремблювання з метою (рандомізації) послідовності вхідних бітів і в результаті PSDU має вигляд представлений на рис. 2.10. символи, що заповнюють, вставляються між усіма 32-символьними блоками. Ці символи, що заповнюють, усувають будь-які систематичні відхилення в даних, наприклад, коли одиниць більше, ніж нулів, або навпаки, які могли б привести до небажаних ефектів при подальшій обробці.

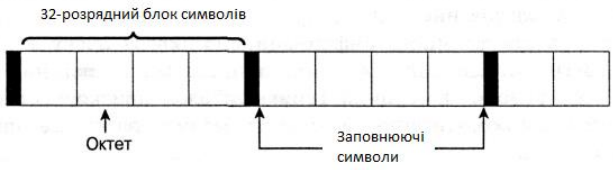


Рисунок 2.10 – Зкрембльований PSDU у технології FHSS

Підрівень PLCP перетворить фрейм у потік бітів і передає його на підрівень *PMD*. Підрівень *PMD* технології *FHSS* модулює потік даних з використанням модуляції, заснованої на Гаусовому методі частотної модуляції (Gaussian Frequency Shift Keying – GFSK).

2.5.3. Бездротові локальні мережі, що використовують широкосмугову модуляцію DSSS з розширенням спектра методом прямої послідовності

У специфікації стандарту *802.11* застережене використання й іншого фізичного рівня – на основі технології широкосмугової модуляції з розширенням спектра методом прямої послідовності

(*DSSS*). Як було зазначено в стандарті *802.11* розробки 1997 року, технологія *DSSS* підтримує швидкості передачі 1 і 2 Мбіт/с.

Аналогічно підрівню PLCP, використовуваному в технології *FHSS*, підрівень PLCP технології *DSSS* стандарту *802.11* додає два поля у фрейм MAC, щоб сформувати PPDU: преамбулу PLCP і заголовок PLCP Формат фрейму представлений на рис. 2.11.

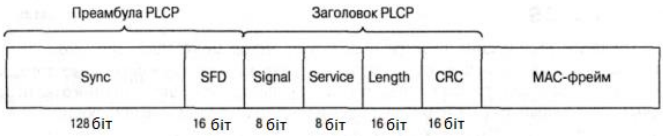


Рисунок 2.11 – Формат фрейму DSSS підрівня PLCP

Преамбула PLCP складається із двох підполів:

– *Підполе Sync шириною 128 біт, що становити собою рядок, що полягає з одиниць*. Завдання цього підполя – забезпечити синхронізацію для приймальної станції.

– *Підполе SFD шириною 16 біт* ; у ньому втримується специфічний рядок OxF3A0; його завдання – забезпечити таймінг (timing) для приймальної станції.

Заголовок PLCP складається із чотирьох підполів:

– *Підполе Signal шириною 8 біт, що вказує тип модуляції й швидкість передачі для даного фрейму*.

– *Підполе Service шириною 8 біт зарезервоване*. Це означає, що під час розробки специфікації стандарту воно залишилося невизначеним; передбачається, що воно буде використано в майбутніх модифікаціях стандарту.

– *Підполе Length шириною 16 біт кількість, що вказує, мікросекунд (з діапазону 16-216), необхідне для передачі* частини Мас-Фрейму.

– *Підполе CRC*. 16-бітна контрольна сума.

Підрівень PLCP перетворить фрейм у потік бітів і передає дані на підрівень *PMD*. Увесь PPDU проходить через процес зкремблювання з метою рандомізації даних.

Зкремблірована преамбула PLCP завжди передається зі швидкістю 1 Мбіт/с, у той час, як зкремблірований фрейм MPDU

передається зі швидкістю, зазначеної в Підполе Signal. Підрівень *PMD* модулює вибілений потік бітів, використовуючи наступні *методи модуляції*:

– Двійкова відносна фазова модуляція (*Differential* Binary *Phase Shift* Keying – DBPSK) для швидкості передачі 1 Мбіт/с.

– Квадратурна відносна фазова модуляція (*Differential Quadrature Phase Shift* Key – *DQPSK*) для швидкості передачі 2 Мбіт/с.

На фізичному рівні до MAC-Кадрам (MPDU) додається заголовок фізичного рівня, що полягає із преамбули й властиво Plcp-Заголовка (рис. 2.12).

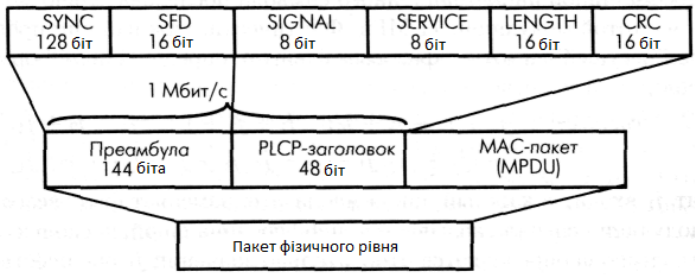


Рисунок 2.12 – Структура кадрів мережі IEEE 802.11b фізичного рівня

Преамбула містить стартову синхропослідовність (*SYNC*) для настроювання приймача й 16-бітний код початку кадра (SFD) – число F3A016.Plcp-Заголовок включає поля SIGNAL (інформація про швидкість і тип модуляції), SERVICE (додаткова інформація, у тому числі про застосування високошвидкісних розширень і Pbcc-*модуляції*) і LENGTH (час у мікросекундах, необхідне для передачі наступної за заголовком частини кадра). Усі три поля заголовка захищені 16-бітною контрольною сумою *CRC*.

У стандарті *IEEE 802.11b* передбачено два типи заголовків: довгий і короткий (рис. 2.13).

Рисунок 2.13 – Короткий заголовок кадрів мережі 802.11b

Вони відрізняються довжиною синхропослідовності (128 і 56 біт), способом її генерації, а також тим, що символ початку кадра в короткому заголовку передається у зворотному порядку. Крім того, якщо всі поля довгого заголовка передаються зі швидкістю 1 Мбіт/с, те при короткому заголовку преамбула транслюється на швидкості 1 Мбіт/с, інші поля заголовка – зі швидкістю 2 Мбіт/с. Іншу частину кадра можна передавати на кожній із припустимим стандартом швидкостей передачі, зазначених у полях SIGNAL і SERVICE. Короткі заголовки фізичного рівня передбачені специфікацією *IEEE 802.11b* для збільшення пропускної здатності мережі.

З опису процедур зв'язку мережі *IEEE 802.11* видне, що «накладні витрати» у цьому стандарті вище, чим у провідній мережі Ethernet. Тому надто важливо забезпечити високу швидкість передачі даних у каналі. Підвищити пропускну здатність каналу із заданою шириною смуги частот можна, розробляючи й застосовуючи нові *методи модуляції*. Цим шляхом пішла група розроблювачів *IEEE 802.11b*.

Нагадаємо, що споконвічно стандарт *IEEE 802.11* передбачав роботу в режимі *DSSS* з використанням так званої Баркеровскої послідовності (Barker) довжиною 11 біт: B1 = (10110111000). Кожний інформаційний біт заміщається своїм добутком по модулю 2 (операція, що виключає «АБО») з даною послідовністю, тобто кожна інформаційна одиниця заміняється на B1, кожний нуль – на інверсію B1. У результаті біт заміняється послідовністю 11 чипів. Далі сигнал кодується за допомогою диференціальної двох – або чотирьохпозиційної фазової модуляції (DBPSK або *DQPSK*, один або два чіпи на символ

відповідно). При частоті модуляції опорної 11 МГц загальна швидкість становить залежно від типу модуляції 1 і 2 Мбіт/с.

Стандарт *IEEE 802.11b* додатково передбачає швидкості передачі 11 і 5,5 Мбіт/с. Для цього використовується так звана ССК – модуляція (*Complementary* Code Keying – кодування комплементарним кодом).

Хоча механізм розширення спектра, використовуваний для одержання швидкостей 5,5 і 11 Мбіт/с із застосуванням ССК, ставиться до методів, які застосовуються для швидкостей 1 і 2 Мбіт/с, він по-своєму унікальний. В обох випадках застосовується метод розширення, але при використанні модуляції ССК розширювальний код являє собою код з 8 комплексних чипів, у той час, як при роботі зі швидкостями 1 і 2 Мбіт/с застосовується 11-розрядний код. 8 – чиповий код визначається або 4, або 8 бітами - залежно від швидкості передачі даних. Швидкість передачі чипів становить 11 Мчіп/с, тобто при 8 комплексних чипах на символ і 4 або 8 бітів на символ можна досягти швидкості передачі даних 5,5 і 11 Мбіт/с.

Для того, щоб передавати дані зі швидкістю 5,5 Мбіт/с, потрібно згрупувати зкрембльований потік бітів у символи по 4 біти (b0, b1, b2 і b3). Останні два біти (b2 і b3) використовуються для визначення 8 послідовностей комплексних чипів, як показано в таблиці 2.3, де {3l, 32, 33, 34, 35, 36, 37, 38} представляють чипи послідовності. У таблиці 2.3 j представляє уявне число, корінь квадратний з -1, і відкладається по уявній, або квадратурної, осі комплексної площини.

Таблиця 2.3 – Послідовність чипів ССК

(b2, b3)	31	32	33	34	35	36	37	38
00	j	1	j	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	j	1
11	j	-1	j	1	-j	1	j	1

Тепер, маючи послідовність чіпів, певними бітами (b2, b3), можна використовувати перші два біти (b0, b1) для визначення повороту фази, здійснюваного при модуляції по методу *DQPSK*,

який буде застосований до послідовності (таблиця 2.4). Ви повинні також пронумерувати кожний 4-бітовий символ PSDU, починаючи з 0, щоб можна було визначити, перетворите ви парний або непарний символ відповідно до цієї таблиці. Слід пам'ятати, що мова йде про використання *DQPSK*, а не *QPSK*, і тому представлені в таблиці зміни фази відлічуються стосовно попереднього символу або, у випадку першого символу PSDU, стосовно останнього символу попереднього Dqpsk-*Символу*, переданого зі швидкістю 2 Мбіт/с.

Це обертання фази застосовується стосовно 8 комплексних чіпів символу, потім здійснюється модуляція на опорній, що підходить частоті.

Щоб передавати дані зі швидкістю 11 Мбіт/с, зкремблюванням послідовність бітів PSDU розбивається на групи по 8 символів. Останні 6 бітів вибирають одну послідовність, що полягає з 8 комплексних чипів, з-поміж 64 можливих послідовностей, майже так само, як використовувалися біти (b2, b3) для вибору однієї із чотирьох можливих послідовностей. Біти (b0, b1) використовуються в такий же спосіб, як при модуляції ССК на швидкості 5,5 Мбіт/с для обертання фази послідовності й подальшої модуляції на опорній частоті, що підходить.

Таблиця 2.4 – Поворот фази при модуляції ССК

(b0,b1)	Зміна фази парних символів	Зміна фази непарних символів
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

У чому гідність ССК-Модуляції? Річ у тому, що чипи символу визначаються на основі послідовностей Уолша-Адамара. Послідовності Уолша-Адамара добре вивчені, мають відмінні авто кореляційні властивості. Що немаловажне, кожна така послідовність мало корелює сама із собою при фазовому зрушенні – дуже корисна властивість при боротьбі з

перевідбитими сигналами. Неважко помітити, що теоретичне операційне посилення ССК-Модуляції – 3 дБ (у два рази), оскільки без кодування Qpsk-*Модульований* із частотою 11 Мбіт/с сигнал може транслювати 22 Мбіт/с. Як видне, ССК-Модуляція являє собою вид блокового коду, а тому досить проста при апаратної реалізації. Сукупність цих властивостей і забезпечила ССК місце в стандарті *IEEE 802.11b* у якості обов'язкового виду модуляції.

На практиці важливо не тільки операційне посилення. Істотну роль відіграє й рівномірність розподілу символів у фазовому просторі – вони повинні якнайдалі відстояти друг від друга, щоб мінімізувати помилки їх детектування. І із цього погляду ССК-Модуляція не виглядає оптимально, її реальне операційне посилення не перевищує 2 дБ. Тому було розроблено інший спосіб модуляції – пакетне бінарне зверткове кодування PBCC (*Packet Binary Convolutional Coding*). Цей метод увійшов у стандарт *IEEE 802.11b* як додаткова (необов'язкова) опція. Механізм PBCC (рис. 2.7) дозволяє домагатися в мережах *IEEE 802.11b* пропускної здатності 5,5, 11 і 22 Мбіт/с.

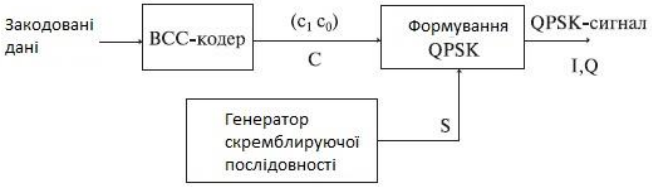


Рисунок 2.7 – Загальна схема PBCC-Модуляції

Як випливає з назви, метод заснований на звертковому кодуванні. Для швидкостей 5,5 і 11 Мбіт/с потік інформаційних бітів надходить у шестирозрядний *зсувний регістр* із суматорами (рис. 2.8).

У початковий момент часу всі тригери *зсувного регістру* ініціюють нулем. У результаті кожний вихідний біт d заміняється двома бітами кодової послідовності (c0, c1). При швидкості 11 Мбіт/с із0 і с1 задають один символ чотирьохпозиційний Qpsk-

Модуляції. Для швидкості 5,5 Мбіт/с використовують двопозиційну Bpsk-*Модуляцію*, послідовно передаючи кодові біти з 0 і з 1. Якщо ж потрібна швидкість 22 Мбіт/с, схема кодування ускладнюється (рис. 2.9): три кодові біти (c0-c2) визначають один символ у 8-позиційної psk-модуляції.

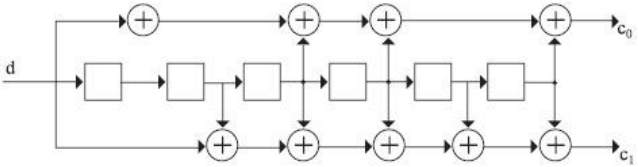


Рисунок 2.8 – Звертковe кодування із двома бітами кодової послідовності

Після формування Psk-*Символів* відбувається зкремблювання. Залежно від сигналу s (рис. 2.7) символ залишається без змін (s = 0), або його фаза збільшується на $\pi/2$ (s = 1). Значення s визначає 256-бітова циклічно повторювана послідовність S. Вона формується на основі початкового вектора U = 338Bh, у якому рівне число нулів і одиниць.

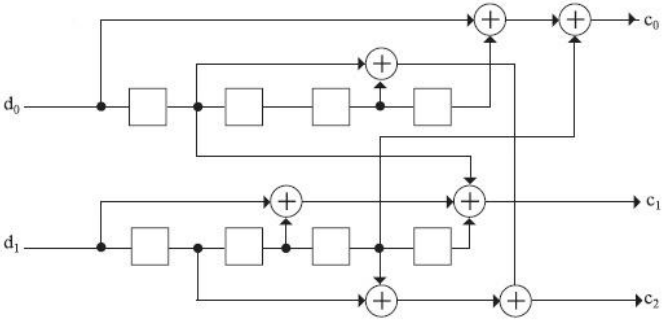


Рисунок 2.9 – Звертковe кодування із трьома бітами кодової послідовності

У шестирозрядного *зсувного регістру*, застосовуваного у РВСС для швидкостей 11 і 5,5 Мбіт/с, 64 можливих вихідних станів. Так що при модуляції РВСС інформаційні біти у фазовому просторі виявляються набагато далі один від одного, чім при ССК-Модуляції. Тому РВСС і дозволяє при тому самому співвідношенні «сигнал-шум» і рівні помилок вести передачу з більшою швидкістю, чім у випадку ССК. Однак плата за більш ефективне кодування – складність апаратної реалізації даного алгоритму.

Стандарт IEEE 802.11a з'явився практично одночасно з *IEEE 802.11b*, у вересні 1999 року. Ця специфікація була орієнтована на роботу в діапазоні 5 ГГц і заснована на принципово іншому, чим описане вище, механізмі кодування даних – на частотному мультиплексуванні за допомогою ортогональних опорних (*OFDM*).

Стандарт *802.11a* визначає характеристики встаткування, застосовуваного в офісних або міських умовах, коли поширення сигналу відбувається по багатопроменевих каналах через безліч відбиттів.

В IEEE 802.11a кожний кадр передається за допомогою 52 ортогональних опорних, кожна із шириною смуги порядку 300 КГц (20 МГц/64). Ширина одного каналу – 20 МГц. Опорні частоти модулюють за допомогою *BPSK*, *QPSK*, а також 16- і 64-позиційної квадратурної амплітудної модуляції (*QAM*). У сукупності з різними швидкостями кодування (1/2 і 3/4, для 64-QAM - 2/3 і 3/4) утворюється набір швидкостей передачі 6, 9, 12, 18, 24, 36, 48 і 54 Мбіт/с. У таблиці 2.5 показане, як необхідна швидкість передачі даних перетвориться у відповідні параметри вузлів передавача *OFDM*.

З 52 опорних частот 48 призначені для передачі інформаційних символів, інші 4 – службові. Структура заголовків фізичного рівня відрізняється від прийнятого в специфікації *IEEE 802.11b*, але незначно (рис. 2.10).

Кадр включає преамбулу (12 символів синхропослідовності), заголовок фізичного рівня (PLCP-заголовок) і властиво інформаційне поле, сформоване на MAC-Рівні. У заголовку передається інформація про швидкість кодування, типі модуляції

й довжині кадра. Преамбула й заголовок транслюються з мінімально можливою швидкістю (*BPSK*, швидкість кодування r = 1/2), а інформаційне поле – із зазначеної в заголовку, як правило, максимальної, швидкістю, залежно від умов обміну.Ofdm-*Символи* передаються через кожні 4 мкс, причому кожному символу тривалістю 3,2 мкс передує захисний інтервал 0,8 мкс (повторювана частина символу). Останній необхідний для боротьби з багатопроменевим поширенням сигналу – відбитий і прийдешнього із затримкою символ потрапить у захисний інтервал і не ушкодить наступний символ.

Таблиця 2.5 – Параметри передавача стандарту 802.11a

Швидкість передачі даних (Мбіт/с)	Модуляція	Швидкість згорткового кодування	Число канальних бітів на, що піднесе	Число канальних бітів на символ	Число бітів даних на символ *OFDM*
6	*BPSK*	1/2	1	48	24
9	*BPSK*	3/4	1	48	36
12	*QPSK*	1/2	2	96	48
18	*QPSK*	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Рисунок 2.10 – Структура заголовка фізичного рівня стандарту IEEE 802.11a

Кадр включає преамбулу (12 символів синхропослідовності), заголовок фізичного рівня (PLCP-Заголовок) і властиво інформаційне поле, сформоване на MAC-Рівні. У заголовку передається інформація про швидкість кодування, типі модуляції й довжині кадра. Преамбула й заголовок транслюються з мінімально можливою швидкістю (*BPSK*, швидкість кодування r = 1/2), а інформаційне поле – із зазначеної в заголовку, як правило, максимальної, швидкістю, залежно від умов обміну. Ofdm-*Символи* передаються через кожні 4 мкс, причому кожному символу тривалістю 3,2 мкс передує захисний інтервал 0,8 мкс (повторювана частина символу). Останній необхідний для боротьби з багатопроменевим поширенням сигналу – відбитий і прийдешнього із затримкою символ потрапить у захисний інтервал і не ушкодить наступний символ.

Природно, формування/декодування Ofdm-*Символів* відбувається за допомогою швидкого перетворення Фур'є (зворотного/прямого, ЗШПФ/ШПФ). *Функціональна схема* трактів приймання/передачі (рис. 2.11) досить стандартна для даного методу й включає звертковий *кодер*, механізм переміщення/перерозподілу (захист від пакетних помилок) і процесор ЗШПФ.

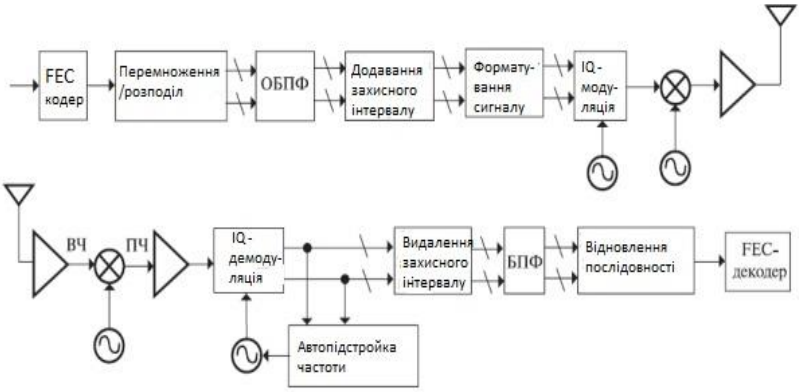


Рисунок 2.11 – Функціональна схема трактів приймання/передачі стандарту IEEE 802.11a

Фур'є – Процесор і формує сумарний сигнал, після чого до символу додається захисний інтервал, остаточно формується OFDM-Символ і за допомогою квадратурного модулятора/ конвертера переноситься в задану частотну область. При прийманні все відбувається у зворотному порядку.

Стандарт *IEEE 802.11g* по суті являє собою перенесення схеми модуляції *OFDM*, що зарекомендувала себе в 802.11a, з діапазону 5 ГГц в область 2,4 ГГц при збереженні функціональності пристроїв стандарту *802.11b*. Це можливо, оскільки в стандартах *802.11* ширина одного каналу в діапазонах 2,4 і 5 ГГц схожа – 22 МГц.

Одним з основних вимог до специфікації *802.11g* була зворотна сумісність із пристроями *802.11b*. Дійсно, у стандарті *802.11b* в якості основного способу модуляції прийнята схема CCK (*Complementary* Code Keying), а як додаткова можливість допускається модуляція *PBCC* (*Pocket* Binary *Convolutional Coding*).

Розроблювачі *802.11g* передбачили CCK-Модуляцію для швидкостей до 11 Мбіт/с і *OFDM* для більш високих швидкостей. Але мережі стандарту *802.11* при роботі використовують принцип *CSMA*/CA – *множинний доступ* до каналу зв'язку з *контролем опорної* й запобіганням колізій. Жоден пристрій *802.11* не повинен починати передачу, поки не переконається, що ефір у його діапазоні вільний від інших пристроїв. Якщо в зоні чутності виявляться пристрої *802.11b* і *802.11g*, причому обмін буде відбуватися між пристроями *802.11g* за допомогою *OFDM*, те встаткування *802.11b* просто не зрозуміє, що інші пристрої мережі ведуть передачу, і спробує почати трансляцію. Наслідки очевидні.

Щоб не допустити подібної ситуації, передбачена можливість роботи в змішаному режимі – *CCK-OFDM*. Інформація в мережах *802.11* передається кадрами. Кожний інформаційний кадр включає два основні поля: преамбулу із заголовком і інформаційне поле (рис. 2.12).

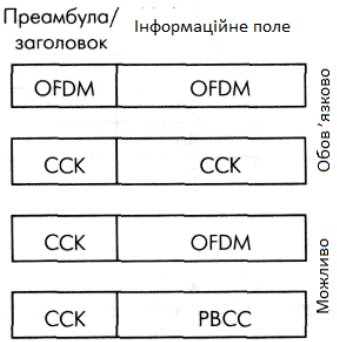


Рисунок 2.12 – Кадри IEEE 802.11g у різних режимах модуляції

Преамбула містить синхропослідовність і код початку кадра, заголовок – службову інформацію, у тому числі про тип модуляції, швидкості й тривалості передачі кадра. У режимі *CCK-OFDM* преамбула й заголовок модулюються методом CCK (реально – шляхом прямого розширення спектра *DSSS* за допомогою послідовності Баркера, тому в стандарті *802.11g* цей режим йменується *DSSS-OFDM*), а інформаційне поле – методом *OFDM*. Таким чином, усі пристрої *802.11b*, постійно «що прослуховують» ефір, ухвалюють заголовки кадрів і довідаються, скільки часу буде транслюватися кадр *802.11g*. У цей період вони «мовчать». Природно, пропускна здатність мережі падає, оскільки швидкість передачі преамбули й заголовка – 1 Мбіт/с. Очевидно, даний підхід не влаштовував табір прихильників технології *PBCC*, і для досягнення компромісу в стандарт *802.11g* у якості додаткової можливості ввели, так само як і в *802.11b*, необов'язковий режим – *PBCC*, у якому заголовок і преамбула передаються, так само як і при CCK, а інформаційне поле модулюється за схемою *PBCC* і передається на швидкості 22 або 33 Мбіт/с. У результаті пристрою стандарту *802.11g* повинні виявитися сумісними з усіма модифікаціями встаткування *802.11b* і не створювати взаємних перешкод. Діапазон підтримуваних їм швидкостей відбито в таблиці 2.6, залежність швидкості від типу модуляції – на рис. 2.13.

Таблиця 2.6 – Можливі швидкості й тип модуляції в специфікації *IEEE 802.11g*

Швидкість, Мбіт/с	Тип модуляції	
	Обов'язково	Припустиме
1	Послідовність Баркера	
2	Послідовність Баркера	
5,5	*CCK*	PBCC
6	*OFDM*	*OFDM*
9		*OFDM*, *CCK-OFDM*
11	*CCK*	PBCC
12	*OFDM*	*CCK-OFDM*
18		*OFDM*, *CCK-OFDM*
22		PBCC
24	*OFDM*	*CCK-OFDM*
33		PBCC
36		*OFDM*, *CCK-OFDM*
48		*OFDM*, *CCK-OFDM*
54		*OFDM*, *CCK-OFDM*

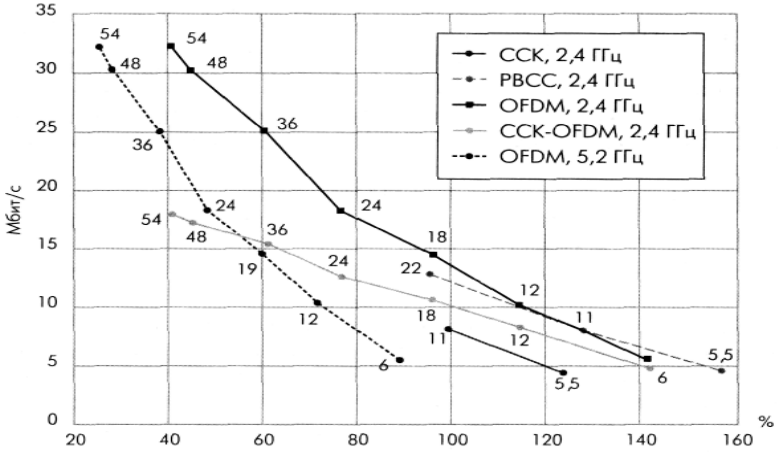


Рисунок 2.13 – Залежність швидкості передачі від відстані для різних технологій передачі. Відстань наведена у відсотках, 100% – дальність передачі з модуляцією ССК на швидкості 11 Мбіт/с

Очевидно, що пристроям стандарту *IEEE 802.11g* досить довго доведеться працювати в одних мережах з устаткуванням *802.11b*. Також очевидно, що виробники в більшості випадків не будуть підтримувати режими *CCK-OFDM* і *PBCC* внаслідок їх необов'язковості, адже майже все вирішує ціна пристрою. Тому одна з основних проблем даного стандарту – як забезпечити безконфліктну роботу змішаних мереж *802.11b*/g.

Таблиця 2.7 – Зведена інформація з параметрів фізичних рівнів

Параметр	802.11 DSSS	802.11 FHSS	802.11b	802.11a	802.11g
Частотний діапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальна швидкість передачі даних (Мбит/с)	2	2	11	54	54
Технологія	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляції (для максимальної швидкості передачі)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число каналів	3	3	3	15	3

Основний принцип роботи в мережах *802.11* – «слухати, перш ніж віщати». Але пристрої *802.11b* не здатні почути пристрої *802.11g* в *OFDM-режимі*. Ситуація аналогічна проблемі схованих станцій: два пристрої вилучені настільки, що не чують один одного й намагаються звернутися до третього, яке перебуває в зоні чутності обох. Для запобігання конфліктів у подібній ситуації в *802.11* уведений захисний механізм, що передбачає перед початком інформаційного обміну передачу короткого кадра «запит на передачу» (*RTS*) і одержання кадра підтвердження «можна передавати» (*CTS*). Механізм *RTS*/*CTS* застосуємо й до змішаних мереж *802.11b*/g. Природно, ці кадри повинні транслюватися в режимі ССК, який зобов'язані «розуміти» всі пристрої. Однак захисний механізм суттєво знижує пропускну здатність мережі.

3. РЕЖИМИ МЕРЕЖ Й ОСОБЛИВОСТІ ЇХ ОРГАНІЗАЦІЇ

3.1. Режим Ad Hoc

У режимі *Ad Hoc* (рис. 3.1) клієнти встановлюють *зв'язок* безпосередньо один з одним. Установлюється однорангова взаємодія по типу «точка-*точка»*, і комп'ютери взаємодіють прямо без застосування крапок доступу. При цьому створюється тільки одна зона обслуговування, що не має інтерфейсу для підключення до провідної локальної мережі.

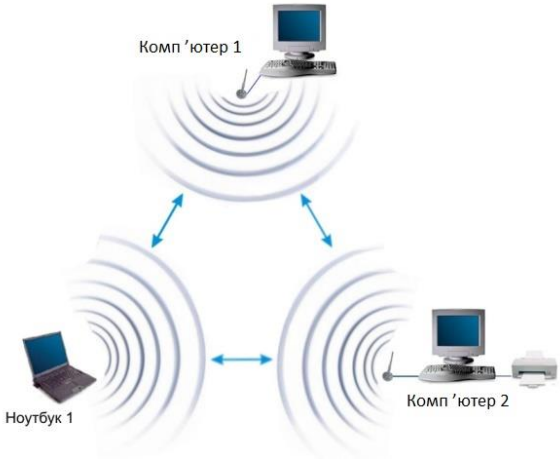


Рисунок 3.1 – Ad Hoc

Основна перевага даного режиму – простота організації: він не вимагає додаткового встаткування (точка доступу). Режим може застосовуватися для створення тимчасових мереж для передачі даних.

Однак необхідно мати на увазі, що режим Ad Hoc дозволяє встановлювати з'єднання на швидкості не більш 11 Мбіт/с, незалежно від використовуваного встаткування. Реальна швидкість обміну даними буде нижче й складе не більш 11/N Мбіт/с, де N – число пристроїв у мережі. Дальність зв'язку

становить не більш ста метрів, а *швидкість передачі* даних швидко падає зі збільшенням відстані.

Для організації довгочасних бездротових мереж слід використовувати інфраструктурний режим.

Для побудови з'єднання в режимі Ad Hoc на клієнтській стороні будемо використовувати бездротовий Usb-Адаптер. Усі настроювання для інших типів адаптерів (PCI, PCMCI, Expresscard і т.д.) проводяться аналогічним образом.

При підключенні адаптера необхідно встановити драйвер, який іде в комплекті з усім бездротовим устаткуванням. У вікні *Мережні підключення* повинен з'явитися значок *Бездротове мережне з'єднання* (рис. 3.2)

Бездротову мережу в режимі Ad Hoc спочатку будемо будувати з комп'ютера 1 і ноутбука 1 (рис. 4.1), а потім можна буде приєднати й інші комп'ютери. Це можна зробити двома способами: за допомогою вбудованої служби Windows і програмою D-Link Airplus Xtremeg Wireless Utility, яка йде в комплекті з устаткуванням D-Link.

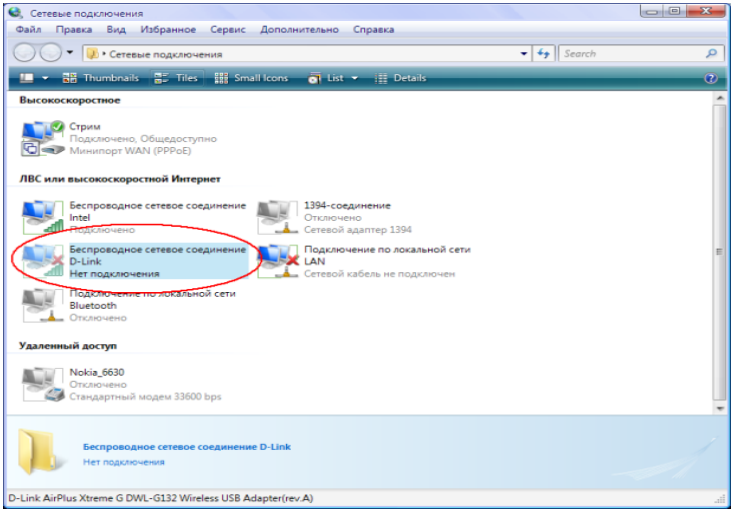


Рисунок 3.2 – Налаштування підключення за допомогою вбудованої служби Windows

При наявності вбудованої утиліти Windows, додаткові програми не потрібні. Але для цього необхідно встановити галочку *Використовувати Windows для настроювання мережі* на вкладці *Бездротові мережі* у властивостях бездротового з'єднання (рис. 3.3).

Перед установкою з'єднання необхідно настроїти статичні Ip-Адреси. Вони настроюються у властивостях бездротового з'єднання, на вкладці *Загальні*, у властивостях *Протокол Інтернету (TCP/IP)* (рис. 3.4).

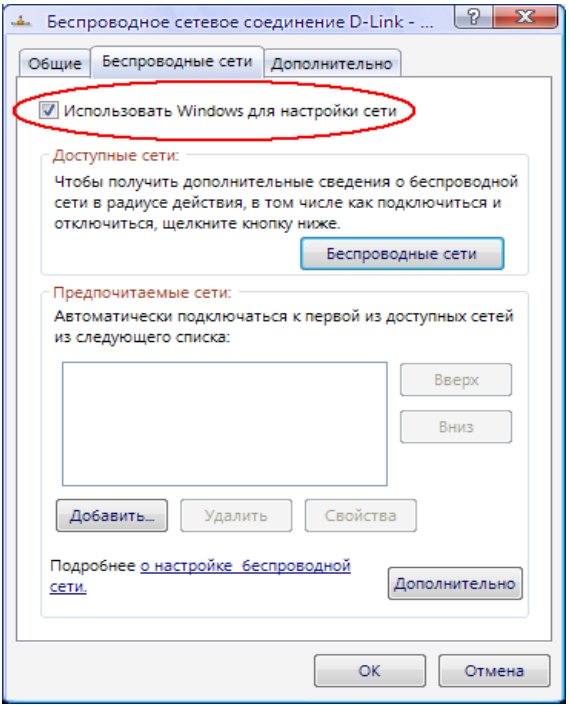


Рисунок 3.3 – Налаштування підключення за допомогою вбудованої служби Windows

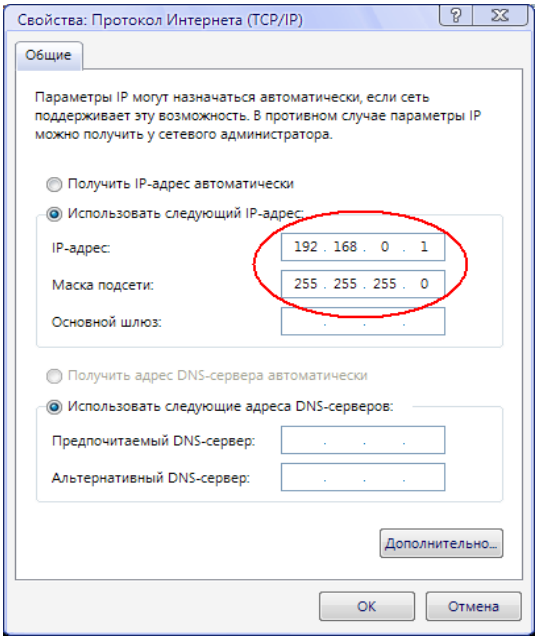


Рисунок 3.4 – Налаштування підключення за допомогою вбудованої служби Windows

Перший комп'ютер (*Комп'ютер 1*) нехай буде мати Ip-Адреса 192.168.0.1, а другий (*Ноутбук 1*) – 192.168.0.2, а маска підмережі – 255.255.255.0.

Тепер для організації мережі в режимі Ad Hoc подвійним клацанням лівої кнопки миші по бездротовому інтерфейсу (рис. 3.2) запустимо службу Windows. Тут на одному з комп'ютерів запустимо *Встановити бездротову мережу* (рис. 3.5). У майстру, що з'явився, треба *ввести* SSID (наприклад, Ad hoc net) і ключ доступу. На цьому конфігурування одного комп'ютера закінчується.

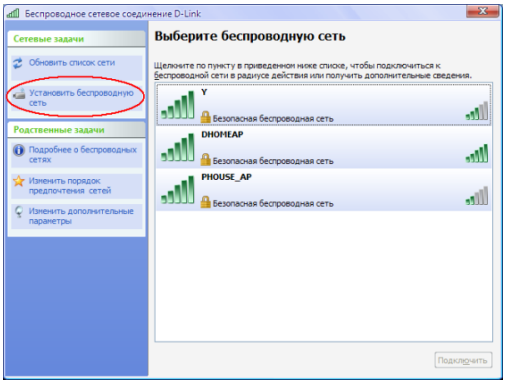


Рисунок 3.5 – Налаштування підключення за допомогою вбудованої служби Windows

На іншому комп'ютері теж запускаємо службу Windows рис. 3.5), і в основному вікні вибираємо мережу, що з'явився (Ad hoc net). При збігу ключів доступу цей комп'ютер підключається до першого, і в такий спосіб створюється бездротова мережа Ad Hoc.

Якщо потрібно приєднати ще комп'ютери, виконуються ті ж дії, що й із другим. У цьому випадку мережа вже буде складатися з декількох комп'ютерів.

У випадку налаштування підключення за допомогою програми D-Link Airplus Xtremeg Wireless Utilit треба встановити цю програму й забрати галочку *Використовувати Windows для налаштування мережі*, показану на рис. 3.3.

Щоб організувати бездротовий зв'язок Ad Hoc, запустіть цю програму на першому комп'ютері й перейдіть на вкладку *налаштування* (рис. 3.6).

Потім уведіть *SSID* створюваної мережі (наприклад, Ad hoc net), виберіть режим Ad Hoc і встановите Ip-Адресу з маскою бездротового інтерфейсу. Автентифікація й шифрування поки залишимо відкритими. Якщо потрібні додаткові настроювання, їх можна зробити на вкладці *розширене налаштування*.

На інших комп'ютерах також запускаємо цю програму й відкриваємо вкладку *Огляд мереж* (рис. 3.7).

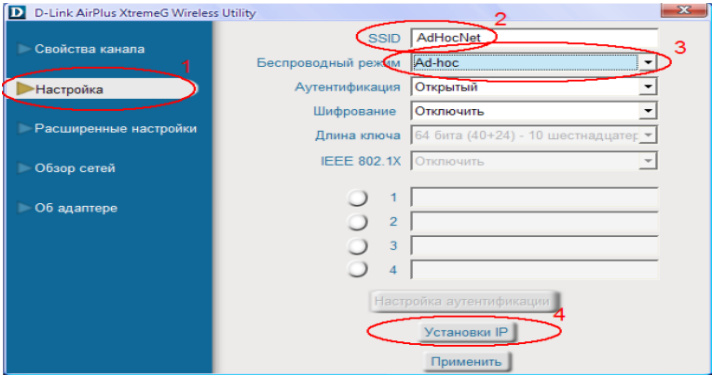


Рисунок 3.6 – Налаштування підключення за допомогою програми D-Link Airplus Xtremeg Wireless Utilit

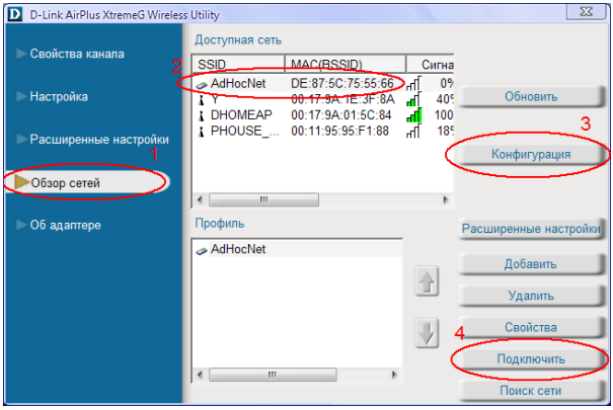


Рисунок 3.7 – Огляд мереж

У вікні, що з’явилося, слід вибрати мережа й для настроювання Ір-Адреси другого комп’ютера натиснути *кнопку Конфігурація*. Потім потрібно натиснути кнопку *Приєднати*, і при збігу ключів доступу бездротовий адаптер приєднається до першого комп’ютера. Інші комп’ютери підключаються

аналогічним чином. Відновлення доступних мереж проводиться натисканням кнопки *Обновити*.

3.2. Інфраструктурний режим

У цьому режимі точка доступу забезпечують зв'язок клієнтських комп'ютерів (рис. 3.8). Точку доступу можна розглядати як бездротовий комутатор. Клієнтські станції не зв'язуються безпосередньо одна з одною, а зв'язуються із точкою доступу, і вона вже направляє пакети адресатам.

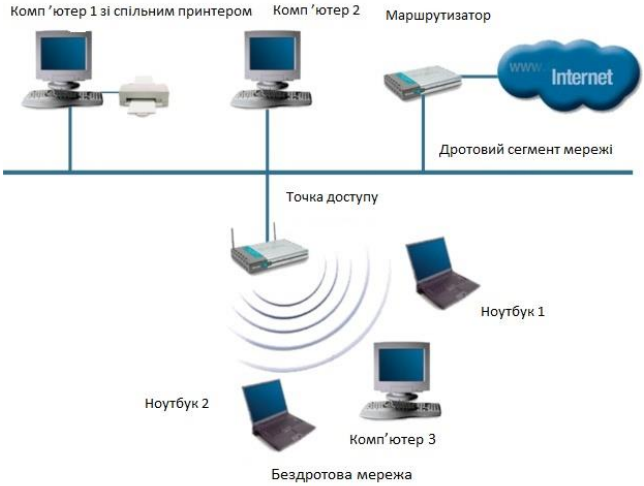


Рисунок 3.8 – Інфраструктурна мережа

Точка доступу має порт Ethernet, через який базова зона обслуговування підключається до провідної або змішаній мережі – до мережної інфраструктури.

Налаштуємо бездротову точку доступу в інфраструктурному режимі.

Налаштування проводиться через дротовий інтерфейс (порт Ethernet), тобто використовуючи Ethernet-з'єднання. Хоча можна це робити й через бездротовий інтерфейс, але ми цього не

рекомендуємо, тому що при досить великій кількості точок доступу може виникнути плутанина в налаштуваннях.

1. У вікні Мережні підключення відключите мережні адаптери (рис. 3.2). У контекстному меню необхідно вибрати «Відключити» для кожного адаптера.

У результаті всі комп'ютери будуть ізольовані друг від друга, мережних підключень немає.

2. Налаштуємо мережні адаптери для зв'язку із точкою доступу.

Підключення через локальну мережу → Властивості → Протокол TCP/IP → Властивості

Використовувати наступний Ip-Адресу

Укажіть адресу 192.168.0.xxx, де xxx – номер вашого комп'ютера (1, 2, 3 і т.д). Укажіть маску 255.255.255.0

Ввімкніть кабельне з'єднання

3. Підключаємося до точки доступу.

З'єднуємо точку доступу мережним кабелем з мережним адаптером ПК, подаємо живлення.

Скидаємо налаштування точки. Для цього протягом п'яти секунд натискаємо й утримуємо кнопку reset. Не вимикайте живлення при натиснутій reset!

Час завантаження точка - близько 20 секунд. По закінченню завантаження на точці загоряються індикатори Power і LAN.

У браузері Internet Explorer наберіть http://192.168.0.50. З'явиться запрошення на введення імені й пароля (рис. 3.9).

4. Починаємо налаштування.

Введіть у якості імені користувача «admin» з порожнім паролем. Настроїмо спочатку Ip-Адресу точки. Це потрібно лише в тому випадку, коли у вас багато точок доступу. На вкладці *Home* натискаємо кнопку *Lan* (ліворуч).

Виставляємо адресу 192.168.0.xxx, де xxx – унікальний номер точки.

Маска 255.255.255.0

Default Gateway 192.168.0.50

По завершенню *налаштування* слід натиснути «Apply», щоб перезавантажити точку з новими налаштуваннями.

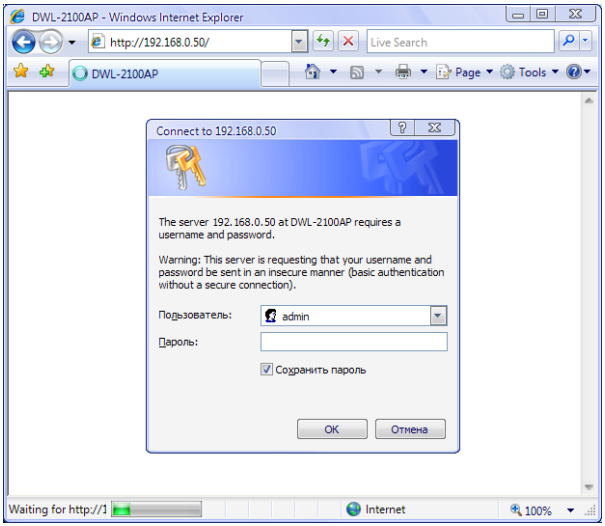


Рисунок 3.9 – Вікно запрошення на введення імені й пароля

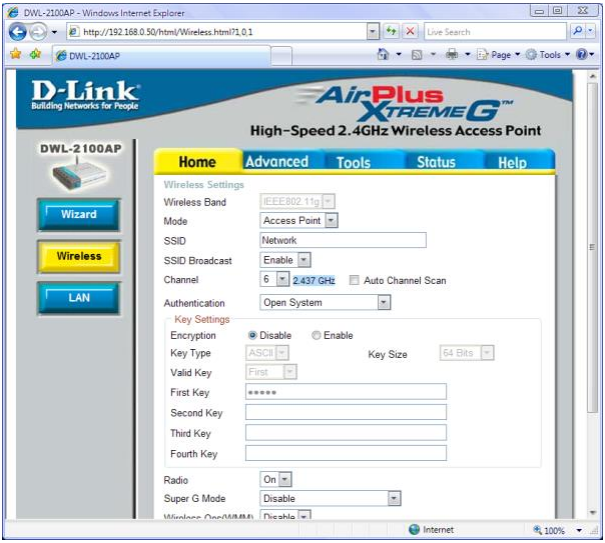


Рисунок 3.10 – Вкладка Home

5. Ввімкнення режиму точки доступу.

Дочекайтеся завантаження точка й уведіть у браузері нова адреса http://192.168.0.xxx

На вкладці *Home* натисніть кнопку *Wireless* (ліворуч)

Встановлюємо (рис. 3.10):

Mode (режим): *Access Point*
SSID: Network
SSID Broadcast: Enable
Channel: 6
Authentication: *Open System*
Encryption: Disable

Помітьте, що обрані нами установки не забезпечують безпека бездротового підключення й використовуються тільки з метою навчання.

Якщо потрібно зробити більш тонкі налаштування, перейдіть на вкладку *Advanced*. Рекомендуємо перед настроюванням точка доступу прочитати документацію про налаштування; короткий опис усіх параметрів є на вкладці *Help*.

По завершенню настроювання потрібно натиснути «Apply», щоб перезавантажити точку з новим налаштуванням.

Відключить точку від мережного інтерфейсу. Тепер ваша точка налаштована на підключення бездротових клієнтів. У найпростішому випадку, щоб надати клієнтам Internet, потрібно до точка приєднати широкосмуговий канал або Adsl-*Модем*.

Клієнтські комп'ютери підключаються аналогічно, як це було описано в попередньому прикладі (рис. 3.7).

3.3. Топологія типу «зірка»

«Зірка» – це топологія з явно виділеним центром, до якого підключаються всі інші абоненти (рис. 3.11). Увесь обмін інформацією йде винятково через центральну точку доступу, на яку в результаті лягає дуже велике навантаження.

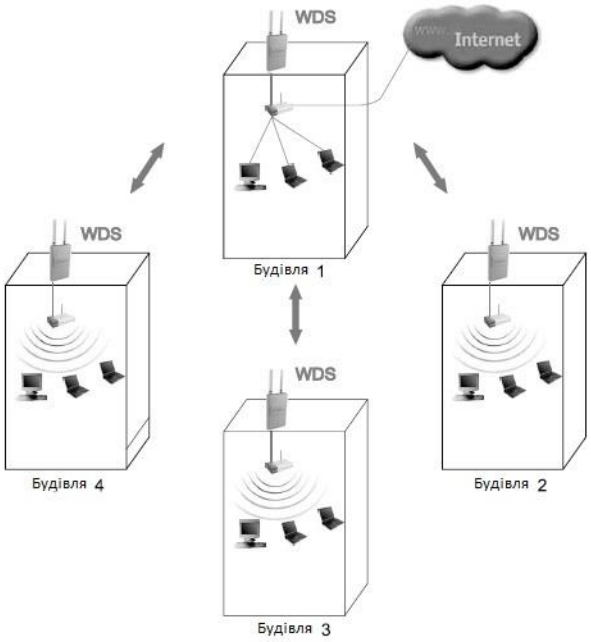


Рисунок 3.11 – Топологія типу «зірка»

Якщо говорити про стійкість «**зірки»** до відмов точок, то вихід з ладу звичайної точки доступу ніяк не впливає на функціонування частини мережі, що залишилася, зате будь-яка відмова центральної точки робить мережа повністю непрацездатної.

Істотний недолік топології «зірка» полягає в обмеженні кількості абонентів. Тому що всі точка працюють на одному каналі, звичайно центральний абонент може обслуговувати не більш 10 периферійних абонентів через велике падіння швидкості.

У більшості випадків, наприклад для об’єднання декількох районів у місті, використовують комбіновані топології.

3.4. Топологія міст типу «точка-точка»

Створимо міст типу «точка-точка». Для цього знадобиться дві точки доступу.

1. Налаштуємо IP-адресу провідним інтерфейсам точок доступу:

Відімкнемо бездротові інтерфейси й запускаємо браузер Internet Explorer, в адресному рядку вводимо 192.168.0.50, за замовчуванням логін: admin, пароль порожньої.

Рисунок 3.12 – Налаштування мостового з'єднання

Заходимо на вкладку Home → LAN і в поле IP address уводимо: 192.168.0.5X, де X – номер точки доступу (наприклад, 1, 2, 3 і т.д.).

2. Налаштовуємо мостове з'єднання, показане на рис. 3.12.

3. Заходимо на вкладку Home → Wireless у першій точці доступу робимо режим (Mode): *WDS* (рис. 3.13), у другий – *WDS* with AP (рис. 3.14).

4. У другій точці вказуємо *SSID*: Network (у першій точці доступу можна вказати будь-який *SSID*, тому що до неї однаково не можна буде приєднатися бездротовим клієнтам).

5. У двох точках доступу вказуємо той самий канал: 6.

У першій точці доступу в поле Remote AP *MAC Address* указуємо Mac-Адресу другої точки (наприклад, 00:13:46:75:85:64), у другій точці доступу вказуємо Mac-Адресу першої точки (наприклад, 00:17:9A:01:5C:84).

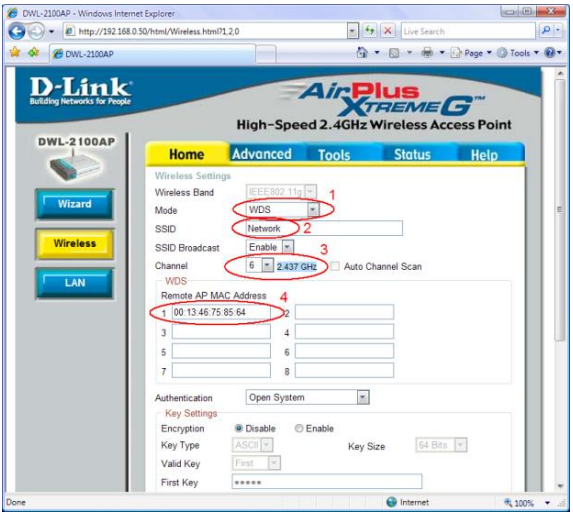


Рисунок 3.13 – Вкладка Home → Wireless режим (Mode): WDS

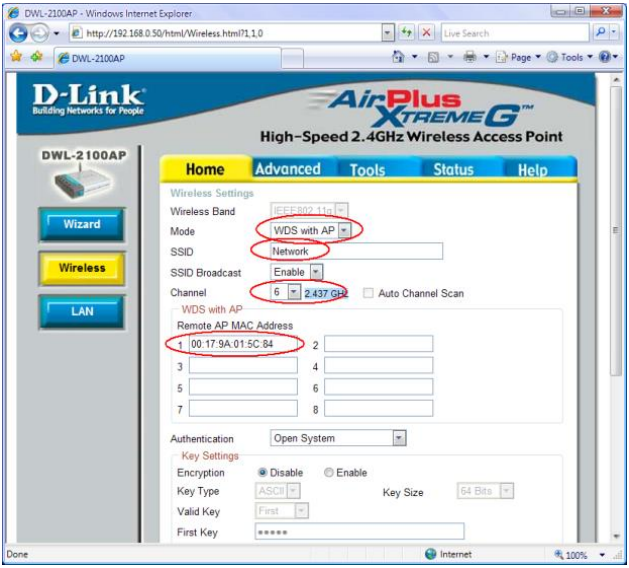


Рисунок 3.14 – Вкладка Home → Wireless режим (Mode): – WDS with AP

При бажанні можна налаштувати шифрування даних.

Застосовуємо настроювання, і після перезавантаження точка доступу ввійдуть у режим мосту.

6. Перевіряємо з'єднання:

Підключаємося бездротовими адаптерами до другої точка доступу.

Командою *ping* послідовно перевіряємо другу точку, першу й, якщо перша точка підключена до Internet, сайт: ping 192.168.0.5X, де X - номер точки доступу.

3.5. Топологія міст типу «точка – багато точок»

Створимо міст «точка – багато точок» (рис. 3.15). Для цього нам знадобиться не менш трьох крапок доступу.

1. Одна точка доступу переводиться в режим *WDS*:

Заходимо на вкладку Home → Wireless, у першій точці доступу встановлюємо режим (Mode): *WDS*.

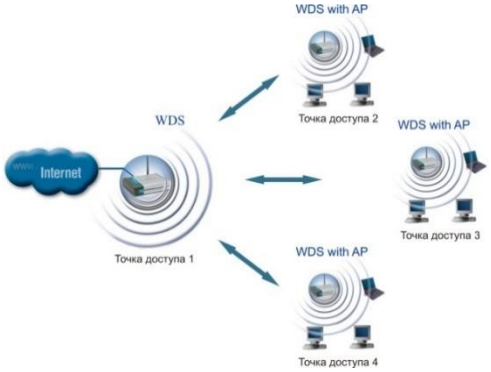


Рисунок 3.15 – Міст «точка – багато точок»

Указуємо канал (наприклад, 1, 6 або 11). У полях Remote AP *MAC Address* указуємо Mac-Адреси інших крапок доступу.

При бажанні можна настроїти шифрування даних.

2. Інші точка доступу переводяться в режим *WDS* with AP (рис. 3.14):

3. Заходимо на вкладку Home → Wireless і задаємо режим (Mode): *WDS* with A P.

4. Указуємо *SSID*: Networkx, де X – номер підмережі.

5. Указуємо такий же канал, як і в першої точці доступу.

6. У всіх точках доступу в поле Remote AP *MAC Address* указуємо Mac-Адресу першої точки.

7. Якщо в першій точці налаштовано шифрування даних, то тут теж треба налаштувати точно таке ж шифрування.

8. Застосовуємо налаштування, і після перезавантаження точки доступу ввійдуть у режим мосту.

9. Перевіряємо з'єднання:

Підключаємося бездротовими адаптерами до будь-якої точки доступу. Командою ping послідовно перевіряємо другу (третю або четверту) крапку, першу й сайт в Internet: ping 192.168.0.5X, де X – номер точка доступу.

3.6. Режим повторювача

Може виникнути ситуація, коли виявляється неможливо (незручно) з'єднати точку доступу із провідною інфраструктурою або яка-небудь перешкода утрудняє здійснення зв'язку точки доступу з місцем розташування бездротових станцій клієнтів прямо. У такій ситуації можна використовувати точку в *режимі повторювача (Repeater)* (рис. 3.16).

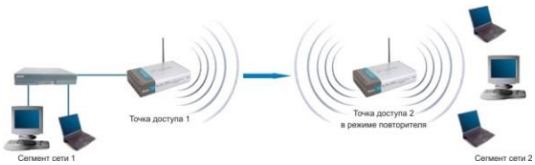


Рисунок 3.16 – Режим повторювача

Аналогічно провідному повторювачу, бездротовий *повторювач* просто ретранслює всі пакети, що отримали на його бездротовий інтерфейс. Ця ретрансляція здійснюється через той же канал, через який вони були отримані.

При застосуванні точки доступу в режимі повторювача слід пам’ятати, що накладення широкомовних доменів може привести до скорочення пропускної здатності каналу вдвічі, тому що початкова *точка доступу* також «чує» ретрансльований сигнал.

Режим повторювача не включено в стандарт 802.11, тому для його реалізації рекомендується використовувати однотипне встаткування (аж до версії прошивання) і від одного виробника. З появою *WDS* даний режим втратив свою актуальність, тому що *WDS* заміняє його. Однак його можна зустріти в старих версіях прошивань і в застарілому обладнанні.

3.7. Режим клієнта

При переході від провідної архітектури до бездротової іноді можна виявити, що наявні мережні пристрої підтримують провідну *мережу Ethernet*, але не мають інтерфейсних роз’ємів для бездротових мережних адаптерів. Для підключення таких пристроїв до бездротової мережі можна використовувати точку доступу «клієнт» (рис. 3.17).

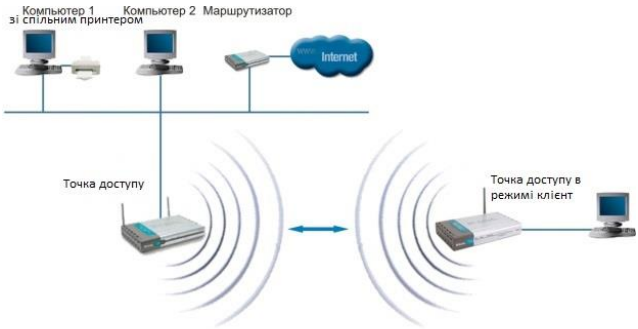


Рисунок 3.17 – Режим клієнта

За допомогою точки доступу, що функціонує в режимі клієнта, до бездротової мережі підключається тільки один пристрій. Цей режим не включено в стандарт 802.11 і підтримується не всіма виробниками.

4. ОРГАНІЗАЦІЯ І ПЛАНУВАННЯ БЕЗДРОТОВИХ МЕРЕЖ

При організації бездротової локальної мережі необхідно враховувати деякі особливості навколишнього середовища. На якість і дальність роботи зв'язку впливає безліч фізичних факторів: число стін, перекриттів і інших об'єктів, через які повинен пройти сигнал. Звичайна *відстань* залежить від типу матеріалів і радіочастотного шуму від інших електроприладів у приміщенні. Для поліпшення якості зв'язку треба додержуватися базових принципів:

– Скоротити число стін і перекриттів між абонентами бездротової мережі – кожна стіна й перекриття віднімає від максимального радіуса від 1 м до 25 м. Розташувати точку доступу й абонентів мережі так, щоб кількість перешкод між ними було мінімальним.

– Перевірити кут між точками доступу й абонентами мережі. Стіна товщиною 0,5 м при куті в 30 градусів для радіохвилі стає стіною товщиною 1 м. При куті у 2 градуси стіна стає перешкодою товщиною в 12 м! Треба намагатися розташувати абонентів мережі так, щоб сигнал проходив під кутом в 90 градусів до перекриттів або стін.

– Будівельні матеріали впливають на проходження сигналу по-різному – цілком металеві двері або алюмінієве облицювання негативно позначаються на передачі радіохвиль. Бажане, щоб між абонентами мережі не було металевих або залізобетонних перешкод.

– За допомогою програмного забезпечення перевірки потужності сигналу треба позиціювати антену на краще приймання.

– Вилучити від абонентів бездротових мереж принаймні на 1-2 метри електроприлади, що генерують радіоперешкоди, мікрохвильові печі, монітори, електромотори, ИБП. Для зменшення перешкод ці прилади повинні бути надійно заземлені.

– Якщо використовуються бездротові телефони стандарту 2,4 ГГц або встаткування X-10 (наприклад, системи сигналізації),

якість бездротового зв’язку може помітно погіршитися або перерватися.

Для типового житла відстань зв’язку не представляє особливої проблеми. Якщо виявлений невпевнений зв’язок у межах будинку, то треба розташувати точку доступу між кімнатами, які слід зв’язати бездротовою мережею.

Для виявлення точок доступу, що попадають у зону дії бездротової мережі, і визначення каналів, на яких вони працюють, можна використовувати програму Network Stumbler (http://www.stumbler.net/). З її допомогою також можна оцінити співвідношення" сигнал-шум" на обраних каналах.

4.1. Офісна мережа

Проста бездротова мережа для невеликого офісу або домашнього використання *(Small Office / Home Office – SOHO) може бути побудовано на основі однієї* точки доступу (рис. 4.1).

Для організації мережі адаптери переводяться в режим інфраструктури, а точка доступу – у режим точка доступу. При цьому створюється одна зона обслуговування, у якій перебувають усі користувачі мережі.

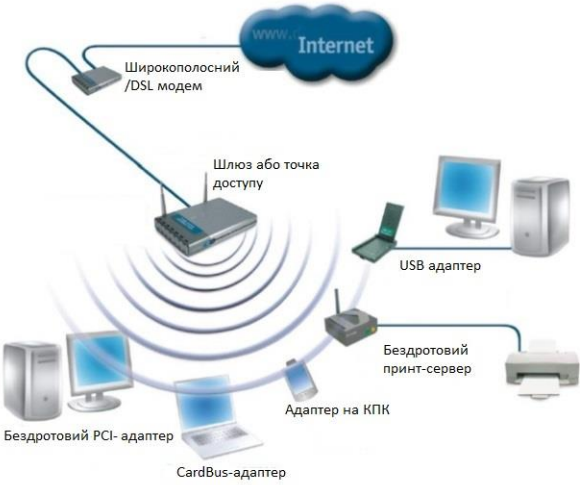


Рисунок 4.1 – Офісна мережа

При розміщенні точка доступу при розгортанні малої мережі слід забезпечити достатня якість зв'язку на всіх робочих місцях, а також зручність у розміщенні самої точка. Типовий розв'язок – закріпити крапку доступу безпосередньо на фальш-стелі, при цьому проведення електроживлення й провідної мережі будуть проходити над фальш-стелею або в коробах.

Необхідно мати на увазі, що при розширенні мережі й збільшенні кількості користувачів швидкість зв'язку буде падати (пропорційно числу користувачів). Найбільша розумна кількість користувачів звичайно становить 16-20. Крім цього швидкість і якість зв'язки залежать і від відстані між клієнтом і точкою. Ці міркування можуть зажадати розширення базової мережі.

Для розширення мережі можна використовувати uplink-*порт* точки доступу. Він може використовуватися як для об'єднання базових зон обслуговування в мережу, так і для інтеграції в наявну провідну або бездротову інфраструктуру, наприклад для забезпечення користувачів доступом до поділюваних ресурсів інших підрозділів або для підключення до Internet.

При розширенні мережі необхідно стежити щоб частоти сусідніх точок доступу не перекривалися, щоб уникнути взаємних перешкод і зниження швидкості передачі. Це досягається налаштуванням сусідніх точок на канали, що не перекриваються по частоті, 1, 6 чергуючи канали таким чином, що сусідні точки з каналами 1, 6 і 11 розміщалися у вершинах рівностороннього трикутника, можна охопити бездротовим зв'язком як завгодно більшу площу без перекриття частот (рис. 4.2).

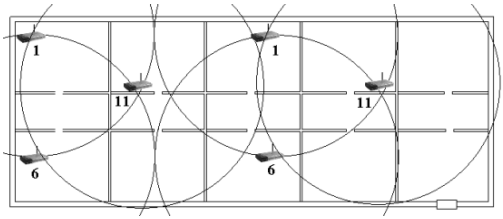


Рисунок 4.2 – Розширення бездротової мережі

На розгортання бездротових мереж використовувані додатки впливають по-різному. Найбільш важливі фактори – це:

– Розрахункова швидкість у перерахуванні на один клієнта;
– Типи використовуваних додатків;
– Затримки в передачі даних.

Розрахункова швидкість кожного клієнта зменшується з уведенням у зону обслуговування нових клієнтів. Отже, якщо вдома або в офісі використовуються вимогливі до швидкості додатка (наприклад, програма Internet-Телефонії *Skype*), необхідно збільшити кількість точок доступу на одиницю площі (рис. 4.3).

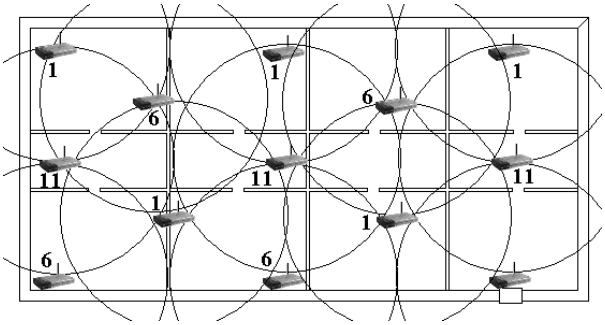


Рисунок 4.3 – Розширення бездротової мережі з максимальною швидкістю

Для визначення границі дії точок доступу використовується ноутбук з установленою програмою Network Stumbler. Вона показує, на якій швидкості буде працювати адаптер залежно від відстані від точка доступу. У міру видалення швидкість автоматично падає, і при досягненні граничного рівня необхідно ставити нову точку.

Об’єднання всіх точок доступу в офісі в локальну мережу можна здійснити декількома способами. Найпростішим і розповсюдженим методом організації є об’єднання через провідну інфраструктуру (рис. 4.4).

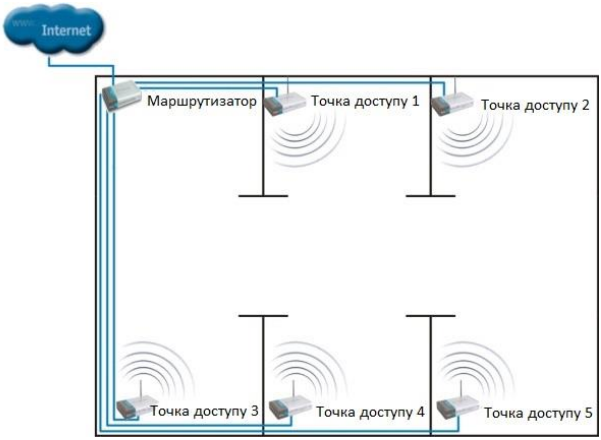


Рисунок 4.4 – Об'єднання точок доступу через провідну інфраструктуру

У такому випадку встановлюється комутатор, до якого підключаються точки доступу за допомогою звитої пари через uplink-*порт*. Також до цього комутатора можна підвести широкосмуговий Internet. Перевагою такого підключення є простота налаштування зони дії точок доступу на різні канали, недоліком - прокладка проводів від точок доступу до комутатора.

Другий спосіб - підключення з використанням режиму *WDS* (рис. 4.5).

Одна точка доступу, яка має підключення до Internet, переводиться в мостовий режим *WDS*, інші точка настроюються на той же канал, що й перша, і встановлюється режим *WDS* with AP. Використання такого способу небажане, тому що всі точка працюють на одному каналі, і при досить великій їхній кількості різко зменшується швидкість. Рекомендується встановлювати не більш 2-3 точок.

Третій спосіб підключення аналогічний попередньому, але додатково до кожної точки доступу через провідний інтерфейс підключена ще одна точка, що працює на іншому каналі, для організації зв'язку в одній кімнаті (рис. 4.6).

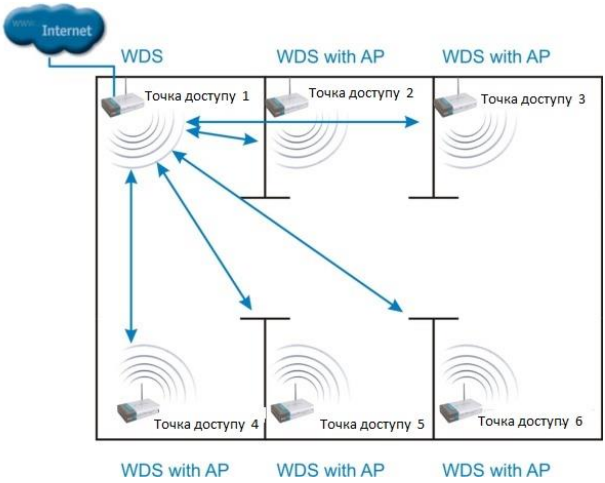


Рисунок 4.5 – Об'єднання точок доступу з використанням розширеного режиму WDS

Тут переводяться ті точки доступу в режим WDS, які будуть пов'язані з першої, а інші через провідні інтерфейси підключаються до них. Вони повинні працювати в режимі точка доступу й на інших каналах, щоб не було колізій. Перевагою такого способу підключення є повна відсутність провідної інфраструктури (за винятком зв'язку між сусідніми точками), недоліком – висока вартість, у зв'язку з більшою кількістю точок доступу, і використання одного каналу для зв'язку з базовою точкою.

Щоб користувач міг пересуватися від однієї точка доступу до іншої без втрати доступу до мережних служб і розриву з'єднання, у всьому встаткуванні компанії D-Link передбачена функція роумінгу.

Роумінг – це можливість радіопристрою переміщатися за межі дії базової станції й, перебуваючи в зоні дії «гостьової» станції, мати доступ до «домашньої» мережі (рис. 4.7).

При організації роумінгу всі точки доступу, що забезпечують роумінг, конфігуруються на використання однакового ідентифікатора зони обслуговування (SSID). Усі

точка доступу відносяться до одного широкомовного домену, або одного домену роумінгу.

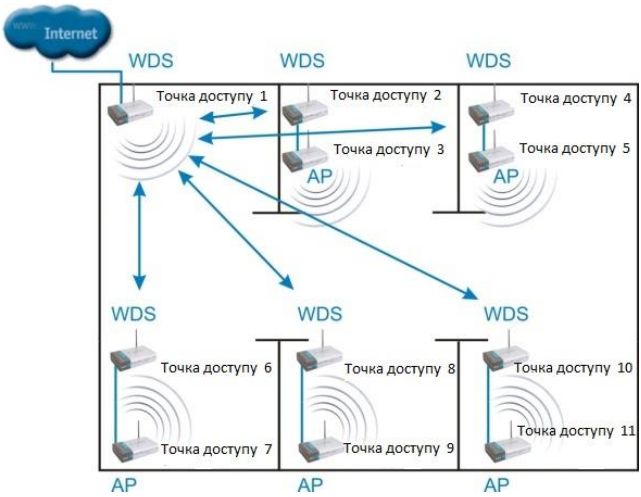


Рисунок 4.6 – Об'єднання точок доступу з додатковими точками

Рисунок 4.7 – Роумінг

Механізм визначення моменту часу, коли необхідно почати процес роумінгу, не визначено в стандарті 802.11, і, таким чином, залишений на розсуд постачальників устаткування. Найбільш простий, широко розповсюджений, алгоритм перемикання полягає в тому, що адаптер взаємодіє з однієї точкою аж до того

моменту, коли рівень сигналу не впаде нижче припустимої межі. Після цього здійснюється пошук точка доступу з однаковим SSID і максимальним рівнем сигналу, і перепідключення до неї.

Роумінг включає значно більше процесів, що необхідно для пошуку точки доступу, з якою можна зв'язатися. Опишемо деякі із завдань, які повинні вирішуватися в ході роумінгу на канальному рівні:

– Попередня точка доступу повинна визначити, що клієнт іде з її області дії.

– Попередня точка доступу повинна буферизувати дані, призначені для клієнта, що здійснює роумінг.

– Нова точка доступу повинна показати попередній, що клієнт успішно перемістився в її зону.

– Попередня точка доступу повинна послати буферизовані дані новій точці доступу.

– Попередня точка доступу повинна визначити, що клієнт покинув її зону дії.

– Точка доступу повинна обновити таблиці MAC-Адрес на комутаторах інфраструктури, щоб уникнути втрати даних клієнта, що переміщається.

4.2. Мережа між декількома офісами

Бездротовий зв'язок може використовуватися для об'єднання підмереж окремих будинків, наприклад центрального офісу й філій, там, де прокладка кабелю між будинками небажана або неможлива (рис. 4.8).

Для організації зв'язку між будинками можуть використовуватися зовнішні бездротові точки, що працюють у режимі мосту. Через uplink-*порт* зовнішня точка підключається до звичайного комутатора й через нього забезпечує зв'язок з усіма комп'ютерами в підмережі.

Зовнішні бездротові точки мають водонепроникний термостатований корпус, систему грозового захисту, систему живлення Power-over-Ethernet. Завдяки змінній антені можна забезпечувати стійкий радіозв'язок на відстані до декількох кілометрів на спеціалізовані вузькоспрямовані антени.

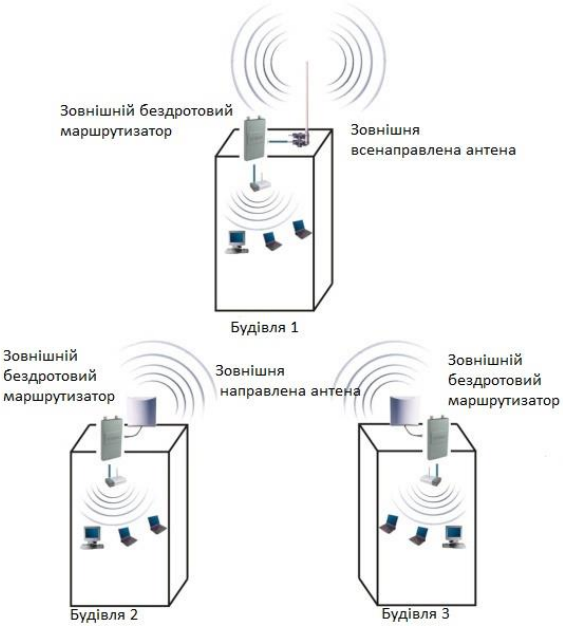


Рисунок 4.8 – Мережа між декількома офісами

При організації зовнішнього бездротового зв'язку особливу увагу слід звернути на забезпечення безпеки передачі даних, у зв'язку з її більшою уразливістю як при прослуховуванні, так і у випадку прямого фізичного впливу. Тому рекомендується використовувати точку доступу, спеціально призначені для зовнішнього застосування, що й дозволяють залучити автентифікацію, контроль доступу й шифрування переданих даних.

Необхідно також звернути увагу на те, що для зовнішніх точок передбачена більш складна процедура одержання дозволів на використання частот. Правила застосування радіочастотного спектра в Україні наведені в Додатоку Б.

4.3. Бездротова технологія Wimax

При всьому багатстві вибору мережних підключень складно одночасно дотримати трьох основних вимог до мережних з'єднань: висока пропускна здатність, надійність і мобільність. Розв'язати подібне завдання може наступне покоління бездротових технологій – Wimax (Worldwide Interoperability for Microwave Access), стандарт IEEE 802.16.

Для просування й розвитку технології *Wimax* був сформований Wimax-*Форум*: http://www.wimaxforum.org на базі робочої групи *IEEE* 802.16, створеної в 1999 році. У форум увійшли такі фірми, як Nokia, Harris Corporation, *Ensemble*, Crosspan і Aperto. До травня 2005 року форум поєднував уже більш як 230 учасників. У тому ж році Всесвітній з'їзд із питань інформаційного товариства (World Summit on *Information* Society – WSIS) сформулював наступні завдання, які були покладені на технологію *Wimax*:

1. Забезпечити за допомогою *Wimax* доступ до послуг інформаційних і комунікаційних технологій для невеликих поселень, віддалених регіонів, ізольованих об'єктів, враховуючи при цьому, що в країнах, які розвиваються 1, 5 мільйони поселень із числом жителів більш як 100 людей не підключені до телефонних мереж і не мають кабельного з'єднання з великими містами.

2. Забезпечити за допомогою *Wimax* доступ до послуг інформаційних і комунікаційних технологій більш половини населення планети в межах досяжності, враховуючи при цьому, що загальне число користувачів Internet у 2005 році становило приблизно 960 млн чоловік, або близько 14,5 % усього населення Землі.

Мета технології *Wimax* полягає в тому, щоб надати універсальний бездротовий доступ для широкого спектра пристроїв (робочих станцій, побутової техніки «розумного будинку», *портативних пристроїв* і мобільних телефонів) і їх логічного об'єднання – локальних мереж. Треба відзначити, що дана технологія має ряд переваг:

– У порівнянні із провідними (*xdsl* або широкосмуговим), бездротовими або супутниковими системами мережі *Wimax* повинні дозволити операторам і сервіс-провайдерам економічно ефективно охопити не тільки нових потенційних користувачів, але й розширити спектр інформаційних і комунікаційних технологій для користувачів, що вже мають фіксований (стаціонарний) доступ.

– Стандарт поєднує технології рівня *оператора зв'язку* (для об'єднання багатьох підмереж і надання їм доступу до Internet), а також технології «останньої милі» (кінцевого відрізка від точки входу в мережу провайдера до комп'ютера користувача), що створює універсальність і, як наслідок, підвищує надійність системи.

– Бездротові технології більш гнучкі й, як наслідок, простіше в розгортанні, тому що в міру потреби можуть масштабуватися.

– Простота установки як фактор зменшення витрат на розгортання мереж у країнах, що розвивати, малонаселених або вилучених районах.

– Дальність обхвату є істотним показником системи радіозв'язку. На цей час більшість бездротових технологій широкосмугової передачі даних вимагають наявності прямої видимості між об'єктами мережі. *Wimax* завдяки використанню технології *OFDM* створює зони покриття в умовах відсутності прямої видимості від клієнтського обладнання до базової станції, при цьому відстані обчислюються кілометрами.

– Технологія *Wimax* містить протокол IP, що дозволяє легко й прозоро інтегрувати її в локальні мережі.

– Технологія *Wimax* підходить для фіксованих, переміщуваних і рухливих об'єктів мереж на єдиній інфраструктурі.

Система *Wimax* складається із двох основних частин:

– Базова станція *Wimax*, може розміщатися на висотному об'єкті – будинку або вежі.

– Приймач *Wimax*: антена із приймачем (рис. 4.9).

З'єднання між базовою станцією й клієнтським приймачем проводиться у СВЧ діапазоні 2-11 ГГц. Дане з'єднання в

ідеальних умовах дозволяє передавати дані зі швидкістю до 20 Мбіт/с і не вимагає, щоб станція перебувала на відстані *прямої* видимості від користувача. Цей режим роботи базової станції *Wimax* близький широко використовуваному стандарту *802.11* (Wi-Fi), що допускає сумісність уже випущених клієнтських пристроїв і *Wimax*.

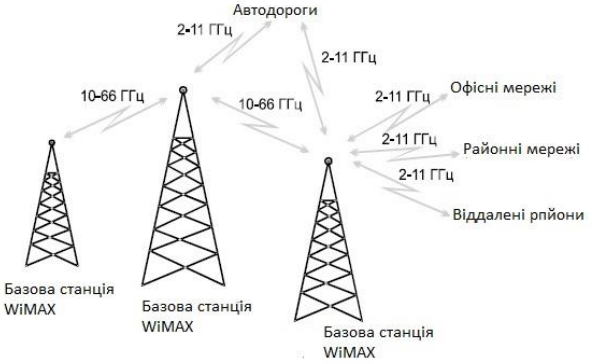


Рисунок 4.9 – Архітектура Wimax

Слід пам’ятати, що технологія *Wimax* застосовується як на «*останній милі»* – кінцевій ділянці між провайдером і користувачем, – так і для надання доступу регіональним мережам: офісним, районним.

Між сусідніми базовими станціями встановлюється постійне з’єднання з використанням надвисокої частоти 10-66 ГГц радіозв’язку *прямої* видимості. Дане з’єднання в ідеальних умовах дозволяє передавати дані зі швидкістю до 120 Мбіт/с. Обмеження *за* умовою *прямої* видимості, зрозуміло, не є перевагою, однак воно накладається тільки на базові станції, що бере участь у цільному покритті району, що цілком можливо реалізувати при розміщенні обладнання.

Як *мінімум* одна з базових станцій може бути постійно пов’язана з мережею провайдера через широкосмугове швидкісне з’єднання. Фактично, чим більше станцій мають *доступ* до мережі провайдера, тем вище швидкість і *надійність* передачі даних. Однак навіть при невеликій кількості точок

система здатна коректно розподілити навантаження шляхом стільникової топології.

На базі стільникового принципу розробляються також шляхи побудови оптимальної мережі, що обгинає великі об'єкти (наприклад, гірські масиви), коли серія послідовних станцій передає дані по естафетному принципу. Подібні розробки планується включити в наступну версію стандарту. Очікується, що ці зміни дозволять суттєво підняти швидкість (рис. 4.10).

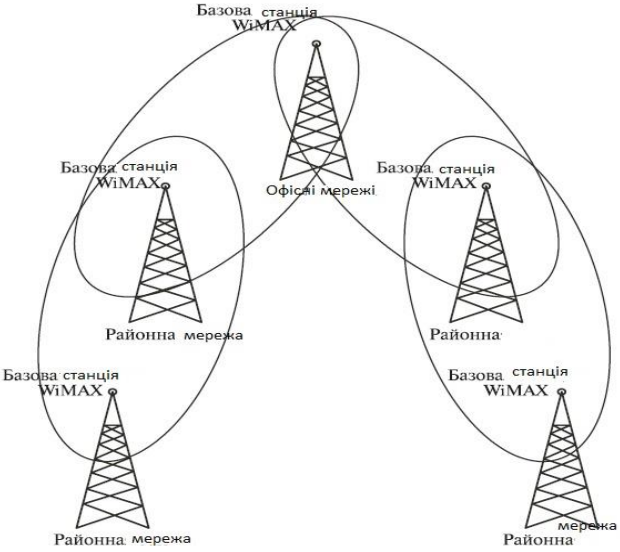


Рисунок 4.10 – Покриття Wimax

За структурою мережі стандарту IEEE 802.16 дуже схожі на традиційні мережі мобільного зв'язку: тут теж є базові станції, які діють у радіусі до 50 км, при цьому їх також необов'язково встановлювати на вежах. Для них цілком підходять дах будинків, потрібно лише дотримання умови прямої видимості між станціями. Для з'єднання базової станції з користувачем необхідна наявність абонентського обладнання. Далі сигнал може надходити по стандартному Ethernet-кабелю, як безпосередньо на конкретний комп'ютер, так і на крапку доступу

стандарту 802.11 Wi-Fi або в локальну провідну мережу стандарту Ethernet.

Це дозволяє зберегти наявну інфраструктуру районних або офісних локальних мереж при переході з кабельного доступу на Wimax. Крім того, це дає можливість максимально спростити розгортання мереж, використовуючи знайомі технології для підключення комп'ютерів.

Стандарт 802.16e-2005 увібрав у себе, що усе раніше виходили версії й тепер надає наступні режими:

- Fixed *Wimax* – фіксований доступ.
- Nomadic *Wimax* – сеансовий доступ.
- Portable *Wimax* – доступ у режимі переміщення.
- Mobile *Wimax* – мобільний доступ.

4.3.1. Fixed Wimax

Фіксований доступ являє собою альтернативу широкосмуговим провідним технологіям (*xdsl*, T1 і т.п.). Стандарт використовує діапазон частот 10-66 ГГц. Цей частотний діапазон через сильне загасання коротких хвиль вимагає прямої видимості між передавачем і приймачем сигналу (рис. 4.11).

З іншого боку, даний частотний діапазон дозволяє уникнути однієї з головних проблем радіозв'язку – багатопроменевого поширення сигналу. При цьому ширина каналів зв'язки в цьому частотному діапазоні досить велика (типове значення – 25 або 28 МГц), що дозволяє досягати швидкостей передачі до 120 Мбіт/с. Фіксований режим включався у версію стандарту 802.16d-2004 і вже використовується в ряді країн. Однак більшість компаній, що пропонують послуги Fixed Wimax, очікують швидкого переходу на портативний і надалі на мобільний Wimax.

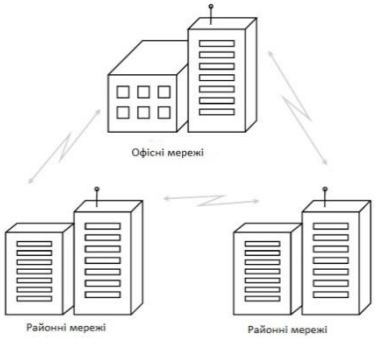


Рисунок 4.11 – Пряма видимість між передавачем і приймачем сигналу

4.3.2. Nomadic Wimax

Сеансовий (той, що кочує) доступ додав поняття сесій до вже наявного Fixed Wimax. Наявність сесій дозволяє вільно переміщати клієнтське встаткування між сесіями й відновлювати з'єднання вже за допомогою інших веж Wimax, ніж ті, що використовувалися під час попередньої сесії. Такий режим розроблений в основному для портативних пристроїв, таких як ноутбуки, КПК. Уведення сесій дозволяє також зменшити витрати енергії клієнтського пристрою, що теж немаловажливе для портативних пристроїв.

4.3.3. Portable Wimax

Для режиму Portable *Wimax* додана можливість автоматичного перемикання клієнта від однієї базової станції *Wimax* до іншої без втрати з'єднання. Однак для даного режиму усе ще обмежена швидкість пересування клієнтського встаткування – 40 км/г. Втім, уже в такому вигляді можна використовувати клієнтські пристрої в дорозі (в автомобілі при русі по житлових районах міста, де швидкість обмежена, на велосипеді, рухаючись пішки та т.п.).

Введення даного режиму зробило доцільним використання технології *Wimax* для смартфонів і КПК (рис. 4.12). У 2006 році початий випуск пристроїв, що працюють у портативному режимі

Wimax. Вважається, що до 2008 року впровадження й просування на ринок саме цього режиму було пріоритетним.

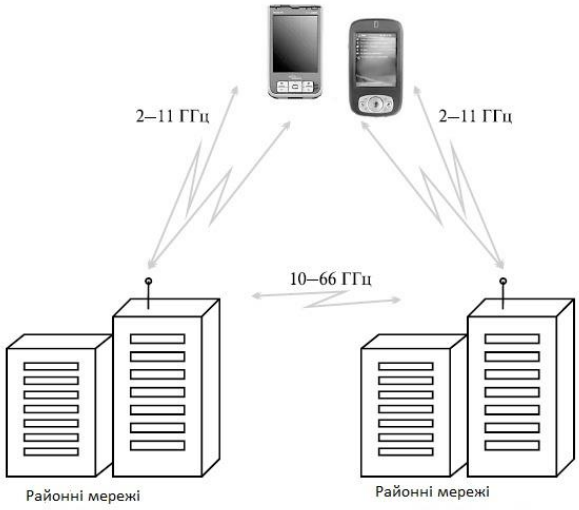


Рисунок 4.12 – Використання технології Wimax для смартфонів і КПК

4.3.4. Mobile Wimax

Цей режим був розроблено в стандарті 802.16e-2005 і дозволив збільшити швидкість переміщення клієнтського встаткування до 120 км/ч. Основні досягнення цього режиму:

– Стійкість до багатопроменевого поширення сигналу й власним перешкодам.

– Масштабована пропускна здатність каналу.

– Технологія *Time Division Duplex* (TDD), яка дозволяє ефективно обробляти асиметричний трафік і спрощує керування складними системами антен шляхом естафетної передачі сесій між каналами.

– Технологія *Hybrid-Automatic Repeat Request* (H-ARQ), яка дозволяє зберігати стійке з'єднання при різкій зміні напрямку руху клієнтського встаткування.

– Розподіл виділюваних частот і використання субканалів при високому завантаженні дозволяє оптимізувати передачу даних з урахуванням сили сигналу клієнтського встаткування.

– Керування енергоощадженням дозволяє оптимізувати витрати енергії на підтримку зв'язку *портативних пристроїв* у режимі очікування або простою.

– Технологія Network-Optimized Hard Handoff (HHO), яка дозволяє до 50 мілісекунд і менш скоротити час на перемикання клієнта між каналами.

– Технологія Multicast and Broadcast Service (MBS), яка поєднує функції DVB-H, Mediaflo і 3GPP E-UTRA для:

– досягнення високої швидкості передачі даних з використанням одночастотної мережі;

– гнучкого розподілу радіочастот;

– низького споживання енергії портативними пристроями;

– швидкого перемикання між каналами.

– Технологія Smart Antenna, що підтримує субканали й естафетну передачу сесії між каналами, що дозволяє використовувати складні системи антен, включаючи формування діаграми спрямованості, просторово-тимчасове маркування, просторове мультиплексування (ущільнення).

– Технологія Fractional Frequency Reuse, яка дозволяє контролювати накладення/перетинання каналів для повторного використання частот з мінімальними втратами.

– Розмір фрейму в 5 мілісекунд забезпечує компроміс між надійністю передачі даних шляхом використання малих пакетів і накладними витратами внаслідок збільшення числа пакетів (і, як наслідок, заголовків).

Стандарт *Wimax* сьогодні перебуває в стадії тестування. Єдина конкурентоспроможна версія стандарту, для якої існує *ліцензія* на встаткування, – це *Fixed Wimax*. Однак провайдери не поспішають заміняти дороге, але працююче встаткування новим тому, що це вимагає істотних вкладень без можливості підняти *продуктивність* (і, відповідно, ціну на послуги) і повернути вкладені кошти швидко.

При розгортанні Wimax-Мереж там, де доступу до Internet раніше не було, доводиться зустрічатися із проблемою наявності в малонаселених або вилучених регіонах достатнього числа потенційних користувачів, що володіють необхідним устаткуванням або коштами на його придбання. Те ж стосується й переходу на Mobile Wimax після його ліцензування тому, що, крім витрат провайдерів на модернізацію операторського встаткування, слід ураховувати затрати користувачів на модернізацію клієнтського встаткування: придбання Wimax-Карт і відновлення портативних пристроїв.

Другим, стримуючим фактором, є позиція багатьох фахівців, які вважають неприпустимим використання надвисоких частот радіозв'язку прямої видимості, шкідливих для здоров'я людини. Наявність веж на відстані десятків метрів від житлових об'єктів (а базові станції рекомендується встановлювати на дахах будинків) може згубно позначитися на здоров'ї жителів, особливо дітей. Однак результатів медичних експериментів, що підтверджують наявність або високу ймовірність шкоди, поки не опубліковано.

Третім фактором є, як не дивно, швидкий розвиток стандарту. Поява нових, принципово різних версій стандарту Wimax, призводить до питання про неминучу зміну встаткування через кілька років. Так, станції, що зараз працюють у режимі *Fixed Wimax*, не зможуть підтримувати *Mobile Wimax*. При переході на наступний стандарт буде потрібно відновлення частини встаткування, що відлякує великих провайдерів. На цей час впровадження й використання *Fixed Wimax* на комерційній основі можуть дозволити собі тільки невеликі компанії, які не планують значного розширення (у тому числі територіального) і використовують нові технології для залучення клієнтів.

І, нарешті, четвертим фактором є наявність конкурентного стандарту широкосмуговому зв'язку, що використовує близькі діапазони радіочастот – Wbro. Цей стандарт теж до кінця не ліцензований, однак він уже одержав певну популярність. А тому завжди існує *ймовірність*, що через кілька років кращим виявиться не *Wimax*, а Wbro. І компанії, що вклали засоби в розробку й впровадження Wimax-*Систем*, серйозно

постраждають. Втім, через схожість стандартів існує також імовірність злиття й надалі використання встаткування, що підтримує обоє стандартів одночасно.

Таким чином, при видимих перевагах стандарту ще рано говорити про тотальне впровадження технології або навіть про можливість переходу на неї й відмови від наявних мережних розв'язків. Необхідно спочатку одержати перше ліцензоване встаткування стандарту *Mobile Wimax*, а також результати польових випробувань. Потім можна чекати твердження стандартів версії 802.16f (*Fullmobile Wimax*) і 802.16m.

Перший з них містить у собі алгоритми обходу перешкод і оптимізацію стільникової топології покриття між базовими станціями. Другий стандарт повинен підняти *швидкість передачі* даних зі стаціонарним клієнтським устаткуванням до 1 Гбіт/с й мобільним клієнтським устаткуванням – до 100 Мбіт/с.

5. ПОГРОЗИ Й РИЗИКИ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

Головна відмінність бездротових мереж від провідних пов'язана з абсолютно неконтрольованою областю між кінцевими точками мережі. У досить широкому просторі мереж бездротове середовище ніяк не контролюється. Сучасні бездротові технології пропонують обмежений набір засобів керування всією областю розгортання мережі. Це дозволяє атакувальним що, перебувають у безпосередній близькості від бездротових структур, робити цілий ряд нападів, які були неможливі в провідній мережі. Обговоримо характерні тільки для бездротового оточення погрози безпеки, устаткування, яке використовується при атаках, проблеми, що виникають при роумінзі від однієї точка доступу до іншої, укриття для бездротових каналів і криптографічний захист відкритих комунікацій.

5.1. Підслуховування

Найпоширеніша проблема в таких відкритих і некерованих середовищах, як бездротові мережі, – можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати передані дані, як показано на рис. 5.1.

Рисунок 5.1 – Атака «підслуховування»

Устаткування, використовуване для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен перебувати поблизу від передавача. Перехоплення такого типу практично неможливо зареєструвати, і ще важче перешкодити їм. Використання антен і підсилювачів дає зловмисникові можливість перебувати на значній відстані від мети в процесі перехоплення.

Підслуховування дозволяє зібрати інформацію в мережі, яку згодом передбачається атакувати. Первинна мета зловмисника – зрозуміти, хто використовує мережу, які дані в ній доступні, які можливості мережного встаткування, у які моменти його експлуатують найбільше й найменш інтенсивно і яка територія розгортання мережі. Усе це придається для того, щоб організувати атаку на мережу. Багато загальнодоступні мережні протоколи передають таку важливу інформацію, як ім'я користувача й пароль, відкритим текстом. Перехоплювач може використовувати добуті дані для того, щоб одержати доступ до мережних ресурсів. Навіть якщо передана інформація зашифрована, у руках зловмисника виявляється текст, який можна запам'ятати, а потім уже розкодувати.

Інший спосіб підслуховування – підключення до бездротової мережі. Активне підслуховування в локальній бездротовій мережі звичайно засноване на неправильному використанні протоколу *Address Resolution Protocol* (ARP). Споконвічно ця технологія була створена для «прослуховування» мережі. Насправді ми маємо справу з атакою типу MITM (Man In The Middle – «людей посередині») на рівні зв'язку даних. Вони можуть ухвалювати різні форми й використовуються для руйнування конфіденційності й цілісності сеансу зв'язку. Атаки MITM більш складні, ніж більшість інших атак: для їхнього проведення потрібна докладна інформація про мережу. Зловмисник звичайно підмінює ідентифікацію одного з мережних ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його й потім завершує з'єднання з необхідним ресурсом, а потім пропускає всі з'єднання із цим ресурсом через свою станцію. При цьому атакувальний може посилати й

змінювати інформацію або підслуховувати всі переговори й потім розшифровувати їх.

Атакувальний посилає Arp-Відповіді, на які не було запиту, до цільової станції локальної мережі, яка відправляє йому весь трафік, що проходить через неї. Потім зловмисник буде відсилати пакети зазначеним адресатам.

Таким чином, бездротова станція може перехоплювати трафік іншого бездротового клієнта (або провідного клієнта в локальній мережі).

5.2. Відмова в обслуговуванні (Denial of Service – DOS)

Повну паралізацію мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції й клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним (рис. 5.2).

Рисунок 5.2 – Атака «відмова в обслуговуванні» у бездротових комунікаціях

Ця атака виключає всі комунікації в певному районі. Якщо вона проводиться в досить широкій області, то може зажадати значних потужностей. Атаку DOS на бездротові мережі важко запобігти або зупинити. Більшість бездротових мережних технологій використовує неліцензовані частоти – отже, припустима інтерференція від цілого ряду електронних пристроїв.

5.3. Глушіння клієнтської станції

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, і канал виходить із ладу. Атакувальний може використовувати різні способи глушіння.

Глушіння клієнтської станції дає шахраєві можливість підставити себе на місце заглушеного клієнта, як показано на рис. 5.3.

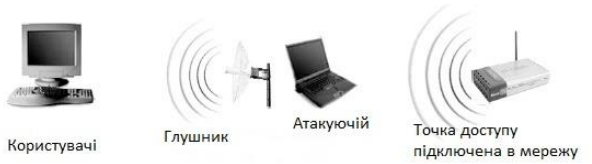


Рисунок 5.3 – Атака глушіння клієнта для перехоплення з'єднання

Також глушіння може використовуватися для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

5.4. Глушіння базової станції

Глушіння базової станції надає можливість підмінити її атакувальною станцією, як показано на рис. 5.4. Таке глушіння позбавляє користувачів доступу до послуг.

Рисунок 5.4 – Атака глушіння базової станції для перехоплення з'єднання

Як відзначалося вище, більшість бездротових мережних технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи спостереження й мікрохвильові печі, можуть впливати на роботу бездротових мереж і глушити бездротове з'єднання. Щоб запобігти таким випадкам ненавмисного глушіння, перш ніж купувати дороге бездротове встаткування, треба ретельно проаналізувати місце його установки. Такий аналіз допоможе переконатися в тому, що інші пристрої не перешкодять комунікаціям.

5.5. Погрози крипто-захисту

У бездротових мережах застосовуються *криптографічні засоби* для забезпечення цілісності й конфіденційності інформації. Однак помилки приводять до порушення комунікацій і використанню інформації зловмисниками.

WEP – це криптографічний механізм, створений для забезпечення безпеки мереж стандарту 802.11. Цей механізм розроблений з єдиним статичним ключем, який застосовується всіма користувачами. *Керівний доступ* до ключів, часта їхня зміна й *виявлення порушень* практично неможливі. Дослідження Wep-*Шифрування* виявило вразливі місця, через які атакувальний може повністю відновити ключ після захвата мінімального мережного трафіка. В Internet є засоби, які дозволяють зловмисникові відновити ключ протягом декількох годин. Тому на *WEP* не можна покладатися як на засіб автентифікації й конфіденційності в бездротовій мережі. Використовувати описані криптографічні механізми краще, чим не використовувати ніяких, але, з урахуванням відомої уразливості, необхідні інші методи захисту від атак. Усі бездротові *комунікаційні мережі* піддаються атакам прослуховування в період контакту (установки з'єднання, сесії зв'язку й припинення з'єднання). Сама природа бездротового з'єднання не дозволяє його контролювати, і тому воно вимагає захисту. Керування ключем, як правило, викликає додаткові проблеми, коли застосовується при роумінзі й у випадку

загального користування *відкритим середовищем*. Далі ми більш уважно розглянемо проблеми криптографії і їх розв'язку.

5.6. Анонімність атак

Бездротовий доступ забезпечує повну анонімність атаки. Без відповідного встаткування в мережі, що дозволяє визначати місце розташування, що атакує може легко зберігати анонімність і ховатися де завгодно на території дії бездротової мережі. У такому випадку зловмисника важко піймати й ще складніше передати справа до суду.

У недалекому майбутньому прогнозується погіршення розпізнаваності атак в Internet через широке поширення анонімних входів через небезпечні точки доступу. Уже існує багато сайтів, де публікуються списки таких точок, які можна використовувати з метою вторгнення. Важливо відзначити, що багато шахраїв вивчають мережі не для атак на їхні внутрішні ресурси, а для одержання безплатного анонімного доступу в Internet, прикриваючись яким, вони атакують інші мережі. Якщо оператори зв'язку не вживають запобіжних заходів проти таких нападів, вони повинні відповідати за шкоду, заподіяну іншим мережам при використанні їх доступу до Internet.

5.7. Фізичний захист

Пристрої бездротового доступу до мережі повинні бути маленькими й середніми (КПК, ноутбуки), як і точка доступу. Крадіжка таких пристроїв багато в чому призводить до того, що зловмисник може потрапити в мережу, не вживаючи складних атак, тому що основні механізми автентифікації в стандарті 802.11 розраховані на реєстрацію саме фізичного апаратного пристрою, а не облікові записи користувача. Так, що втрата одного мережного інтерфейсу й несвоєчасне повідомлення адміністратора може призвести до того, що зловмисник одержить доступ до мережі без особливих турбот.

6. ОСНОВИ КРИПТОГРАФІЇ

6.1. Терміни і їх визначення

Автентифікація: визначення джерела інформації, тобто кінцевого користувача або пристрої (центрального комп'ютера, сервера, комутатора, маршрутизатора і т.д.).

Цілісність даних: забезпечення незмінності даних у ході їх передачі.

Конфіденційність даних: забезпечення перегляду даних у прийнятному форматі тільки для осіб, що мають право на доступ до цих даних.

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

Розшифрування: метод відновлення зміненої інформації й приведення її у вигляд, що читається.

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

Загальний ключ: цифровий код, використовуваний для шифрування/розшифрування інформації й перевірки цифрових підписів; цей ключ може бути широко розповсюджений; загальний ключ використовується з відповідним приватним ключем.

Приватний ключ: цифровий код, використовуваний для шифрування/розшифрування інформації й перевірки цифрових підписів; власник цього ключа повинен тримати його в секреті; приватний ключ використовується з відповідним загальним ключем.

Секретний ключ: цифровий код, спільно використовуваний двома сторонами для шифрування й розшифрування даних.

Хэш-Функція: математичний розрахунок, результатом якого є послідовність бітів (цифровий код). Маючи цей результат, неможливо відновити вихідні дані, що використовувалися для розрахунків.

Хеш: послідовність бітів, отримана в результаті розрахунків хеш-функції.

Результат обробки повідомлення (Message digest): величина, видавана хеш-функцією (те ж, що й «хеш»).

Шифр: будь-який метод шифрування даних.

Цифровий підпис: послідовність бітів, прикладена до повідомлення (зашифрований хеш), яка забезпечує автентифікацію й цілісність даних.

AAA (Authentication, Authorization, Accounting): архітектура автентифікації, авторизації й обліку.

VPN (Virtual Private Networks): віртуальні частки мережі.

IDS (Intrusion Detection System): системи виявлення вторгнень.

Криптографією називається наука про складання й розшифруванню закодованих повідомлень. Криптографія є важливим елементом для механізмів *автентифікації, цілісності й конфіденційності*.

Автентифікація служить засобом підтвердження особистості відправника або одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність забезпечує ситуацію, при якій дані не може зрозуміти ніхто, крім їхнього відправника й одержувача. Звичайно криптографічні механізми існують у вигляді алгоритму (математичної функції) і секретної величини (ключа).

Автентифікація, цілісність даних і конфіденційність даних підтримуються трьома типами криптографічних функцій: симетричним шифруванням, асиметричним шифруванням і хэш-функциями.

6.2. Симетричне шифрування

Симетричне шифрування, яке часто називають шифруванням за допомогою секретних ключів, в основному використовується для забезпечення конфіденційності даних. Для того, щоб забезпечити конфіденційність даних, абоненти повинні спільно вибрати єдиний математичний алгоритм, який буде використовуватися для шифрування й розшифрування даних. Крім того, їм потрібно вибрати загальний ключ (секретний ключ),

який буде використовуватися із прийнятим ними алгоритмом шифрування/розшифрування.

Приклад симетричного шифрування показаний на рис. 6.1.

Рисунок 6.1 – Симетричне шифрування

Сьогодні широко використовуються такі алгоритми секретних ключів, як *Data Encryption Standard* (DES), *3DES* (або «*потрійний DES»*) і International Data *Encryption Algorithm* (*IDEA*). Ці алгоритми шифрують повідомлення блоками по 64 біта. Якщо обсяг повідомлення перевищує 64 біта (як це звичайно й буває), необхідно розбити його на блоки по 64 біта в кожному, а потім якимось образом звести їх воєдино. Таке об'єднання, як правило, здійснюється одним із чотирьох методів:

- електронної кодової книги (Electronic Code Book – *ECB*);
- ланцюжка зашифрованих блоків (*Cipher* Block Changing – *CBC*);
- x-бітовому зашифрованому зворотньому зв'язку (*Cipher Feedback – Cfb-x*);
- вихідному зворотньому зв'язку (Output *Feedback – OFB*).

Шифрування за допомогою секретного ключа найчастіше використовується для підтримки конфіденційності даних і дуже ефективно реалізується за допомогою незмінних «вшитих» програм (*firmware*). Цей метод можна використовувати для автентифікації й підтримки цілісності даних, але метод цифрового підпису є більш ефективним. З методом секретних ключів пов'язані наступні проблеми:

– необхідно часто міняти секретні ключі, оскільки завжди існує ризик їх випадкового розкриття;

– важко забезпечити *безпечну генерацію* й поширення секретних ключів.

6.3. Асиметричне шифрування

Асиметричне шифрування часте називають шифруванням за допомогою загального ключа, при якому використовуються різні, але, що взаємно доповнюють один одного ключі й алгоритми шифрування й розшифрування. Для того щоб встановити зв'язок з використанням шифрування через загальний ключ, обом сторонам потрібно одержати два ключі: загальний і приватний (рис. 6.2). Для шифрування й розшифрування даних сторони будуть користуватися різними ключами.

Рисунок 6.2 – Асиметричне шифрування

Ось деякі найбільш типові цілі використання алгоритмів загальних ключів:

– забезпечення конфіденційності даних;
– автентифікація відправника;
– безпечне одержання загальних ключів для спільного використання.

Механізми генерування пара загальних/приватних ключів є досить складними, але в результаті виходять пари більших випадкових чисел, одне з яких стає загальним ключем, а інше – часткам. Генерація таких чисел вимагає більших процесорних потужностей, оскільки ці числа, а також їх добутки, повинні відповідати суворим математичним критеріям. Однак цей процес абсолютно необхідний для забезпечення унікальності кожної пари загальних/приватних ключів. Алгоритми шифрування за допомогою загальних ключів рідко використовуються для підтримки конфіденційності даних через обмеження продуктивності. Замість цього їх часто використовують у додатках, де автентифікація проводиться за допомогою цифрового підпису й керування ключами.

З найбільш відомих алгоритмів загальних ключів можна назвати RSA (Rivest-Shamir-Adleman, Ривест-Шамир-Адельман) і Elgamal (Ель-Гамал).

6.4. Безпечна хэш-функція

Безпечної хэш-функцією називається та функція, яку легко розрахувати, але зворотне відновлення практично неможливе, тому, що вимагає непропорційно більших зусиль. Вхідне повідомлення пропускається через математичну функцію (хэш-функцію), і в результаті на виході ми одержуємо якусь послідовність бітів (рис. 6.3). Ця послідовність називається «хеш» (або «результат обробки повідомлення»). Хеш-Функція ухвалює повідомлення будь-якої довжини й видає на виході хеш фіксованої довжини.

Рисунок 6.3 – Обчислення хеш-функції

Звичайні хеш-функції включають:

- алгоритм *Message Digest* 4 (*MD4*);
- алгоритм *Message Digest* 5 (*MD5*);
- алгоритм безпечного хеша (Secure *Hash Algorithm – SHA*).

6.5. Цифровий підпис

Цифровий підпис являє собою зашифрований хеш, який додається до документа. Принцип шифрування із цифровим підписом пояснює рис. 6.4.

Рисунок 6.4 – Перевірка дійсності повідомлення із цифровим підписом

Вона може використовуватися для автентифікації відправника й цілісності документа. Цифрові підписи можна створювати за допомогою комбінації хеш-функцій і криптографії загальних ключів.

6.6. Цифровий сертифікат

Цифровим сертифікатом називається повідомлення із цифровим підписом, яке в цей час використовується для підтвердження дійсності загального ключа. Загальний формат широко розповсюдженого сертифіката X.509 включає наступні елементи:

- версії;
- серійний номер сертифіката;
- емітент інформації про алгоритм;
- емітент сертифіката;
- дати початку й закінчення дії сертифіката;
- інформацію про алгоритм загального ключа *суб'єкта сертифіката*;
- підпис організації, що емітує.

Організація, що емітує, видає сертифікат, *або центр* сертифікації *(Certification* Authority – CA), є надійною третьою стороною, якій ви повністю довіряєте. Передача загального ключа відбувається в такий спосіб (рис. 6.5):

– відправник створює сертифікат, у який включає загальний ключ;

– одержувач запитує в *центрі сертифікації* сертифікат відправника;

– *центр сертифікації* підписує сертифікат відправника;

– *центр сертифікації* посилає підписаний сертифікат одержувачеві;

– одержувач перевіряє підпис *центру сертифікації* й витягає загальний ключ відправника.

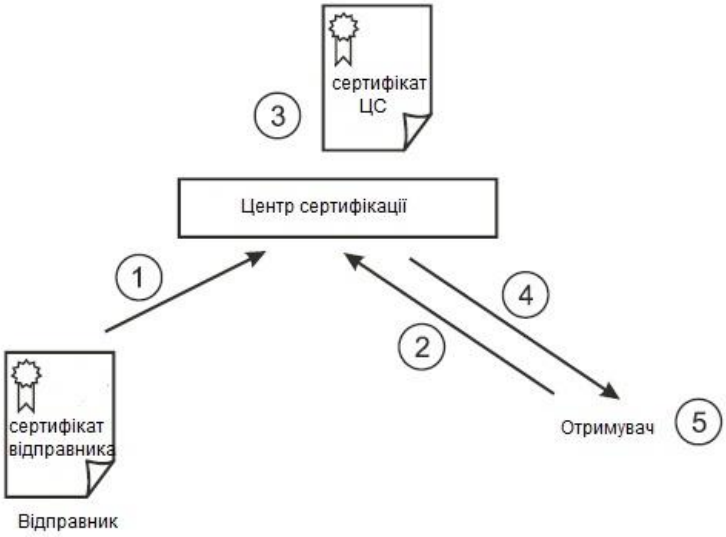


Рисунок 6.5 – Передача ключа із цифровим сертифікатом

Для реалізації цієї схеми необхідна надійна система поширення загального ключа СА серед користувачів. Для цього створена *інфраструктура відкритих ключів PKI* (Public Key Infrastructure). Використання PKI дозволяє спростити керування безпекою шляхом автоматизації, підсилити режим безпеки завдяки значній складності компрометації цифрових сертифікатів, удосконалити й інтегрувати керування захистом, підсилити контроль захищеного доступу до бізнес-ресурсам.

PKI представляє ієрархічну архітектуру керування атрибутами безпеки користувачів, що брали участь у захищеному обміні інформацією. Крім людей в PKI також можуть брати участь елементи інфраструктури мережі – міжмережеві екрани, концентратори віртуальних приватних мереж, маршрутизатори, захищені сервери додатків та інші програмно-апаратні комплекси, що бідують у перевірці дійсності й шифруванні.

Кожний суб'єкт PKI має цифровий сертифікат, що озивається й підписаний органом сертифікації. Сертифікат представляє впорядковану структуру даних, що зв'язує загальний ключ із його власником, і містить набір елементів, використовуваних суб'єктами при встановленні захищених з'єднань.

7. ПРОТОКОЛ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

Існує безліч технологій безпеки, і всі вони пропонують вирішення для найважливіших компонентів політики в області захисту даних: автентифікації, підтримки цілісності даних і активної перевірки. Ми визначаємо автентификацию як автентификацию користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, міжмережевого екрана і т.д.) і його місця розташування з наступною авторизацією користувачів і кінцевих пристроїв.

Цілісність даних включає такі області, як безпека мережевої інфраструктури, безпека периметра й конфіденційність даних. Активна перевірка допомагає впевнитися в тому, що встановлена політика в області безпеки дотримується, і відстежити всі аномальні випадки й спроби несанкціонованого доступу.

7.1. Механізм шифрування WEP

Шифрування *WEP* (*Wired Equivalent Privacy* – таємність на рівні провідного зв'язку) засноване на алгоритмі *RC4* (Rivest's *Cipher* v.4 – код Ривеста), яке демонструє симетричне *потокове шифрування*. Як було відзначено раніше, для нормального обміну користувацькими даними ключі шифрування в абонента й точці радіодоступу повинні бути ідентичними.

Ядро алгоритму складається з функції генерації ключового потоку. Ця функція генерує послідовність бітів, яка потім поєднується з відкритим текстом за допомогою підсумовування по модулю два. Дешифрування складається з регенерації цього ключового потоку й підсумовування його із шифрограмой по модулю два для відновлення вихідного тексту. Інша головна частина алгоритму – функція ініціалізації, яка використовує ключ змінної довжини для створення початкового стану генератора ключового потоку.

RC4 – фактично клас алгоритмів, обумовлених розміром його блоку. Цей параметр n є розміром слова для алгоритму. Звичайно, $n = 8$, але з метою аналізу можна зменшити його. Однак для підвищення рівня безпеки необхідно задати більше значення

цієї величини. Внутрішній стан *RC4* складається з масиву розміром 2^n слів і двох лічильників, кожний розміром в одне слово. Масив відомий як *S-Бокс*, і далі він буде позначатися як *S*. Він завжди містить перестановку 2^n можливих значень слова. Два лічильники позначені через *i* та *j*.

Алгоритм ініціалізації *RC4* наведений нижче.

Цей алгоритм використовує ключ, збережений в *Key*, що й має довжину l байт. Ініціалізація починається із заповнення масиву *S*, далі цей масив перемішується шляхом перестановок, обумовлених ключем. Тому, що над *S* виконується тільки одна дія, повинна виконуватися твердження, що *S* завжди містить усі значення кодового слова.

1. Початкове заповнення масиву:
2. for i = 0 to $2^n - 1$
3. {
4. S[i] = i
   }
5. Зкремблювання:
6. j = 0;
7. for i = 0 to $2^n - 1$
8. {
9. j = (j + S[i] + Key[i mod l]) mod 2^n
10. Перестановка (S[i], S[j])
}

Генератор ключового потоку *RC4* переставляє значення, що зберігаються в *S*, і щораз вибирає нове значення з *S* у якості результату. В одному циклі *RC4* визначається одне n-бітне слово *K* із ключового потоку, яке надалі складається з вихідним текстом для одержання зашифрованого тексту.

11. Ініціалізація:
12. i = 0

j = 0

13. Цикл генерації:
14. i = (i + 1) mod 2^n
15. j = (j + S[i]) mod 2^n
16. Перестановка (S[i], S[j])

Результат: K = S[(S[i] + S[j]) mod 2^n]

Особливості Wep-*Протоколу*:

- досить стійкий до атак, пов'язаних із простим перебором ключів шифрування, що забезпечується необхідною довжиною ключа й частотою зміни ключів та ініціазіруючого вектора;
- самосинхронізація для кожного повідомлення. Ця властивість є ключовою для протоколів рівня доступу до середовища передачі, де велике число перекручених і загублених пакетів;
- ефективність: *WEP* легко реалізувати;
- відкритість;
- використання Wep-*Шифрування* не є обов'язковим у мережах стандарту *IEEE 802.11*.

Для безперервного шифрування потоку даних використовується потокове й блокове шифрування.

7.1.1. Потокове шифрування

При *потоковому шифруванні* виконується побітове додавання по модулю 2 (функція, що виключає «АБО», XOR) ключової послідовності, які генеруються алгоритмом шифрування на основі заздалегідь заданого ключа, і вихідного повідомлення. Ключова послідовність має довжину, відповідну до довжини вихідного повідомлення, що підлягає шифруванню (рис. 7.1).

Рисунок 7.1 – Потокове шифрування

7.1.2. Блокове шифрування

Блокове шифрування працює із блоками заздалегідь певної довжини, що не міняються в процесі шифрування. Вихідне повідомлення фрагментується на блоки, і функція XOR

обчислюється над ключовою послідовністю й кожним блоком. Розмір блоку фіксований, а останній фрагмент вихідного повідомлення доповнюється порожніми символами до довжини нормального блоку (рис. 7.2). Наприклад, при *блоковому шифруванні* з 16-байтовими блоками вихідне повідомлення довжиною в 38 байтів фрагментується на два блоки довжиною по 16 байтів і 1 блок довжиною 6 байтів, який потім доповнюється 10 байтами порожніх символів до довжини нормального блоку.

Потокове й блокове шифрування використовують метод електронної кодової книги (ECB). Метод ECB характеризується тим, що те саме вихідне повідомлення на вході завжди породжує те саме зашифроване повідомлення на виході. Це потенційний пролом у системі безпеки, тому що сторонній спостерігач, виявивши повторювані послідовності в зашифрованому повідомленні, у стані зробити обґрунтовані припущення щодо ідентичності змісту вихідного повідомлення.

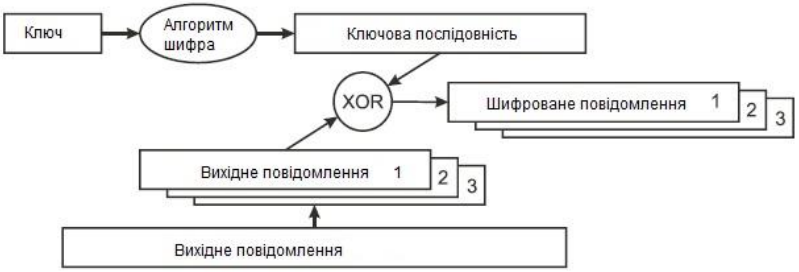


Рисунок 7.2 – Блокове шифрування

Для усунення зазначеної проблеми використовують:

Вектори ініціалізації (Initialization Vectors – Ivs).

Зворотний зв’язок (feedback modes).

До початку процесу шифрування 40- або 104-бітний секретний ключ розподіляється між усіма станціями, що входять у бездротову мережу. До секретного ключа додається вектор ініціалізації (Initialization Vector – IV).

Вектор ініціалізації використовується для модифікації ключової послідовності. При використанні вектора ініціалізації ключова послідовність генерується алгоритмом шифрування, на

вхід якого подається секретний ключ, сполучений з IV. При зміні вектора ініціалізації ключова послідовність також міняється. На рис. 7.3 вихідне повідомлення шифрується з використанням нової ключової послідовності, згенерований алгоритмом шифрування після подачі на його вхід комбінації із секретного ключа й вектора ініціалізації, що породжує на виході шифроване повідомлення.

Стандарт IEEE 802.11 рекомендує використовувати нове значення вектора ініціалізації для кожного нового фрейму, переданого в радіоканал.

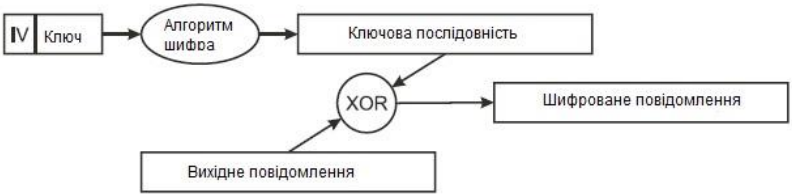


Рисунок 7.3 – Алгоритм шифрування WEP

Таким чином, той самий нешифрований фрейм, переданий багаторазово, щораз буде породжувати унікальний шифрований фрейм.

Вектор ініціалізації має довжину 24 біта й сполучається з 40- або 104-бітовим базовим ключем шифрування WEP таким чином, що на вхід алгоритму шифрування подається 64- або 128-бітовий ключ. Вектор ініціалізації присутній в нешифрованому вигляді в заголовку фрейму в радіоканалі, для того щоб сторона, що ухвалює, могла успішно декодувати цей фрейм. Незважаючи на те, що звичайно говорять про використання шифрування WEP із ключами довжиною 64 або 128 бітів, ефективна довжина ключа становить лише 40 або 104 біта через передачу вектора ініціалізації в нешифрованому вигляді. При налаштуванні шифрування в обладнанні при 40-бітному ефективному ключі вводяться 5 байтових Ascii-Символів $(5 \cdot 8 = 40)$ або 10 шістнадцятирічних чисел $(10 \cdot 4 = 40)$, і при 104-бітному ефективному ключі вводяться 13 байтових Ascii-Символів

$(13 \cdot 8 = 104)$ або 26 шістнадцятирічних чисел $(26 \cdot 4 = 104)$. Деяке встаткування може працювати з 128-бітним ключем.

Зворотний зв'язок модифікує процес шифрування й запобігає породженню тим самим вихідним повідомленням того самого шифрованого повідомлення. Зворотний зв'язок звичайно використовується при *блоковому шифруванні*. Найчастіше зустрічається тип зворотного зв'язку, відомий як ланцюжок шифрованих блоків (*CBC*).

В основі використання ланцюга шифрованих блоків лежить ідея обчислення двійкової функції XOR між блоком вихідного повідомлення й попереднім йому блоком шифрованого повідомлення. Оскільки найперший блок не має попередника, для модифікації ключової послідовності використовують вектор ініціалізації. Роботу ланцюжка шифрованих блоків ілюструє рис.7.4.

7.2. Уразливість шифрування WEP

Атаки на зашифровані дані за допомогою технології WEP можна підрозділити на два методи: пасивні й активні.

7.2.1. Пасивні мережні атаки

У серпні 2001 року криптоаналітики Флурер З, Мантин І. і Шамир А. (Fluhrer S., Mantin I., Shamir A.) установили, що секретний ключ шифрування WEP може бути обчислений з використанням певних фреймів, пасивно зібраних у бездротовій локальній мережі. Причиною уразливості послужила реалізація в WEP методу планування ключів (Key Scheduling Algorithm – KSA) алгоритму потокового шифрування RC4. Деякі вектори ініціалізації (так звані «слабкі» вектори) дають можливість установити побайтовий склад секретного ключа, застосовуючи статистичний аналіз.

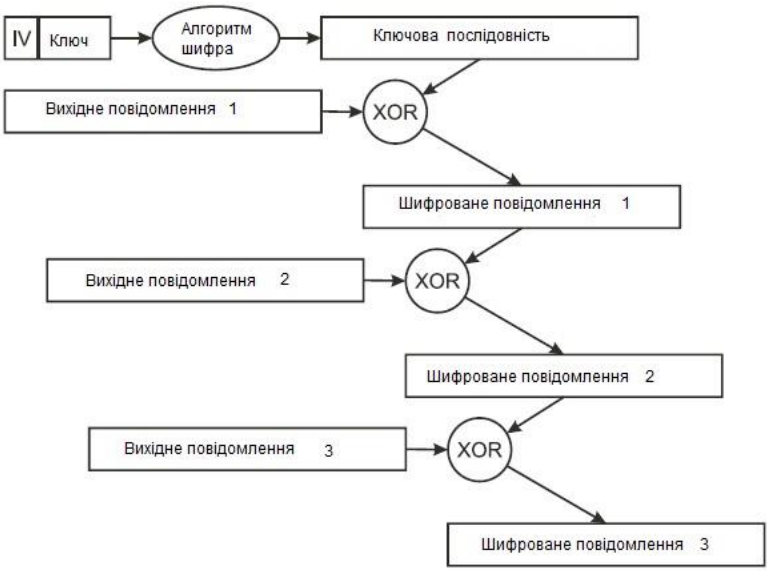


Рисунок 7.4 – Шифрування зі зворотним зв’язком

Дослідниками з AT&T/Rice University і авторами програми Airsnort була продемонстрована можливість визначення секретного ключа довжиною 40 і 104 бітів після аналізу всього лише 4 мільйонів фреймів. Для завантаженої бездротової локальної мережі це еквівалентно приблизно чотирьох годинній роботі, після чого ключ шифрування стане відомий пасивному спостерігачеві.

Подібна уразливість робить шифрування з використанням WEP неефективним. Використання динамічних секретних ключів шифруванняWEP вирішує проблему лише частково, для повного усунення уразливості потрібне посилення самого ключа.

7.2.2. Активні мережні атаки

Індуктивне обчислення секретного ключа шифрування WEP являє собою процес впливу на бездротову локальну мережу для одержання певної інформації й ставиться до класу активних мережних атак. Як було сказано раніше, при потоковому

шифруванні виконується двійкове додавання по модулю 2 (XOR) вихідного повідомлення із ключовою послідовністю з метою одержання шифрованого повідомлення. Цей факт ліг в основу даної атаки.

Висока ефективність атаки індуктивного обчислення ключа, що використовується в бездротовій локальній мережі IEEE 802.11, пояснюється відсутністю діючих засобів контролю цілісності повідомлень (Message Integrity Check, *MIC*). Сторона, що ухвалює, не в змозі розпізнати факт модифікації вмісту фрейму в процесі передачі по загальнодоступному радіоканалу. Більше того, значення ICV (Integrity Check Value), передбачене стандартом для контролю цілісності повідомлень, обчислюється за допомогою функції CRC32 (32-bit Cyclical Redundancy Check, контроль за допомогою циклічного 32-бітного надлишкового коду), яка піддана атакам з маніпуляцією бітами. Таким чином, у відсутності механізмів контролю цілісності повідомлень бездротові локальні мережі піддаються активним атакам: повторному використанню вектора ініціалізації (IV Replay) і маніпуляції бітами (Bit-Flipping).

1) Повторне використання вектора ініціалізації (Initialization Vector Replay Attacks), представляє собою розроблену теоретично й реалізовану практично активну мережну атаку в бездротовій локальній мережі, що існує в декількох різновидах, одна з яких описана нижче й проілюстрована рис. 7.5.

– Хакер багаторазово відправляє абонентові бездротової локальної мережі по провідній мережі повідомлення відомого змісту (наприклад, Ір-Пакет, лист по електронній пошті й т.п.).

– Хакер пасивно прослуховує радіоканал зв'язку абонента із точкою радіодоступу й збирає фрейми, що приблизно містять шифроване повідомлення.

– Хакер обчислює ключову послідовність, застосовуючи функцію XOR до передбачуваного шифрованого й відомого нешифрованого повідомлень.

– Хакер «вирощує» ключову послідовність для пари вектора ініціалізації й секретного ключа, що породила ключову послідовність, обчислену на попередньому кроці.

Атакуючий знає, що пари вектора ініціалізації й секретного ключа шифрування, а значить і породжувана ними ключова послідовність, може бути повторно використана для відтворення ключової послідовності достатньої довжини для порушення конфіденційності в бездротовій локальній мережі в умовах використання шифрування WEP.

Рисунок 7.5 – Повторне використання вектора ініціалізації

Після того, як ключова послідовність обчислена для фреймів деякої довжини, її можна «виростити» до будь-якого розміру, як описано нижче й показане на рис. 7.6.

– Хакер створює фрейм на один байт довше, чим довжина вже відомої ключової послідовності. Пакети ICMP (Internet Control *Message Protocol* – протокол керуючих повідомлень Internet), що посилають командою ping, ідеальні для цих цілей тому, що точка радіодоступу змушена на них відповідати.

– Хакер збільшує довжину ключової послідовності на один байт.

Рисунок 7.6 – «Вирощування» ключової послідовності

– Значення додаткового байта вибирається випадковим образом з 256 можливих Ascii-Символів.

– Якщо передбачуване значення додаткового байта ключової послідовності вірно, то буде отримана очікувана відповідь від точки радіодоступу, у даному прикладі це ICMP

– Процес повторюється доти, поки не буде підібрана ключова послідовність потрібної довжини.

2) Маніпуляція бітами (Bit-Flipping Attacks)

Маніпуляція бітами переслідує ту ж мета, що й повторне використання вектора ініціалізації, і опирається на уразливість вектора контролю цілісності фрейму ICV. Користувацькі дані можуть різнитися від фрейму до фрейму, у той же час багато службових полів і їх положення усередині фрейму залишаються незмінними.

Хакер маніпулює бітами користувацьких даних усередині фрейму 2-го (канального) рівня моделі OSI (Open Systemsinterconnection) з метою викривлення 3-го (мережного) рівня пакета. Процес маніпуляції показаний на рис. 7.7.

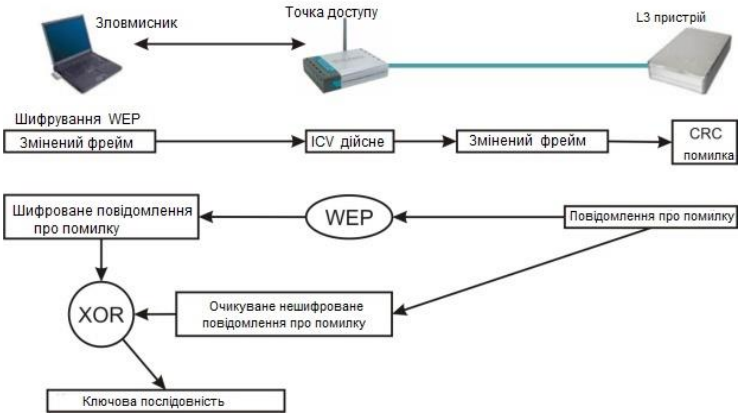


Рисунок 7.7 – Атака з маніпуляцією бітами

– Хакер пасивно спостерігає фрейми бездротової локальної мережі за допомогою засобів *аналізу трафіка* протоколу 802.11.

– Хакер захоплює фрейм і довільно змінює біти в поле даних протоколу 3-го рівня.

– Хакер модифікує значення вектора контролю цілісності фрейму ICV (як саме, буде описано нижче).

– Хакер передає модифікований фрейм у бездротову локальну мережу.

– Сторона, що ухвалює (абонент або точка радіодоступу) обчислює значення вектора контролю цілісності фрейму ICV для отриманого модифікованого фрейму.

– Сторона, що ухвалює, порівнює обчислене значення вектора ICV з наявним в отриманому модифікованому фреймі.

– Значення векторів збігаються, фрейм вважається неспотвореним і не відкидається.

– Сторона, що ухвалює, деінкапсулює вміст фрейму й обробляє пакет мережного рівня.

– Оскільки маніпуляція бітами відбувалася на канальному рівні, контрольна сума пакета мережного рівня виявляється невірною.

– Стік протоколу мережного рівня на стороні, що ухвалює, генерує передбачуване повідомлення про помилку.

– Хакер спостерігає за бездротовою локальною мережею чекаючи зашифрованого фрейму з повідомленням про помилку.

– Хакер захоплює фрейм, що містить зашифроване повідомлення про помилку, і обчислює ключову послідовність, як було описано раніше для атаки з повторним використанням вектора ініціалізації.

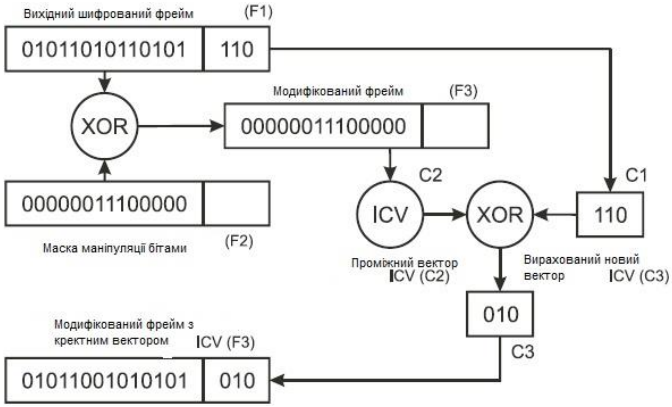


Рисунок 7.8 – Обчислення поля контролю цілісності повідомлень

Вектор ICV перебуває в шифрованій частині фрейму. За допомогою наступної процедури хакер маніпулює бітами шифрованого вектора ICV і в такий спосіб забезпечує коректність самого вектора для нового, модифікованого фрейму (рис. 7.8):

– Вихідний фрейм F1 має вектор C1.

– Створюється фрейм F2 такої ж довжини, що й F1, службовець маскою для модифікації бітів фрейму F1.

– Створюється фрейм F3 шляхом виконання двійкової функції XOR над фреймами F1 і F2.

– Обчислюється проміжний вектор C2 для фрейму F3.

– Вектор C3 для фрейму F3 обчислюється шляхом виконання двійкової функції XOR над C1 і C2.

7.2.3. Проблеми керування статичними Wep-Ключами

Стандартом IEEE 802.11 не передбачені які-небудь механізми керування ключами шифрування. По визначенню, алгоритм WEP підтримує лише статичні ключі, які заздалегідь поширюються тим або іншим способом між абонентами й точками радіодоступу бездротової локальної мережі. Оскільки *IEEE 802.11* автентифікує фізичний пристрій, а не його користувача, втрата абонентського адаптера, точка радіодоступу або властиво секретного ключа становлять небезпеку для системи безпеки бездротової локальної мережі. У результаті при кожному подібному інциденті адміністратор мережі буде змушений вручну зробити зміну ключів у всіх абонентів і в точках доступу. Для цього у всьому встаткуванні D-Link відведено чотири поля для введення ключів. І при зміні всіх ключів необхідно тільки поміняти номер використовуваного ключа.

Ці адміністративні дії підходять для невеликої бездротової локальної мережі, але зовсім неприйнятні для мереж, у яких абоненти обчислюються сотнями й тисячами й/або розподілені територіально. В умовах відсутності механізмів генерації й *поширення ключів* адміністратор змушений ретельно опікувати абонентські адаптери й устаткування інфраструктури мережі.

8. АВТЕНТИФІКАЦІЯ В БЕЗДРОТОВИХ МЕРЕЖАХ

Основними стандартами автентифікації в бездротових мережах є стандарти IEEE *802.11, WPA, WPA2* і 802.1x. Розглянемо основи цих стандартів.

8.1. Стандарт IEEE 802.11 мережі із традиційною безпекою

Стандарт IEEE 802.11 із традиційною безпекою (Tradition Security Network – TSN) передбачає два механізми автентифікації бездротових абонентів: відкриту автентифікацію (Open Authentication) і автентифікацію із загальним ключем (Shared Key Authentication). В автентифікації в бездротових мережах також широко використовуються два інших механізми, що виходять за рамки стандарту 802.11, а саме призначення ідентифікатора бездротової локальної мережі (Service Set Identifier – SSID) і автентифікація абонента по його *Mac-Адресі* (*MAC Address Authentication*).

Ідентифікатор бездротової локальної мережі (SSID) являє собою атрибут бездротової мережі, що дозволяє логічно відрізняти мережі одну від одної. У загальному випадку абонент бездротової мережі повинен задати в себе відповідний SSID для того, щоб одержати доступ до необхідної бездротової локальної мережі. SSID ні в якій мірі не забезпечує конфіденційність даних, так само як і не автентифікує абонента стосовно точки радіодоступу бездротової локальної мережі. Існують точки доступу, що дозволяють розділити абонентів, що підключаються до точки на кілька сегментів, – це досягається тим, що точка доступу може мати не один, а кілька SSID.

8.1.1. Принцип автентифікації абонента в IEEE 802.11

Автентифікація в стандарті *IEEE 802.11* орієнтована на автентифікацію абонентського пристрою радіодоступу, а не конкретного абонента як користувача мережних ресурсів. Процес

автентифікації абонента бездротової локальної мережі *IEEE 802.11* складається з наступних етапів (рис. 8.1):

– Абонент (Client) посилає фрейм *Probe* Request в усі радіоканали.

– Кожна точка радіодоступу (*Access Point* – AP), у зоні радіовидимості якої перебуває абонент, посилає у відповідь фрейм *Proberesponse*.

– Абонент вибирає кращу для нього точку радіодоступу й посилає в радіоканал, що обслуговується нею, запит на Authentication (Authentication Request).

– Точка радіодоступу посилає підтвердження автентифікації (Authentication *Reply*).

– У випадку успішної автентифікації абонент посилає точці радіодоступу фрейм асоціації (Association Request).

– Точка радіодоступу посилає у відповідь фрейм підтвердження асоціації (Association Response).

– Абонент може тепер здійснювати обмін користувацьким трафіком із точкою радіодоступу й провідною мережею.

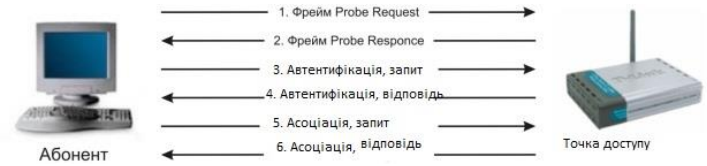


Рисунок 8.1 – Автентифікація по стандарту 802.11

При активізації бездротовий абонент починає пошук точок радіодоступу у своїй зоні радіовидимості за допомогою керуючих фреймів *Probe* Request. Фрейми *Probe* Request посилають у кожний з радіоканалів, підтримуваних абонентським радіоінтерфейсом, щоб знайти всі точки радіодоступу з необхідними клієнтові ідентифікатором *SSID* і підтримуваними швидкостями радіообміну. Кожна точка радіодоступу, що перебувають у зоні радіовидимості абонента, що задовольняє запитуваним у фреймі *Probe* Request параметрам, відповідає фреймом *Probe* Response, що містять синхронізуючу

інформацію й дані про поточне завантаження точки радіодоступу. Абонент визначає, з якою точкою радіодоступу він буде працювати, шляхом зіставлення підтримуваних ними швидкостей радіообміну й завантаження. Після того як краща точка радіодоступу визначена, абонент переходить у фазу автентифікації.

Відкрита автентифікація:

Відкрита автентифікація по суті не є алгоритмом автентифікації у звичному розумінні. Точка радіодоступу задовольнить будь-який запит відкритої автентифікації. На перший погляд використання цього алгоритму може здатися безглуздим, однак слід ураховувати, що розроблені в 1997 році методи автентифікації *IEEE 802.11* орієнтовані на швидке логічне підключення до бездротової локальної мережі. Додатково до цього багато *IEEE 802.11-сумісні* пристрої являють собою портативні блоки збору інформації (сканери штрих-кодів і т.п.), що не мають достатньої процесорної потужності, необхідної для реалізації складних алгоритмів автентифікації.

У процесі відкритої автентифікації відбувається обмін повідомленнями двох типів:

– запит автентифікації (Authentication Request);

– підтвердження автентифікації (Authentication Response).

Таким чином, при відкритій автентифікації можливий доступ будь-якого абонента до бездротової локальної мережі. Якщо в бездротовій мережі шифрування не використовується, будь-який абонент, що знає ідентифікатор *SSID* точки радіодоступу, одержить доступ до мережі. При використанні точками радіодоступу шифрування *WEP* самі ключі шифрування стають засобом контролю доступу. Якщо абонент не розташовує коректним Wep-*Ключем*, то навіть у випадку успішної автентифікації він не зможе не передавати дані через точку радіодоступу, не розшифровувати дані, передані точкою радіодоступу (рис. 8.2).

Рисунок 8.2 – Відкрита автентифікація

8.1.2. Автентифікація із загальним ключем

Автентифікація із загальним ключем є другим методом автентифікації стандарту *IEEE 802.11*. Автентифікація із загальним ключем вимагає настроювання в абонента статичного ключа шифрування *WEP*. Процес автентифікації ілюструє рис. 8.3.

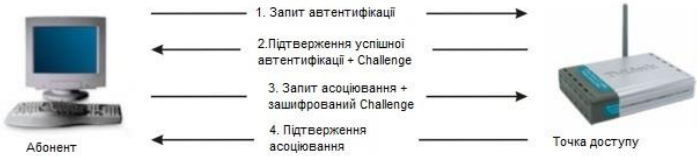


Рисунок 8.3 – Автентифікація із загальним ключем

1. Абонент посилає точці радіодоступу запит автентифікації, указуючи при цьому необхідність використання режиму автентифікації із загальним ключем.
2. Точка радіодоступу посилає підтвердження автентифікації, що містить *Challenge* Text.
3. Абонент шифрує *Challenge* Text своїм статичним Wep-*Ключем* і посилає точці радіодоступу запит автентифікації.
4. Якщо точка радіодоступу в змозі успішно розшифрувати запит автентифікації, що й утримується в ньому *Challenge* Text, вона посилає абонентові підтвердження автентифікації, у такий спосіб надаючи доступ до мережі.

8.1.3. Автентифікація по Mac-Адресі

Автентифікація абонента по його Mac-Адресі не передбачена стандартом *IEEE 802.11*, однак підтримується багатьма виробниками встаткування для бездротових мереж, у тому числі D-Link. При автентифікації по Mac-Адресі відбувається порівняння Mac-Адреси абонента або зі списком, що зберігається локально, дозволених адрес легітимних абонентів, або за допомогою зовнішнього сервера (рис. 8.4). Автентифікація по Mac-адресі використовується на додаток до відкритої автентифікації й автентифікації із загальним ключем стандарту IEEE 802.11 для зменшення ймовірності доступу сторонніх абонентів.

Рисунок 8.4 – Автентифікація за допомогою зовнішнього сервера

8.1.4. Налаштування точки доступу на WEP-Шифрування

1. Підключаємося до точки доступу, вводимо режим, *SSID*, канал, як було описано в прикладі 1.4. Далі в поле Authentication (Автентифікація) ставимо Shared Key (із загальним ключем) (рис. 8.5).

2. Тому, що автентифікація із загальним ключем припускає ще й шифрування даних по *WEP*, то в поле Encryption (Шифрування) активне буде тільки Enable.

3. Вибираємо тип ключа (Key Type) і розмір ключа (Key Size).

4. Уводимо кілька ключів, послідовно вибираючи в поле Valid Key (Діючий ключ). При 64-бітному ключі з типом ключа ASCII потрібно ввести п’ятизначну послідовність, наприклад *passl*.

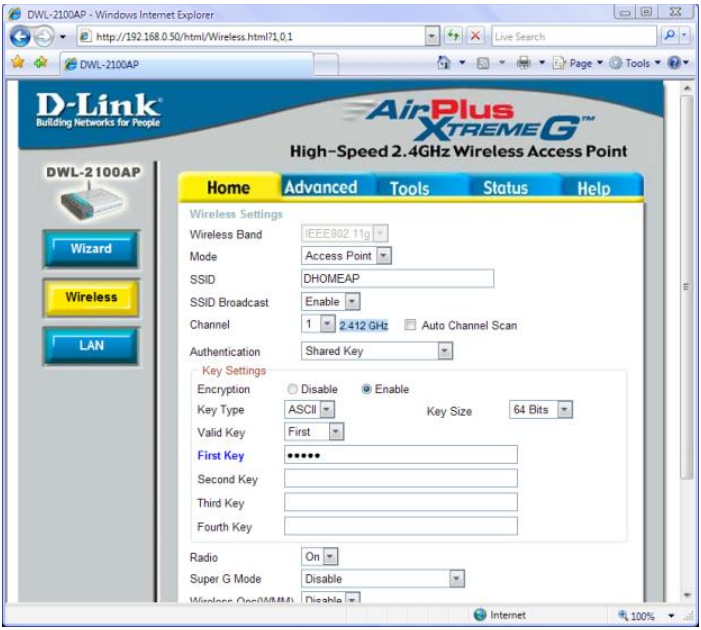


Рисунок 8.5 – Вкладка налаштування WEP-Шифрування

Тепер, після застосування настроювань, на клієнтській стороні треба виставити ті ж самі параметри й підключитися до неї.

8.1.5. Специфікація WPA

До травня 2001 р. стандартизація засобів інформаційної безпеки для бездротових мереж *802.11* ставилася до ведення робочої групи IEEE 802.11e, але потім ця проблематика була виділена в самостійний підрозділ. Розроблений стандарт 802.11i покликано розширити можливості протоколу *802.11*, передбачивши засобу шифрування переданих даних, а також централізованої автентифікації користувачів і робочих станцій.

Основні виробники Wi-Fi устаткування в особі організації *WECA* (*Wireless Ethernet* Compatibility Alliance), інакше іменованої Wi-Fi Alliance, утомившись чекати ратифікації

стандарту *IEEE 802.11i*, разом з IEEE у листопаді 2002 р. анонсували специфікацію Wi-Fi Protected Access (*WPA*), відповідність якої забезпечує сумісність устаткування різних виробників.

Новий стандарт безпеки *WPA* забезпечує рівень безпеки куди більший, ніж може запропонувати *WEP* Він перекидає місток між стандартами *WEP* і 802.11i і має немаловажливу перевагу, яка полягає в тому, що мікропрограмне забезпечення більш старого встаткування може бути замінене без внесення апаратних змін.

IEEE запропонувала тимчасовий протокол цілісності ключа (Temporal Key Integrity Protocol, TKIP).

8.1.6. Основні вдосконалення шифрування, внесені протоколом TKIP

Основні вдосконалення шифрування, внесені протоколом TKIP:

- Пофреймова зміна ключів шифрування. Wep-*Ключ* швидко змінюється, і для кожного фрейму він іншої;
- Контроль цілісності повідомлення. Забезпечується ефективний контроль цілісності фреймів даних з метою запобігання схованих маніпуляцій із фреймами й відтворення фреймів;
- Удосконалений механізм керування ключами.

Атаки, застосовувані в WEP, що використовують уразливість слабких **IV** (**Initialization Vectors**), таких, які застосовуються в додатку Airsnort, засновано на нагромадженні декількох фреймів даних, що містять інформацію, зашифровану з використанням слабких *IV*. Найпростішим способом стримування таких атак є зміна Wep-*Ключа*, використовуваного при обміні фреймами між клієнтом і точкою доступу, перше ніж атакуючий встигне нагромадити фрейми в кількості, достатньому для виводу бітів ключа.

IEEE адаптувала схему, відому як пофреймова зміна ключа (per-frame keying). Основний принцип, на якому засновано пофреймову зміна ключа, полягає в тому, що *IV*, Mac-*Адреса* передавача й Wep-*Ключ* обробляються разом за допомогою двоступінчастої функції перемішування. Результат застосування

цієї функції відповідає стандартному 104-розрядному Wep-*Ключу* й 24-розрядному *IV*.

IEEE запропонувала також збільшити 24-розрядний вектор ініціалізації до 48-розрядного *IV*.

На рис. 8.6 представлений зразок 48-розрядного IV і показане, як він розбивається на частині для використання при пофреймовій зміні ключа.

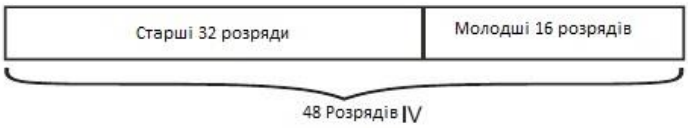


Рисунок 8.6 – Розбивка 48-розрядного IV

Процес пофреймової зміни ключа можна розбити на наступні етапи (рис. 8.7):

– Базовий Wep-*Ключ* перемішується зі старшими 32 розрядами 48-розрядного *IV* (32-розрядні числа можуть ухвалювати значення 0-4 294 967 295) і Mac-*Адресою* передавача. Результат цієї дії називається *ключ 1-й фази*. Цей процес дозволяє занести ключ 1-й фази в кеш і також прямо помістити в ключ.

– Ключ 1-й фази знову перемішується з *IV* і Mac-*Адресою* передавача для виробітку значення пофреймового ключа.

– Вектор ініціалізації (IV), використовуваний для передачі фрейму, має розмір тільки 16 біт (16-розрядні числа можуть ухвалювати значення 0-65 535). 8 біт, що залишилися (у стандартному 24-бітовому IV) являють собою фіксоване значення, використовуване як заповнювач.

– Пофреймовий ключ застосовується для Wep-*Шифрування* фрейму даних.

– Коли 16-бітовий простір IV виявляється вичерпаним, ключ 1-й фази відкидається й 32 старших розряду збільшуються на 1.

– Значення пофреймового ключа обчислюється заново, як на етапі 2.

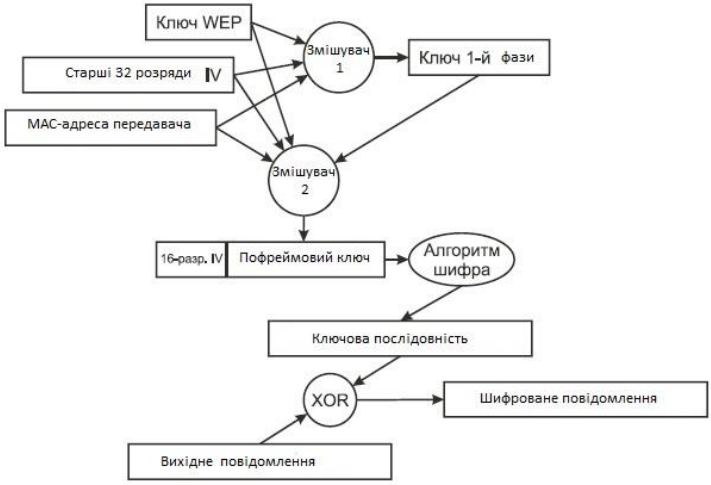


Рисунок 8.7 – Процес створення шифрованого повідомлення в WPA

Процес пофреймової зміни ключа можна розбити на наступні етапи.

– Пристрій ініціює IV, привласнюючи йому значення 0. У двійкому вигляді це буде значення 00000000000000000000000000000000 00000000000000000.

– Перші 32 розряду IV (у розглянутому випадку – перші 32 нуля) перемішуються з Wep-*Ключем* (наприклад, що мають 128-розрядне значення) і Mac-*Адресою* передавача (що мають 48-розрядне значення) для одержання значення ключа 1-й фази (80-розрядне значення).

– Ключ 1-й фази знову перемішується з першими (старшими) 32 розрядами IV і Mac-*Адресою* передавача, щоб одержати 128-розрядний пофреймовий ключ, перші 16 розрядів якого являють собою значення IV (16 нулів).

– Вектор ініціалізації пофреймового ключа збільшується на 1. Після того як пофреймові можливості IV будуть вичерпані, IV 1-й фази (32 біта) збільшується на 1 (він тепер буде складатися з 31 нуля й однієї одиниці, 00000000000000000000000000000001) і т.д.

Цей алгоритм підсилює WEP настільки, що майже всі відомі зараз можливості атак усуваються без заміни існуючого встаткування. Слід зазначити, що цей алгоритм (і TKIP у цілому) розроблено з метою усунути вразливі місця в системі автентифікації WEP і стандарту 802.11. Він жертвує слабкими алгоритмами, замість того щоб заміняти встаткування.

8.1.7. Контроль цілісності повідомлення

Для посилення малоефективного механізму, заснованого на використанні контрольної ознаки цілісності (ICV) стандарту 802.11, буде застосовуватися контроль цілісності повідомлення (**MIC**). Завдяки MIC можуть бути ліквідовані слабкі місця захисту, що сприяють проведенню атак з використанням підроблених фреймів і маніпуляції бітами. IEEE запропонувала спеціальний алгоритм, що одержав назву Michael (Майкл), щоб підсилити роль ICV у шифруванні фреймів даних стандарту *802.11*.

MIC має унікальний ключ, який відрізняється від ключа, використовуваного для шифрування фреймів даних. Цей *унікальний ключ* змішується із призначеним MAC-*Адресом* й вихідним MAC-*Адресом* фрейму, а також з усією незашифрованою частиною фрейму. На рис. 8.8 показана робота алгоритму Michael *MIC*.

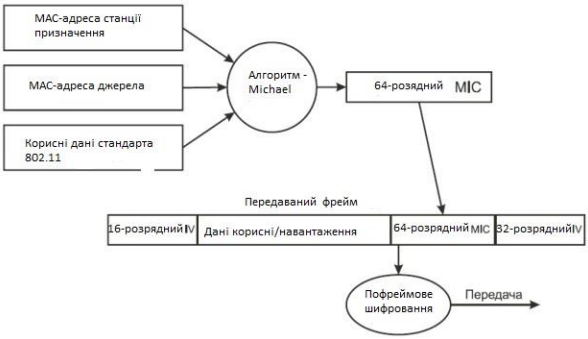


Рисунок 8.8 – Робота алгоритму Michael MIC

Механізм шифрування *TKIP* у цілому здійснюється в такий спосіб:

1. За допомогою алгоритму пофреймового призначення ключів генерується пофреймовий ключ (рис. 8.9).
2. Алгоритм *MIC* генерує *MIC* для фрейму в цілому.
3. Фрейм фрагментується відповідно до установок MAC щодо фрагментації.
4. Фрагменти фрейму шифруються за допомогою пофреймового ключа.
5. Здійснюється передача зашифрованих фрагментів.

Аналогічно процесу шифрування по алгоритму *TKIP*, процес дешифрування по цьому алгоритму виконується в такий спосіб (рис. 8.10):

– Попередньо обчислюється ключ 1-ї фази.

– На підставі IV, отриманого із вхідного фрагмента фрейму *WEP*, обчислюється пофреймовий ключ 2-ї фази.

– Якщо отриманий IV не той, який потрібно, фрейм відкидається.

– Фрагмент фрейму розшифровується, і здійснюється перевірка ознаки цілісності (ICV).

– Якщо контроль ознаки цілісності дає негативний результат, такий фрейм відкидається.

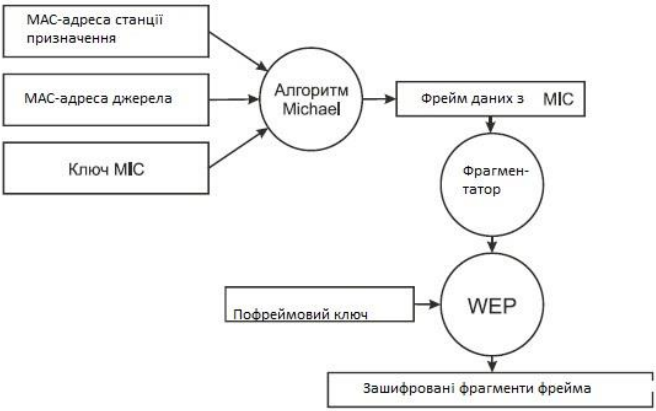


Рисунок 8.9 – Механізм шифрування TKIP

– Розшифровані фрагменти фрейму збираються, щоб одержати вихідний фрейм даних.

– Приймач обчислює значення *MIC* і порівнює його зі значенням, що перебувають у полі *MIC* фрейму.

– Якщо ці значення збігаються, фрейм обробляється приймачем.

– Якщо ці значення не збігаються, виходить, фрейм має помилку *MIC*, і приймач вживає заходів протидії *MIC*.

Заходу протидії MIC полягають у виконанні приймачем наступних завдань:

– Приймач видаляє існуючий ключ на асоціювання.

– Приймач реєструє проблему як стосовну до безпеки мережі.

– Асоційований клієнт, від якого був отриманий неправильний фрейм, не може бути асоційований і автентифікований протягом 60 секунд, щоб сповільнити атаку.

– Клієнт запитує новий ключ.

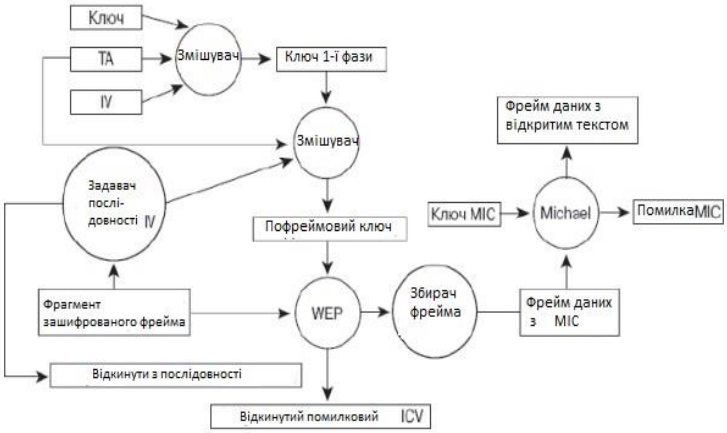


Рисунок 8.10 – Механізм дешифрування TKIP

WPA може працювати у двох режимах: *Enterprise* (корпоративний) і *Pre-Shared Key* (персональний).

У першому випадку – *Enterprise* (корпоративний) зберігання бази даних і перевірка автентичності по стандарту 802.1x у більших мережах звичайно здійснюються спеціальним сервером, найчастіше RADIUS (Remote Authentication Dial-In User Service). Enterprise-Режим ми розглянемо далі.

У другому випадку – *Pre-Shared Key* (персональний), тобто передбачається застосування *WPA* усіма категоріями користувачів бездротових мереж, де має місце спрощений режим, що не вимагає складних механізмів. Цей режим називається *WPA-PSK* і припускає введення одного пароля на кожний вузол бездротової мережі (точку доступу, бездротової маршрутизатор, клієнтський адаптер, міст). Доти, поки паролі збігаються, клієнтові буде дозволений доступ у мережу. Можна помітити, що підхід з використанням пароля робить *WPA-PSK* уразливим для атаки методом добору, однак цей режим рятує від плутанини із ключами *WEP*, заміняючи їх цілісною й чіткою системою на основі цифро-буквеного пароля.

Таким чином, *WPA/TKIP* – це вирішення, що надає більший у порівнянні з *WEP* рівень безпеки, спрямований на усунення слабких місць, що й забезпечує сумісність із більш старим

устаткуванням мереж *802.11* без внесення апаратних змін у пристрої.

Розгляд пофреймового призначення ключів і *MIC* стосувалося в основному ключа шифрування й ключа *MIC*. Але нічого не було сказано про те, як ключі генеруються й пересилаються від клієнта до точка доступу й навпаки. У розділі, присвяченому Enterprise-*Режиму* ми розглянемо пропонований стандартом 802.11i механізм керування ключами.

8.1.8. Стандарт мережі 802.11i з підвищеною безпекою (WPA2)

У червні 2004 р. IEEE ратифікував давно очікуваний стандарт забезпечення безпеки в бездротових локальних мережах – 802.11i.

Дійсно, *WPA* гідний відзначення як шедевр ретроінжинірінга. Створений з урахуванням слабких місць *WEP*, він являє собою дуже надійну систему безпеки для роботи з існуючим Wi-Fi-Устаткуванням. *WPA* – практичне рішення, що забезпечує достатній рівень безпеки для бездротових мереж.

Однак *WPA* – компромісне вирішення. Воно усе ще засноване на алгоритмі шифрування RC4 і протоколі TKIP Імовірність виявлення яких-небудь слабких місць хоча й мала, але все-таки існує.

Абсолютно нова система безпеки, позбавлена недоліків *WEP*, являє собою краще довгострокове й до того ж розширюваний розв'язок для безпеки бездротових мереж. Із цією метою комітет зі стандартів прийняв рішення розробити систему безпеки з нуля. Це новий стандарт 802.11i, також відомий як WPA2 і випущений тим же Wi-Fi Alliance.

Стандарт 802.11i використовує концепцію підвищеної безпеки (*Robust* Security Network – *RSN*), що передбачає, що бездротові пристрої повинні забезпечувати додаткові можливості. Це зажадає змін в апаратної частини й програмному забезпеченні, тобто мережа, що повністю відповідає *RSN*, стане несумісною з існуючим устаткуванням *WEP*. У перехідний період буде підтримуватися як устаткування *RSN*, так і *WEP* (насправді *WPA*/*TKIP* було вирішенням, спрямованим на

збереження інвестицій в устаткування), але надалі пристрої *WEP* почнуть відмирати.

802.11i прикладемо до різних мережних реалізацій і може задіяти *TKIP*, але за замовчуванням *RSN* використовує AES (Advanced Encryption Standard) і CCMP (Counter Mode *CBC* MAC Protocol) і, таким чином, є могутнішим розширюваним рішенням.

У концепції *RSN* застосовується AES у якості системи шифрування, подібно тому як алгоритм *RC4* задіяний в *WPA*. Однак механізм шифрування куди більш складний і не страждає від проблем, властивих *WEP* AES – *блоковий шифр*, що оперує блоками даних по 128 біт. CCMP, у свою чергу, – протокол безпеки, використовуваний AES. Він є еквівалентом *TKIP* в *WPA*. CCMP обчислює *MIC*, прибігаючи до добре відомого й перевіреного методу *Cipher* Block Chaining *Message Authentication* Code (*CBC-MAC*). Зміна навіть одного біта в повідомленні приводить до зовсім іншого результату.

Однієї зі слабких сторін *WEP* було керування секретними ключами. Багато адміністраторів більших мереж знаходили його незручним. Ключі *WEP* не мінялися тривалий час (або ніколи), що полегшувало завдання зловмисникам.

RSN визначає ієрархію ключів з обмеженим терміном дії, подібну з *TKIP* В AES/CCMP, щоб умістити всі ключі, потрібно 512 біт – менше, чим в *TKIP* В обох випадках майстер-ключі використовуються не прямо, а для виводу інших ключів. На щастя, адміністратор повинен забезпечити єдиний майстер-*ключ*. Повідомлення складаються з 128-бітного блоку даних, зашифрованого секретним ключем такої ж довжини (128 біт). Хоча процес шифрування складний, адміністратор знов-таки не повинен вникати в нюанси обчислень. Кінцевим результатом є шифр, який набагато складніше, ніж навіть *WPA*.

802.11i (*WPA2*) – це найбільш стійке, розширюване і безпечне вирішення, призначене в першу чергу для великих підприємств, де керування ключами й адміністрування доставляє безліч турбот.

Стандарт 802.11i розроблений на базі перевірених технологій. *Механізми безпеки* були спроектовані з нуля в тісному співробітництві із кращими фахівцями із криптографії й

мають усі шанси стати тим рішенням, яке необхідно бездротовим мережам. Хоча жодна система безпеки від злому не застрахована, 802.11i – це розв'язок, на який можна покладатися, у ньому немає недоліків попередніх систем. І, звичайно, WPA придатний для адаптації вже існуючого встаткування, і тільки коли його ресурси будуть остаточно вичерпані, ви зможете замінити його новим, повністю відповідним до концепції *RSN*.

Продуктивність каналу зв'язку, як свідчать результати тестування встаткування різних виробників, падає на 5-20% при включенні як WEP, так і WPA. Однак випробування того встаткування, у якому включено шифрування AES замість *TKIP*, не показали скільки-небудь помітного падіння швидкості. Це дозволяє сподіватися, що *WPA 2-сумісне* встаткування надасть нам довгоочікуваний надійно захищений канал без втрат у продуктивності.

WPA2, як і *WPA*, може працювати у двох режимах: *Enterprise* (корпоративний) і *Pre-Shared Key* (персональний).

8.1.9. Налаштування точки доступу із застосуванням персональної специфікації WPA2-PSK

1. Для цього підключаємося до точки доступу по провідному *інтерфейсу, вводимо* режим, *SSID*, канал, як було описано в прикладі 1.4. Далі в поле Authentication (Автентифікація) ставимо *WPA2-PSK* (рис. 8.11).

2. Вибираємо тип шифрування (Cipher Type). Можливі варіанти: AUTO, TKIP, AES. Якщо виставлене AUTO, точка доступу буде підбудовувати тип шифрування під першого клієнта, що підключився.

3. Виставляємо інтервал відновлення групового ключа (Group Key Update Interval), який задається в секундах.

4. Уводимо в поле Passphrase ключ будь-якої довжини, але не менш 8 символів, наприклад secretpass.

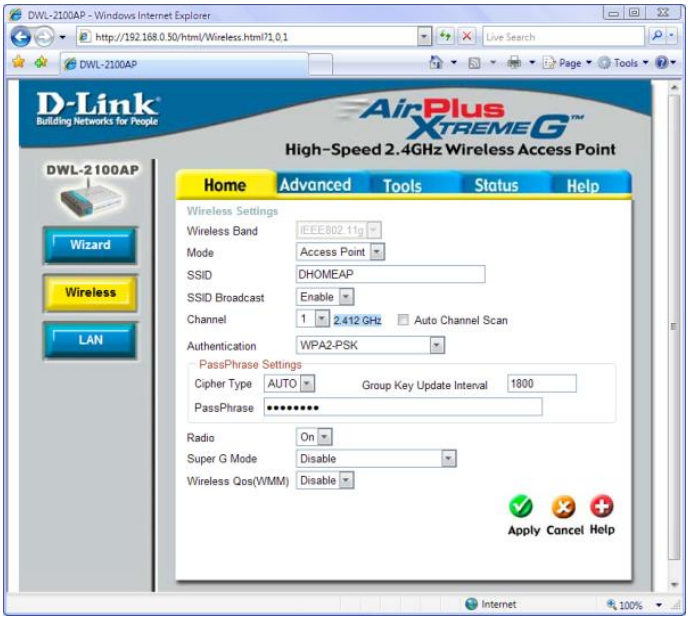


Рисунок 8.11 – Налаштування точки доступу із застосуванням персональної специфікації WPA2-PSK

Тепер, після застосування настроювань, на клієнтській стороні треба виставити ті ж самі параметри й підключитися до неї.

8.1.10. Стандарт 802.1x/EAP (Enterprise-Режим)

Проблеми, з якими зіштовхнулися розроблювачі й користувачі мереж на основі стандарту *802.11*, змусили шукати нові вирішення захисту бездротових мереж. Були виявлені компоненти, що впливають на системи безпеки бездротової локальної мережі:

– Архітектура автентифікації.
– Механізм автентифікації.
– Механізм забезпечення конфіденційності й цілісності даних.

Архітектура автентифікації IEEE 802.1x – стандарт IEEE 802.1x описує єдину архітектуру контролю доступу до портів з використанням різноманітних методів автентифікації абонентів.

Алгоритм автентифікації Extensible Authentication Protocol або EAP (розширюваний протокол ідентифікації) підтримує централізовану автентифікацію елементів інфраструктури бездротової мережі і її користувачів з можливістю динамічної *генерації ключів* шифрування.

Архітектура IEEE 802.1x містить у собі наступні обов'язкові логічні елементи (рис.8.12):

– Клієнт (Supplicant) – перебуває в операційній системі абонента;

– *Автентифікатор* (Authenticator) – перебуває в програмному забезпеченні точкарадіодоступу ;

– Сервер автентифікації (*Authentication Server*) – перебуває на Radius-Сервері.

IEEE 802.1x надає абонентові бездротової локальної мережі лише засобу передачі атрибутів серверу автентифікації й допускає використання різних методів і алгоритмів автентифікації. Завданням сервера автентифікації є підтримка дозволених політикою мережної *безпеки методів* автентифікації.

Автентифікатор, перебуваючи в точці радіодоступу, створює логічний порт для кожного клієнта на основі його ідентифікатора асоціювання. Логічний порт має два канали для обміну даними. Неконтрольований канал безперешкодно пропускає трафік з бездротового сегмента в провідний і назад, у той час як контрольований канал вимагає успішної автентифікації для проходження фреймів.

Таким чином, у термінології стандарту 802.1x точка доступу відіграє роль комутатора в провідних мережах Ethernet. Очевидно, що провідний сегмент мережі, до якого підключена точка доступу, потребує сервера автентифікації. Його функції звичайно виконує Radius-Сервер, інтегрований з тієї або іншою *базою даних користувачів*, у якості якої може виступати стандартний RADIUS, LDAP, *NDS* або Windows Active Directory. Комерційні бездротові шлюзи високого класу можуть

реалізовувати як функції сервера автентифікації, так і автентифікатора.

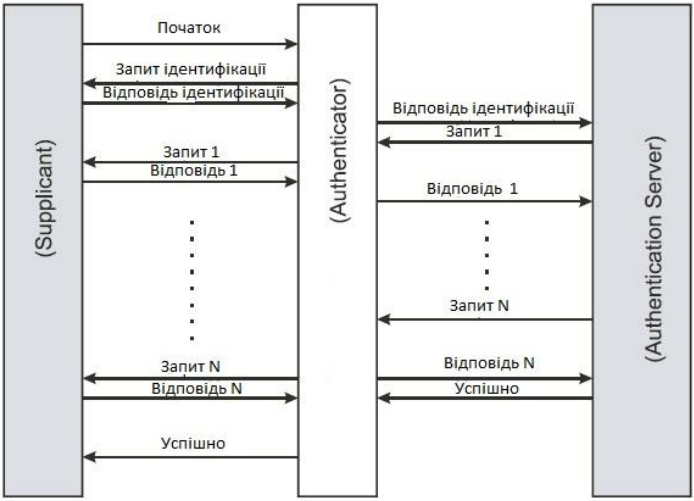


Рисунок 8.12 – Архітектура IEEE 802.1x

Клієнт активізується й асоціюється із точкою радіодоступу (або фізично підключається до сегмента у випадку провідної локальної мережі). *Автентифікатор* розпізнає факт підключення й активізує логічний порт для клієнта, відразу переводячи його в стан «неавторизований». У результаті через клієнтський порт можливий лише обмін трафіком протоколу IEEE 802.1x, для всього іншого трафіка порт заблокований. Клієнт також може (але не зобов'язаний) відправити повідомлення *EAP* Start (початок автентифікації *EAP*) (рис. 8.13) для запуску процесу автентифікації.

Автентифікатор відправляє повідомлення *EAP* Request Identity (запит імені *EAP*) і очікує від клієнта його ім'я (Identity). Відповідне повідомлення клієнта *EAP* Response (відповідь *EAP*), що містить атрибути, перенаправляється серверу автентифікації.

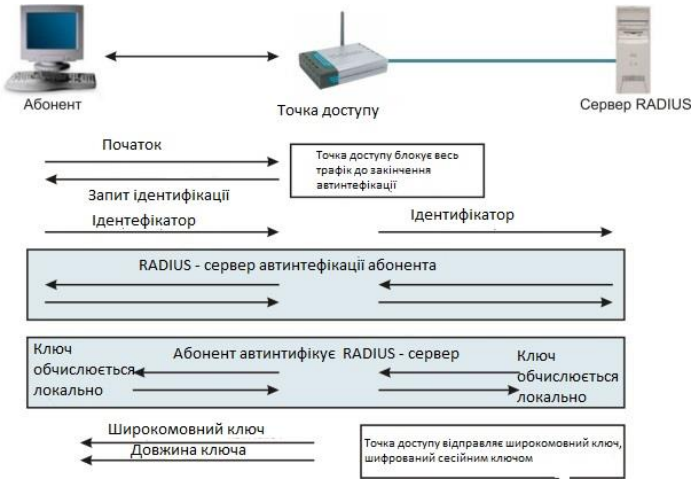


Рисунок 8.13 – Обмін повідомленнями в 802.1x/EAP

Після завершення автентифікації сервер відправляє повідомлення RADIUS-ACCEPT (прийняти) або RADIUS-REJECT (відхилити) *автентифікатору*. При одержанні повідомлення RADIUS-ACCEPT *автентифікатор* переводить порт клієнта в стан «авторизований», і починається передача всього трафіка абонента.

8.2. Механізм автентифікації

Спочатку стандарт 802.1x замислювався для того, щоб забезпечити автентифікацію користувачів на канальному рівні в провідних мережах, що комутируються.

Алгоритми автентифікації стандарту *802.11* можуть забезпечити клієнта динамічними, орієнтованими на користувача ключами. Але той ключ, який створюється в процесі автентифікації, не є ключем, використовуваним для шифрування фреймів або перевірки цілісності повідомлень. У стандарті *WPA* для одержання всіх ключів використовується так званий майстер-*ключ* (Master Key). На рис. 8.14 представлена ієрархія ключів з урахуванням послідовності їх створення.

Механізм *генерації ключів* шифрування здійснюється в чотири етапи:

1. Клієнт і точка доступу встановлюють динамічний ключ (він називається *парний майстер-ключ*, або PMK, від англ. Pairwise Master Key), отриманий у процесі автентифікації по стандарту 802.1x.

2. Точка доступу посилає клієнтові секретне випадкове число, яке називається *тимчасовий автентифікатор* (Authenticator Nonce – Anonce), використовуючи для цього повідомлення Eapol-key стандарту 802.1x.

3. Цей клієнт локально генерує секретне випадкове число, називане *тимчасовий прохач* (Supplicant Nonce – Snonce).

4. Клієнт генерує *парний перехідний ключ* (Pairwise Transient Key – PTK) шляхом комбінування PMK, Snonce, Anonce, Mac-Адреси клієнта, Mac-Адреси точка доступу й рядка ініціалізації.Mac-Адреси впорядковані, Mac-Адреси нижчого порядку передують Mac-Адресам вищого порядку. Завдяки цьому гарантується, що клієнт і точка доступу «вибудують» Mac-Адреси однаковим образом (рис. 8.16).

5. Це комбіноване значення пропускається через псевдовипадкову функцію (Pseudo Random Function – PRF), щоб одержати 512-розрядний PTK.

6. Клієнт посилає число Snonce, згенероване їм на етапі 3, крапці доступу за допомогою повідомлення Eapol-key стандарту 802.1x, захищеного ключем Eapol-key *MIC*.

7. Точка доступу використовує число Snonce для обчислення PTK у такий же спосіб, як це зробив клієнт.

8. Точка доступу використовує виведений ключ Eapol-key *MIC* для перевірки цілісності повідомлення клієнта.

9. Точка доступу посилає повідомлення Eapol-key, що показує, що клієнт може встановити PTK і його Anonce, захищені ключем Eapol-key *MIC*. Даний етап дозволяє клієнтові впевнитися в тому, що число Anonce, отримане на етапі 2, дійсно.

10. Клієнт посилає повідомлення Eapol-key, захищене ключем Eapol-key *MIC*, що вказує, що ключі встановлені.

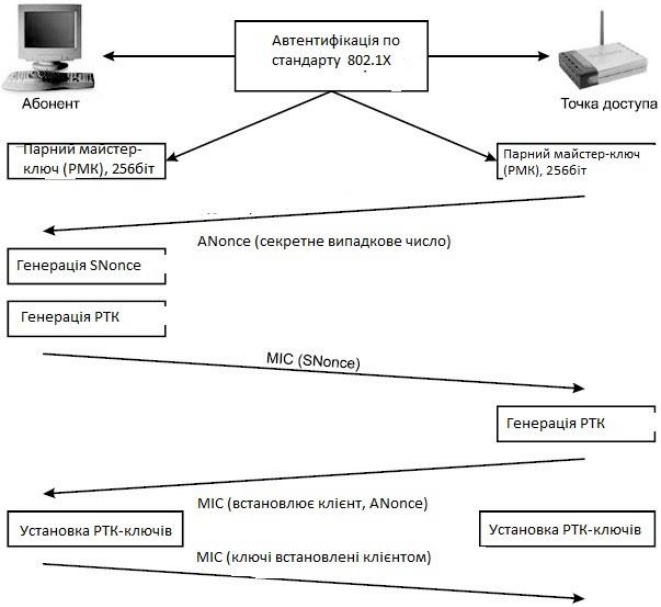


Рисунок 8.14 – Створення ключів

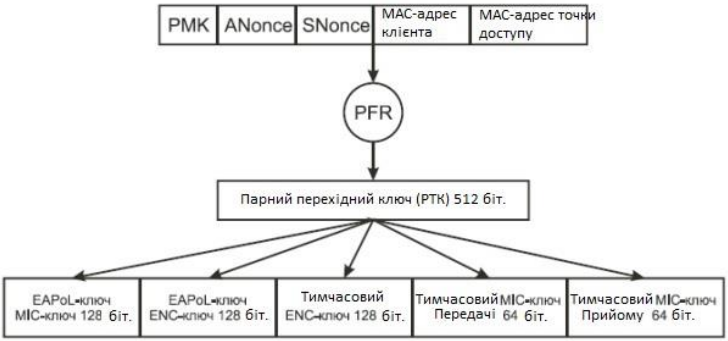


Рисунок 8.15 – Генерація парного перехідного ключа

Парний майстер-*ключ* (PMK) і парний перехідний ключ (PTK) є одноадресними. Вони тільки шифрують і дешифрують

одноадресні фрейми, і призначені для єдиного користувача. Широкомовні фрейми вимагають окремої ієрархії ключів, тому що використання із цією метою одноадресних ключів приведе до різкого зростання трафіка мережі. Крапці доступу (єдиному об'єкту BSS, що має право на розсилання широкомовних або багатоадресних повідомлень) довелося б посилати той самий широкомовний або багатоадресний фрейм, зашифрований відповідними пофреймовими ключами, кожному користувачеві.

Широкомовні або багатоадресні фрейми використовують ієрархію *групових ключів*. Груповий майстер-*ключ* (Group Master Key – GMK) перебуває на вершині цієї ієрархії й виводиться в крапці доступу. Вивід GMK заснований на застосуванні PRF, у результаті чого виходить 256-розрядний GMK. Вхідними даними для PRF-256 є шифрувальне секретне випадкове число (або Nonce), текстовий рядок, Мас-Адреса точка доступу й значення часу у форматі синхронізуючого мережного протоколу (NTP). На рис. 8.16 представлена ієрархія групових ключів.

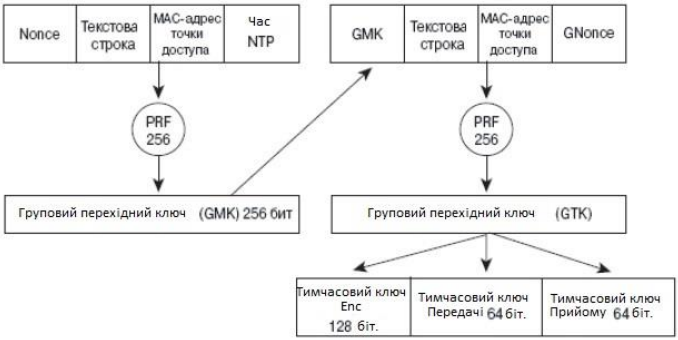


Рисунок 8.16 – Ієрархія групових ключів

Груповий майстер-*ключ*, текстовий рядок, Мас-Адреса точка доступу й Gnonce (значення, яке береться з лічильника ключа точка доступу) поєднуються й обробляються за допомогою PRF, у результаті чого виходить 256-розрядний груповий перехідний ключ (Group Transient Key – GTK). GTK ділиться на 128-розрядний ключ шифрування широкомовних/багатоадресних

фреймів, 64-розрядний ключ передачі *MIC* (transmit *MIC* key) і 64-розрядний ключ приймання *MIC* (*MIC* receive key).

За допомогою цих ключів широкомовні й багатоадресні фрейми шифруються й дешифруються точно так само, як за допомогою одноадресних ключів, отриманих на основі парного майстер-ключа (PMK).

Клієнт обновляється за допомогою групових ключів шифрування через повідомлення Eapol-key Точка доступу посилає такому клієнтові повідомлення Eapol, зашифроване за допомогою одноадресного ключа шифрування. Групові ключі віддаляються й регенеруються щораз, коли яка-небудь станція дисоціюється або деавтентифікується в BSS. Якщо відбувається помилка *MIC*, однієї із заходів протидії також є видалення всіх ключів із прийомної станції, що має відношення до помилки, включаючи групові ключі.

У домашніх мережах або мережах, призначених для малих офісів, розгортання Radius-Сервера з базою даних кінцевих користувачів малоймовірно. У такому випадку для генерування сеансових ключів використовується тільки попередньо розділений PMK (уводиться вручну). Це аналогічно тому, що робиться в оригінальному протоколі *WEP*.

Оскільки в локальних мережах *802.11* немає фізичних портів, асоціація між бездротовим клієнтським пристроєм і точкою доступу вважається мережним портом доступу. Бездротовий клієнт розглядається як претендент, а точка доступу – як *автентифікатор*.

У стандарті 802.1x автентифікація користувачів на канальному рівні виконується по протоколу *EAP*, який був розроблений Групою із проблем проектування Internet (IETF). Протокол *EAP* – це заміна протоколу CHAP (*Challenge* Handshake *Authentication Protocol* – протокол взаємної автентифікації), який застосовується в PPP (Point to Point Protocol – протокол з'єднання «точка-точка»), він призначений для використання в локальних мережах. Специфікація EAPOL визначає, як фрейми EAP інкапсулюються у фрейми 802.3, 802.5 і *802.11*. Обмін фреймами між об'єктами, певними в стандарті 802.1x, схематично зображений на рис. 8.17.

EAP є «узагальненим» протоколом у *системі автентифікації*, авторизації й обліку (Authentication, Authorization, and Accounting – AAA), що забезпечують роботу різноманітних методів автентифікації. AAA-Клієнт (сервер доступу в термінології AAA, у бездротовій мережі представлений точкою радіодоступу), що підтримує *EAP*, може не розуміти конкретних методів, використовуваних абонентом і мережею в процесі автентифікації. Сервер доступу тунелює повідомлення протоколу автентифікації, що циркулюють між абонентом і сервером автентифікації. Сервер доступу цікавить лише факт початку й закінчення процесу автентифікації.

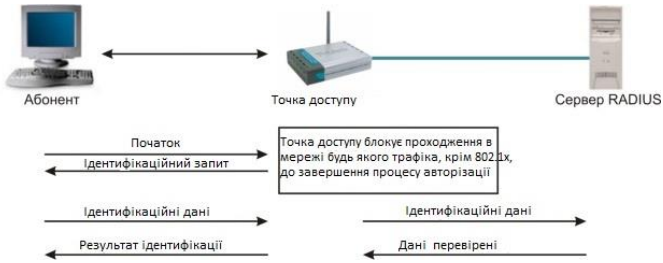


Рисунок 8.17 – Механізм автентифікації в 802.1x/EAP

Є кілька варіантів EAP, спроектованих за участю різних компаній-виробників. Така різноманітність вносить додаткові проблеми сумісності, так що вибір підходящого встаткування й програмного забезпечення для бездротової мережі стає нетривіальним завданням. При конфігуруванні способу автентифікації користувачів у бездротовій мережі вам, імовірно, прийде зіштовхнутися з наступними варіантами EAP:

– *EAP-MD*5 – це обов'язковий рівень EAP, який повинен бути присутнім у всіх реалізаціях стандарту 802.1x, саме він був розроблений першим. З погляду роботи він дублює протокол CHAP. Ми не рекомендуємо користуватися протоколом *EAP-MD*5 по трьом причинам. По-перше, він не підтримує динамічний розподіл ключів. По-друге, він уразливий для атаки «людей посередині» із застосуванням фальшивої точка доступу й для атаки на сервер автентифікації, тому що автентифікується

тільки клієнти. І нарешті, у ході автентифікації супротивник може підслухати запит і зашифрована відповідь, після чого почати атаку з відомим відкритим або шифрованим текстом;

– *EAP-TLS* (*Eap-transport* Layer Security – протокол захисту транспортного рівня) підтримує взаємну автентифікацію на базі сертифікатів. *EAP-TLS* заснований на протоколі Sslv3 і вимагає наявності центру, що засвідчує. Протоколи TLS і SSL використовують ряд елементів інфраструктури PKI (Public Key Infrastructure): Абонент повинен мати діючий сертифікат для автентифікації стосовно мережі. Ааа-Сервер повинен мати діючий сертифікат для автентифікації стосовно абонента.

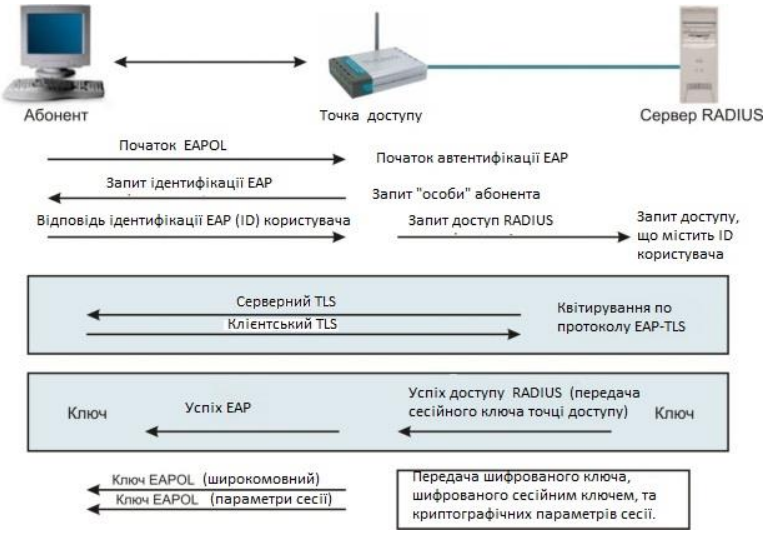


Рисунок 8.18 – Процес автентифікації EAP-TLS

Орган сертифікації із супутньою інфраструктурою управляє сертифікатами суб'єктів PKI. Клієнт і Radius-Сервер повинні підтримувати метод автентифікації *EAP-TLS*. Точка радіодоступу повинна підтримувати процес автентифікації в рамках 802.1x/*EAP*, хоча може й не знати деталей конкретного методу автентифікації. Загальний вид *EAP-TLS* виглядає приблизно так (рис. 8.18).

– *EAP-LEAP* (Lightweight EAP, полегшений *EAP*) – це запатентований компанією Cisco варіант EAP, реалізований у точках доступу й бездротових клієнтських картах Cisco. LEAP був першою (і протягом тривалого часу єдиної) схемою автентифікації в стандарті 802.1x, заснованої на паролях. Тому LEAP набув величезну популярності й навіть підтриманий у сервері Free-radius, незважаючи на те, що цей запатентований розв'язок. Сервер автентифікації посилає клієнтові запит, а той повинен повернути пароль, попередньо виконавши його згортку з рядком запиту. Заснований на застосуванні паролів, *EAP-LEAP* аутентифікує користувача, а не пристрій. У той же час очевидна уразливість цього варіанта для атак методом повного перебору й по словникові, нехарактерна для методів автентифікації із застосуванням сертифікатів.

– PEAP (Protected EAP – захищений *EAP*) і *EAP-TTLS* (Tunneled Transport Layer Security EAP, протокол захисту транспортного рівня *EAP*), розроблений компанією Certicom and Funk Software. Ці варіанти також досить розвинені, і підтримуються виробниками, зокрема D-link. Для роботи *EAP-TTLS* потрібно, щоб був сертифікований тільки сервер автентифікації, а в претендента сертифіката може й не бути, так що процедура розгортання спрощується. *EAP-TTLS* підтримує також ряд застарілих методів автентифікації, у тому числі PAP, CHAP, MS-CHAP, Ms-chapv2 і навіть *EAP-MD*5. Щоб забезпечити безпека при використанні цих методів, *EAP-TTLS* створює зашифрований по протоколу TLS тунель, усередині якого ці протоколи й працюють. Прикладом практичної реалізації *EAP-TTLS* може служити програмне забезпечення для керування доступом у бездротову мережу Odyssey від компанії Funk Software. 2. У загальному виді схема обміну PEAP виглядає в такий спосіб (рис. 8.19):

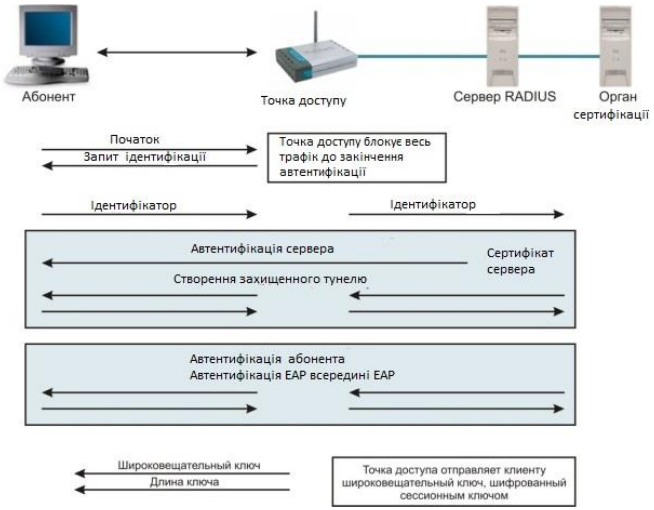


Рисунок 8.19 – Процес автентифікації PEAP

Протокол PEAP дуже схожий на *EAP-TTLS*, тільки він не підтримує застарілих методів автентифікації типу PAP і CHAP. Замість них підтримуються протоколи Peap-ms-chapv2 і PEAP-EAP-TLS, що працюють усередині безпечного тунелю. Підтримка PEAP реалізована в пакеті програм точок доступу D-link і успішно реалізована в Windows XP, починаючи з Service Pack

– Ще два варіанти EAP – це *EAP-SIM* і EAP-AKA для автентифікації на базі SIM і USIM. У даний момент обоє мають статус попередніх документів IETF і в основному призначені для автентифікації в мережах GSM, а не в бездротових мережах *802.11*. Проте протокол *EAP-SIM* підтриманий у точках доступу й клієнтських пристроях деяких виробників.

Рівні архітектури 802.1x показані на рис. 8.20.

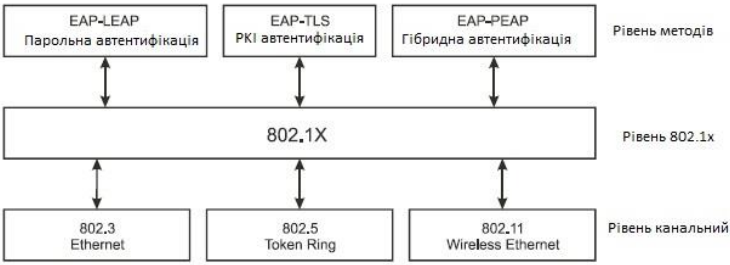


Рисунок 8.20 – Рівні архітектури 802.1x

Тут у якості механізму забезпечення конфіденційності й цілісності даних виступають стандарти шифрування WPA і WPA2.

9. РОЗГОРТАННЯ БЕЗДРОТОВИХ ВІРТУАЛЬНИХ МЕРЕЖ

9.1. Технології цілісності й конфіденційності переданих даних

Віртуальна приватна *мережа* (*Virtual Private Network – VPN*) – це метод, що дозволяє скористатися загальнодоступною телекомунікаційною інфраструктурою, наприклад *Internet*, для надання вилученим офісам або окремим користувачам безпечного доступу до мережі організації. Оскільки бездротові мережі *802.11* працюють у неліцензованому діапазоні частот і доступні для прослуховування. Саме в них розгортання й обслуговування VPN здобуває особливу важливість, якщо необхідно забезпечити високий рівень захисту інформації.

Захищати потрібно як з'єднання між хостами в бездротовій локальній мережі, так і двухточковіканали між бездротовими мостами. Для забезпечення безпеки особливо секретних даних не можна покладатися на якийсь один механізм або на захист лише одного рівня мережі. У випадку двухточкових каналів простіше й економічніше розгорнути *VPN*, що покриває дві мережі, чим реалізовувати захист на базі стандарту 802.11i, що включає Radius-Сервер і базу даних про користувачів.

Користуватися ж реалізацією стандарту на базі попередньо розділених ключів (PSK) і протоколу 802.1x при наявності високошвидкісного каналу між мережами – не самий безпечний метод. VPN – це повна протилежність дорогій системі власних або орендованих ліній, які можуть використовуватися тільки однією організацією. Завдання VPN – надати організації ті ж можливості, але за набагато менші гроші. Зрівняєте це із забезпеченням зв'язку за рахунок двухточкових бездротових каналів з мостами замість дорогих виділених ліній.

VPN і бездротові технології не конкурують, а доповнюють один одного. VPN працює поверх поділюваних мереж загального користування, забезпечуючи в той же час конфіденційність за рахунок спеціальних заходів безпеки й застосування тунельних

протоколів, таких як тунельний протокол на канальному рівні (Layer Two Tunneling Protocol – L2TP). Зміст їх у тому, що,здійснюючи шифрування даних на кінці, що відправляє, і дешифрування на, що ухвалює, протокол організує «тунель», у який не можуть проникнути дані, не зашифровані належним чином. Додаткову безпеку може забезпечити шифрування не тільки самих даних, але й мережних адрес відправника й одержувача. Бездротову локальну мережу можна зрівняти з поділюваною мережею загального користування, а в деяких випадках (хот-споти, вузли, що належать співтовариствам) вона такий і є.

VPN відповідає трьом умовам: конфіденційність, цілісність і доступність. Слід зазначити, що ніяка VPN не є стійкою до Dos- або Ddos-Атакам і не може гарантувати доступність на фізичному рівні просто в силу своєї віртуальної природи й залежності від нижченаведених протоколів.

Дві найбільш важливі особливості VPN, особливо в бездротових середовищах, де є лише обмежений контроль над поширенням сигналу, – це цілісність і, що ще більш суттєво, конфіденційність даних. Поберемо життєву ситуацію, коли зловмисникові вдалося подолати шифрування по протоколу WEP і приєднатися до бездротової локальної мережі. Якщо VPN відсутній, то він зможе прослуховувати дані й втручатися в роботу мережі. Але якщо пакети автентифіковані, *атака* «людей посередині» стає практично неможливої, хоча *перехопити дані* як і раніше легко. Включення в *VPN*елемента шифрування зменшує негативні наслідки *перехоплення даних*. *VPN* забезпечує не стільки повну ізоляцію всіх мережних взаємодій, скільки здійснення таких взаємодій у більш контрольованих умовах із чітко певними групами допущених учасників.

Є багато способів класифікації VPN, але основні три види – це «мережа-мережа», «хост-мережа» і «хост-хост».

9.2. Топологія «мережа-мережа»

Цим терміном іноді описують VPN-Тунель між двома географічно рознесеними приватними мережами (рис. 9.1).

Рисунок 9.1 – Топологія «мережа-мережа»

VPN такого типу звичайно застосовуються, коли потрібно об'єднати локальні мережі за допомогою мережі загального користування так, начебто вони перебувають усередині одного будинку.

Основна перевага такої конфігурації полягає в тому, що мережі виглядають як суміжні, а робота VPN-Шлюзів прозора для користувачів. У цьому випадку також важливо тунелювання, оскільки в приватних мережах звичайно використовуються описані в RFC 1918 зарезервовані адреси, які не можуть маршрутизуватися через Internet. Тому для успішної взаємодії трафік необхідно інкапсулювати у тунель.

Типовим прикладом такої мережі може бути з'єднання двох філій однієї організації по двухточковому бездротовому каналу. Хоча трафік і не виходить за межі внутрішньої інфраструктури організації, до її бездротової частини потрібно ставитися так само уважно, як якби трафік маршрутизувався через мережу загального користування. Ви вже бачили, що протокол WEP можна легко подолати й навіть TKIP іноді вразливий, тому ми настійно рекомендуємо всюди, де можливо, реалізовувати додаткове шифрування.

9.3. Топологія «хост-мережа»

При такій конфігурації віддалені користувачі підключаються до корпоративної мережі через Internet.

Спочатку мобільний клієнт установлює з'єднання з Internet, а потім ініціює запит на організацію зашифрованого тунелю корпоративним Vpn-Шлюзом. Після успішної автентифікації створюється *тунель* поверх мережі загального користування, і клієнт стає просто ще однієї машиною у внутрішній мережі. Усе більш широке поширення надомної роботи стимулює інтерес до такого застосування VPN.

На відміну від VPN типу «мережа-мережа», де число учасників невелике й більш-менш передбачуване, VPN типу «хост-мережа» легко може вирости до неосяжних розмірів. Тому системний адміністратор повинен заздалегідь продумати масштабований механізм автентифікації клієнтів і керування ключами.

9.4. Топологія «хост-хост»

Така топологія, очевидно, зустрічається рідше всього. Мова йде про два хости, що обмінюються один з одним шифрованими й нешифрованими даними. У такій конфігурації *тунель* організує між двома хостами й увесь трафік між ними інкапсулюється усередині VPN. У таких мереж не багато практичних застосувань, але, як приклад, можна назвати географічно вилучений сервер резервного зберігання. Обоє хостів підключені до Internet, і дані із центрального сервера дзеркально копіюються на резервний. Наприклад, прості мережі VPN типу «хост-хост» можна використовувати для захисту однорангових (Ad Hoc) мереж.

10. РОЗПОВСЮДЖЕНІ МЕРЕЖНІ ТУНЕЛЬНІ ПРОТОКОЛИ

10.1. Протокол Ipsec

Ipsec – це найбільше широко визнаний, підтримуваний і стандартизований із усіх протоколів VPN. Для забезпечення спільної роботи він підходить краще інших. *Ipsec* лежить в основі відкритих стандартів, у яких описаний цілий набір безпечних протоколів, що працюють поверх існуючого стека IP. Він надає служби автентифікації й шифрування даних на мережному рівні (рівень 3) моделі OSI і може бути реалізований на будь-якому пристрої, який працює по протоколу IP. На відміну від багатьох інших схем шифрування, які захищають конкретний протокол верхнього рівня, *Ipsec*, що працює на нижньому рівні, може захистити весь Ip-Трафік. Він застосовується також у комбінації з тунельними протоколами на канальному рівні (рівень 2) для шифрування й автентифікації трафіка, переданого по протоколах, відмінних від IP.

Протокол *Ipsec* складається із трьох основних частин:

– заголовка автентифікації (Authentication Header – AH);

– безпечно інкапсульованого корисного навантаження (*Encapsulating Security Payload – ESP*);

– схеми обміну ключами через Internet (Internet Key Exchange – *IKE*).

Заголовок AH додається після заголовка IP і забезпечує автентифікацию на рівні пакета й цілісність даних. Іншими словами, гарантується, що пакет не був змінений на шляху проходження й зробив з очікуваного джерела. *ESP* забезпечує конфіденційність, *автентифікацию джерела даних*, цілісність, опціональний захист від атаки повторного сеансу й певною мірою *скритність* механізму керування потоком. Нарешті, *IKE* забезпечує узгодження настроювань служб безпеки між боками-учасниками.

10.2. Протокол PPTP

Двухточковий тунельний протокол (Point-to-Point *Tunneling* Protocol – PPTP) – це запатентована розробка компанії Microsoft, він призначений для організації взаємодії по типу VPN. PPTP забезпечує автентифікацию користувачів за допомогою таких протоколів, як MS-CHAP, *CHAP*, SPAP і PAP. Цьому протоколу бракує гнучкості, властивої іншим розв'язкам, він не занадто добре пристосований для спільної роботи з іншими протоколами VPN, зате простий і широко розповсюджений в усьому світі.

Протокол визначає наступні типи комунікацій:

- PPTP-З'єднання, по якому клієнт організує PPTP-Канал із провайдером;
- Керуюче PPTP-З'єднання, яке клієнт організує з Vpn-Сервером і по якому погодить характеристики *тунелю*;
- PPTP-Тунель, по якому клієнт і сервер обмінюються зашифрованими даними.

Протокол PPTP звичайно застосовується для створення безпечних каналів зв'язки між багатьма Windows-Машинами в мережі *Intranet*.

10.3. Протокол L2TP

Цей протокол, спільно розроблений компаніями Cisco, Microsoft і *3Com*, обіцяє замінити PPTP у якості основного тунельного протоколу. По суті *L2TP* (Layer Two *Tunneling* Protocol, протокол *тунелювання* канального рівня) являє собою комбінацію PPTP і створеного Cisco протоколу Layer Two Forwarding (L2F). Протокол *L2TP* застосовується для *тунелювання*ppp-*трафіка* поверх Ip-Мережі загального користування. Для встановлення з'єднання по лінії, що комутується, у ньому використовується PPP із автентифікацією по протоколу та, *або* CHAP, але, на відміну від PPTP, *L2*TP визначає власний тунельний протокол.

Оскільки *L2TP* працює на канальному рівні (рівень 2), через *тунель* можна пропускати й не-IP трафік. Разом з тим *L2TP*совместим з будь-яким канальним протоколом, наприклад

ATM, *Frame Relay* або *802.11*. Сам по собі протокол не містить засобів шифрування, але може бути використаний у комбінації з іншими протоколами або механізмами шифрування на прикладному рівні.

10.4. Системи виявлення вторгнення в бездротові мережі

Системи виявлення вторгнення (*Intrusion Detection System – IDS*) – це пристрої, за допомогою яких можна виявляти й вчасно запобігати вторгненням в обчислювальні мережі. Вони діляться на два види: на базі мережі й на базі хоста.

Мережні системи (*Network Intrusion Detection* Systems – *NIDS*) аналізують трафік з метою виявлення відомих атак на підставі наявних у них наборів правил (експертні системи). *Виключення* з погляду принципів аналізу становлять системи на базі нейромереж і штучного інтелекту. Підмножиною мережних систем виявлення вторгнень є системи для спостереження тільки за одним вузлом мережі (*Network Node IDS*).

Інший вид систем виявлення вторгнень представляють системи на базі хоста (*Host Intrusion Detection* Systems – *HIDS*). Вони встановлюються безпосередньо на вузлах і здійснюють спостереження за цілісністю файлової системи, системних журналів і т.д.

NIDS діляться у свою *чергу* на дві більші категорії: на основі сигнатур і на основі бази знань. Сигнатурні (*Intrusion Detection* Systems *IDS* найпоширеніші й простіше реалізуються, але їх легко обійти й вони не здатні розпізнавати нові атаки. У таких системах події, що відбуваються в мережі, рівняються з ознаками відомих атак, які й називаються сигнатурами. Якщо інструмент злому модифікувати з метою зміни якої-небудь частини *сигнатури атаки*, то швидше за все *атака* залишиться непоміченої. Крім того, *бази даних*, що містять сигнатури, необхідно надійно захищати й часто обновляти. *IDS* на основі бази знань стежать за мережею, збирають статистику про її поведінку в нормальних умовах, виявляють різні особливості й

позначають їх як підозрілі. Тому такі *IDS* ще називають заснованими на поведінці або статистичними.

Найпростіша архітектура IDS представлена на рис. 10.1.

Рисунок 10.1 – Основні елементи архітектури систем виявлення вторгнень

Для ефективної роботи статистичної *IDS* необхідно мати надійну інформацію про те, як поводиться *мережа* в нормальних умовах, – точку відліку. Хоча таку *IDS* обдурити складніше, але й у неї є свої слабкі місця – неправильні спрацьовування й труднощі при виявленні деяких видів комунікацій по схованому каналу. Неправильні спрацьовування особливо ймовірні в бездротових мережах через нестабільність передавального середовища. Крім того, атаки, проведені на ранніх стадіях періоду фіксації точка відліку, можуть спотворити процедуру навчання статистичної *IDS*, тому її *розгортання* в промисловій мережі – заняття ризиковане. Як бути, якщо нормальна поведінка мережі вже змінена зломщиком у момент розгортання?

IDS для бездротової мережі повинна бути одночасно сигнатурної й статистичної. Деякі інструменти для проведення атак на бездротові мережі мають чітко виражені сигнатури. Якщо вони виявляються в базі даних, то можна здіймати тривогу. З

іншого боку, у багатьох атак очевидних сигнатур ні, зате вони викликають відхилення від нормальної роботи мережі на нижніх рівнях стека протоколів. Відхилення може бути малопомітним. Виявлення таких аномалій – непросте завдання, оскільки не існує двох однакові бездротові мереж. Те ж ставиться й до провідних локальних мереж, але там хоча б немає радіоперешкод, відбиття, рефракції й розсіювання сигналу. Тому ефективне застосування *IDS* у бездротових мережах можливо тільки після тривалого періоду детального дослідження мережі. При розгортанні системи необхідно чітко розуміти, що, як і навіщо ми прагнемо аналізувати, і постаратися відповісти на ці питання, щоб сконструювати потрібну нам систему *IDS* (рис. 10.2).

Рисунок 10.2 – Характеристики систем виявлення вторгнень

Тільки зібравши значний обсяг статистичних даних про роботу конкретної мережі, можна розв’язати, що є аномальною поведінкою, а що – ні, і ідентифікувати проблеми зі зв’язком, помилки користувачів і атаки. Багаторазові запити на автентифікацію по протоколу 802.1x/*LEAP* можуть свідчити про спробу атаки методом повного перебору. Але це може пояснюватися й тим, що *користувач* забув свій *пароль*, або роботою погано написаного клієнтського додатка, який продовжує вживати спроби ввійти в *мережу*, поки не буде введений правильний *пароль*. Збільшення числа фреймів-маяків може бути ознакою Dos-*Атаки* або присутності в мережі

фальшивої точка доступу, але не виключене, що вся справа в несправній або неправильно сконфігурованійточці доступу.

Події, зафіксовані *IDS* на верхніх рівнях стека протоколів, наприклад велике число фрагментовних пакетів або запитів *TCP SYN*, може вказувати на сканування портів або Dos-Атаку, але, можливо, це просто результат поганого зв'язку на фізичному рівні (рівень 1).

1. Події на фізичному рівні:
   - наявність додаткових передавачів у зоні дії мережі;
   - використання каналів, які не повинні бути задіяні в мережі, що захищається;
   - канали, що перекриваються;
   - раптова зміна робочого каналу одним або декількома пристроями, за якими ведеться спостереження;
   - погіршення якості сигналу, високий рівень шуму або низьке *значення відносини* «сигнал-шум».

Ці події можуть свідчити про наявність проблем зі зв'язком або з мережею, про помилки, допущені при конфігуруванні мережі, про появу шахрайських пристроїв, про навмисне глушіння або про атаки «людей посередині» на рівень 1 або 2.

2. Події, пов'язані з адміністративними або керуючими фреймами:
   - підвищена частота появи деяких типів фреймів;
   - фрейми незвичайного розміру;
   - фрейми невідомих типів;
   - неповні, зіпсовані або неправильно сформовані фрейми;
   - потік фреймів із запитами на від'єднання й припинення сеансу;
   - часта поява фреймів із запитом на повторне приєднання в мережах, де не включений роумінг;
   - фрейми з неправильними порядковими номерами;
   - часта поява пробних фреймів;
   - фрейми, у яких *SSID* відрізняється від *SSID* даної мережі;
   - фрейми із широкомовним *SSID*;
   - фрейми із часто мінливими або випадковими *SSID*;

– фрейми зі значеннями в поле *SSID* або інших полях, типовими для деяких інструментів вторгнення;

– фрейми з MAC-Адресами, відсутніми в списку контролю доступу;

– фрейми з, що дублюються MAC -Адресами;

– фрейми із часто мінливими або випадковими MAC-Адресами.

Ці події можуть указувати на неправильну конфігурацію мережі, проблеми зі зв'язком, сильні перешкоди, спроби застосування інструментів активного сканування мережі, підробку MAC-Адрес, присутність у мережі сторонніх клієнтів, спроби вгадати або підібрати методом повного перебору закритий *SSID* або на більш витончені атаки «людей посередині» на рівень 2, пов'язані з маніпуляцією керуючими або адміністративними фреймами.

3. Події, пов'язані із фреймами протоколів 802.1x/EAP:

– неповні, зіпсовані або неправильно сформовані фрейми протоколу 802.1x;

– фрейми з такими типами протоколу EAP, які не реалізовані в даній бездротовій мережі;

– багаторазові фрейми запиту й відповіді процедури автентифікації EAP;

– багаторазові фрейми з повідомленням про невдалу автентифікації EAP;

– затоплення фреймами початку й завершення сеансу EAP;

– фрейми EAP аномального розміру;

– фрейми EAP з некоректним значенням довжини;

– фрейми EAP з неправильними «вірчими грамотами»;

– фрейми EAP, що приходять від невідомих *автентифікаторів* (фальшива точка доступу);

– незавершена процедура автентифікації по протоколу 802.1x/EAP.

Ці події можуть указувати на спроби прорватися через процедуру автентифікації, описану в протоколі 802.1x, у тому числі й шляхом розміщення фальшивого пристрою й

проникнення в мережу за допомогою атаки методом повного перебору або проведення витонченої Dos-*Атаки*, спрямованої на вивід з ладу механізмів автентифікації. Зрозуміло, неправильно сформовані фрейми можуть виникати й у результаті сильних радіоперешкод або інших проблем на рівні 1.

4. Події, пов'язані із протоколом *WEP*:
   - наявність незашифрованого бездротового трафіка;
   - наявність трафіка, зашифрованої невідомими Wep-*Ключами*;
   - наявність трафіка, зашифрованої Wep-*Ключами* різної довжини;
   - фрейми зі слабкими IV;
   - фрейми, що йдуть підряд, з повторюваними IV;
   - не мінливі IV;
   - відкіт до *WEP* від більш безпечного протоколу, наприклад *TKIP*;
   - помилки при ротації Wep-*Ключів*.

Ці події можуть указувати на серйозні помилки при конфігуруванні мережі, на застосування небезпечного застарілого обладнання або на використання інструментів впровадження трафіка досвідченим зломщиком.

5. Події, пов'язані із загальними проблемами зв'язки:
   - втрата зв'язку;
   - раптовий сплеск навантаження на мережу;
   - раптове зменшення пропускної здатності мережі;
   - раптове збільшення затримок у двухточковому каналі;
   - підвищений рівень фрагментації пакетів;
   - часті повторні передачі.

Ці події заслуговують більш пильного вивчення для виявлення дійсної причини помилок. Механізм побудови виводів, вбудований в IDS, повинен уміти зв'язувати події з різними можливими причинами, тим самим спрощуючи розслідування.

6. Інші події:
   - що приєдналися, але не автентифіковані хости;

– атаки на верхні рівні стека протоколів, що викликають спрацьовування «традиційної» IDS;

– сторонній адміністративний трафік, адресований крапці доступу;

– постійне дублювання або повтор пакетів з даними;

– пакети з даними, у яких зіпсовані контрольні суми або MIC, формовані на канальному рівні;

– затоплення багаторазовими спробами одночасного приєднання до мережі.

Ці події можуть свідчити про успішну або невдалій атаці, про наявність хоста з неправильними настроюваннями безпеки, про спроби одержати контроль над точкою доступу й змінити її конфігурацію, про застосування інструментів для впровадження трафіка, про Dos-Атаці проти хостів із включеним протоколом 802.11i або про спроби переповнити буфер точки доступу більшим числом запитів на з'єднання з боку провідної або бездротової частини мережі. Але, як і раніше, викривлення фрейму або пакета може бути обумовлене проблемами на фізичному рівні, наприклад наявністю перешкод або слабким рівнем сигналу.

З комерційних рішень добре відомі програми Airdefense *Guard* і Isomair *Wireless* Sentry. Вони засновані на розміщенні сенсорів на території.

11. АНТЕНИ

Антену можна визначити як провідник, використовуваний для випромінювання або вловлювання електромагнітної енергії із простору. Для передачі сигналу радіочастотні електричні імпульси передавача за допомогою антени перетворяться в електромагнітну енергію, яка випромінюється в навколишній простір. При одержанні сигналу енергія електромагнітних хвиль, що надходять на антену, перетвориться в радіочастотні електричні імпульси, після чого подається на приймач.

Як правило, при двосторонньому зв'язку та сама антена використовується як для приймання, так і для передачі сигналу. Такий підхід можливий, тому що будь-яка антена з рівною ефективністю поставляє енергію з навколишнього середовища до терміналів, що ухвалюють, і від передавальних терміналів у навколишнє середовище.

Для правильного настроювання антен розберемо деякі її характеристики.

11.1. Діаграма спрямованості

Антени випромінюють енергію у всіх напрямках. Однак у більшості випадків ефективність передачі сигналу для різних напрямків неоднакова. Найпоширенішим способом визначення ефективності антени є *діаграма спрямованості*, яка являє собою залежність випромінюючих властивостей антени від просторових координат. Діаграми *спрямованості антен* представляються як двомірний поперечний переріз тривимірної діаграми.

Один з найбільш простих типів діаграми спрямованості відповідає ідеальному випадку так званої ізотропної антени. Під ізотропною антеною розуміють крапку в просторі, яка випромінює енергію однаково у всіх напрямках. Діаграма спрямованості для ізотропної антени являє собою сферу, центр якої збігається з положенням антени (рис. 11.1а). Відстань від антени до будь-якої точка діаграми спрямованості прямо пропорційно енергії, яка була випроменена антеною в даному

напрямку. На рис. 11.1б представлений ще один ідеалізований випадок – спрямована антена з одним виділеним напрямком випромінювання (уздовж горизонтальної осі).

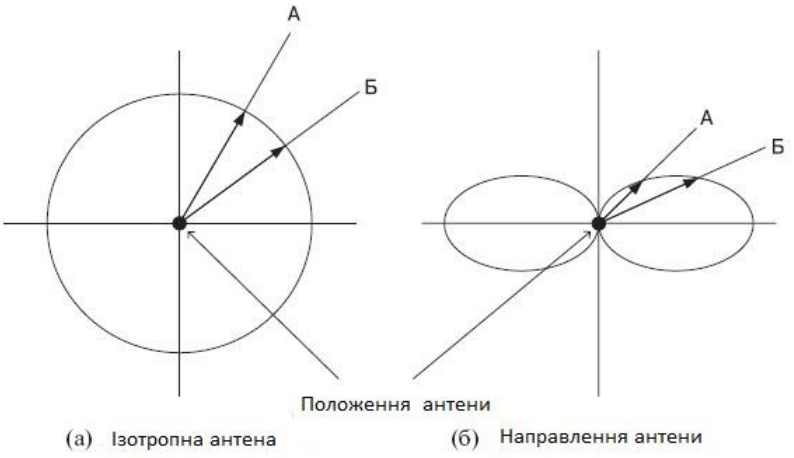


Рисунок 11.1 – Діаграми спрямованості

Розмір діаграми спрямованості може бути довільним. Важливо лише, щоб у кожному напрямку були дотримані пропорції. Щоб на основі відносної відстані визначити наведену потужність у заданому напрямку, від точка розміщення антени до перетинання з діаграмою спрямованості проводять пряму лінію під відповідним кутом нахилу. На рис. 12.1бдля двох антен рівняються два кути передачі сигналу (А и Б). Ізотропній антені відповідає ненаправлена кругова діаграма; вектори А и Б рівні по величині.

11.2. Поляризація антена

Важливою характеристикою антени є її *поляризація*. У системах радіодоступу використовують антени з вертикальної, горизонтальної й круговий (із правим і *лівим обертанням*) поляризаціями (рис. 11.2).

Облік поляризації дозволяє одержати додаткові енергетичні переваги при розв'язку завдань електромагнітної сумісності, плануванні зон обслуговування і т.д. При заповненні певного простору точками доступу до граничного рівня, після якого взаємні радіоперешкоди починають заважати нормальній роботі мереж, досить змінити поляризацію антен, після чого можна продовжувати нарощувати *радіомережу*.

У плоскій електромагнітній хвилі вектори вертикального електричного Е і магнітного Н полів у кожний момент часу орієнтовані в просторі певним чином. Поляризація електромагнітної хвилі є її часовою-просторово-тимчасовою характеристикою й визначається видом траєкторії, описуваної кінцем вектора електричного поля у фіксованій крапці простору. На антенах з поляризацією на задній стороні є покажчик у вигляді стрілки, який і визначає необхідну поляризацію.

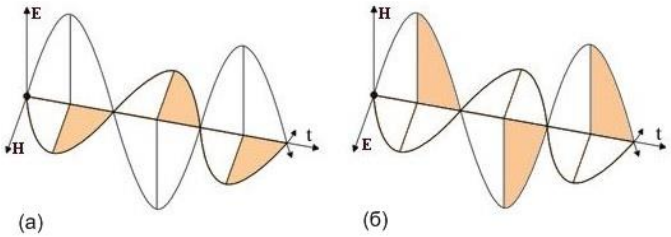


Рисунок 11.2 – Вертикальна (а) і горизонтальна (б) поляризації

При круговій або циклічній поляризації електромагнітне поле обертається навколо осі Х з певним циклом, або кроком, так, що в різних точках простору ухвалює або вертикальну, або горизонтальну поляризацію. Такий вид поляризації застосовується порівняно рідко.

11.3. Коефіцієнти підсилення антен

Коефіцієнт підсилення оцінкою спрямованості антени. Даний параметр визначається як відношення потужності сигналу, випроміненого в певному напрямку, до потужності сигналу,

випромінюваного ідеальної *ненаправленою антеною* в будь-якому напрямку.

Коефіцієнт підсилення антени стосовно дипольної антени звичайно дається в дБ(∂В), а стосовно ізотропної – в дБи(∂Вi).

Уперше використана для вимірів інтенсивності сигналу одиниця виміру децибел була названа так на честь Олександра Грэма Бэлла. Значення в децибелах обчислюються по логарифмічній шкалі, що дозволяє забезпечити специфікацію характеристик у широкому діапазоні напруг або потужностей.

$$\text{Б} = \text{Бел} = log_{10}\left(\frac{P_1}{P_2}\right) = 2 \cdot log_{10}\left(\frac{V_1}{V_2}\right)$$

$$\text{дБ} = \text{децибел} = 10 \cdot log_{10}\left(\frac{P_1}{P_2}\right) = 20 \cdot log_{10}\left(\frac{V_1}{V_2}\right)$$

де P_1 – обмірювана потужність (*Вт*);

P_2 – еталонна потужність (*Вт*);

V_1 – обмірювана напруга (*В*);

V_2 – еталонна напруга (*В*).

Приклад 11.1

Якщо на вході лінії передачі рівень потужності сигналу становить *100 мВт*, а на деякій відстані *50 мВт*, то ослаблення сигналу можна виразити в такий спосіб:

$$L_{\text{дБ}} = 10 \log \frac{100}{50} = 3\text{дБ}$$

У децибелах виражається відносне, а не абсолютна відмінність сигналів. Ослаблення сигналу з *10 Вт* на *5 Вт* також є ослабленням на *3 дБ*.

Приклад 11.2

Використання децибелів корисно при визначенні посилення або зниження потужності, що відбувається на послідовності передавальних елементів. Розглянемо, наприклад, послідовність елементів, на вхід якої подається потужність *4 мВт*, перший елемент є кабельним складанням із загасанням *12 дБ*, другий елемент - це підсилювач із посиленням *35 дБ*, а третій – ще одне

кабельне складання із загасанням *10 дБ*. Сумарне посилення тракту дорівнює:

(-12 + 35 - 10) = *13 дБ*. Обчислюємо потужність на виході:

$$G_{\text{дБ}} = 13 = 10\log\frac{\text{P}_{\text{вих}}}{4}$$

$$\text{P}_{\text{вих}} = 4 \times 10^{1,3} = 79{,}8\ \text{мВт}$$

Значення в децибелах пов'язані з відносними амплітудами або змінами амплітуд, але ніяк не з абсолютними рівнями. Було б зручно представити абсолютний рівень потужності також у децибелах, щоб можна було легко обчислювати посилення або зниження потужності стосовно вихідного сигналу. Тому в якості еталонного рівня обрана величина 1 Вт, а абсолютний рівень потужності – в дБВт або *дВW* (ват^-ватів-ват-децибел-ват). Він визначається в такий спосіб:

$$\text{Потужність, дБ} \cdot \text{Вт} = 10\log\frac{\text{Потужність,мВт}}{1\text{Вт}}.$$

Широко використовується й інша похідна

одиниця – $\text{дБ} \cdot \text{Вт} \cdot (\partial\text{Вт})$ (децибел-міліват). У цьому випадку за еталонний рівень потужності ухвалюється *1 мВт*.

$$\text{Потужність, дБ} \cdot \text{Вт} = 10\log\frac{\text{Потужність,мВт}}{1\text{Вт}}.$$

Збільшення потужності сигналу в одному напрямку можливо лише за рахунок інших напрямків поширення. Інакше кажучи, збільшення потужності сигналу в одному напрямку спричиняє зменшення потужності в інших напрямках. Необхідно відзначити, що коефіцієнт підсилення характеризує спрямованість сигналу, а не збільшення вихідної потужності стосовно вхідної (як може здатися з назви), тому даний параметр часто ще називають коефіцієнтом спрямованого дії.

11.4. Поширення сигналу

При поширенні сигнал, випроменений антеною, може обгинати поверхня Землі, відбиватися від верхніх шарів атмосфери або поширюватися уздовж лінії прямої видимості.

11.4.1. Дифракція електромагнітних хвиль

При обгинанні поверхні Землі (рис. 11.3) шлях поширення сигналу тією чи іншою мірою повторює контур планети. Передача може проводитися на значні відстані, що набагато перевищують межі прямої видимості. Даний ефект має місце для частот до 2 Мгц. На здатність сигналів, що належать даній смузі частот, повторювати кривизну земної поверхні впливає фактор *дифракції електромагнітних хвиль*. Дане явище пов'язане з поведінкою електромагнітних хвиль при наявності перешкод.

Рисунок 11.3 – Поширення навколоземних хвиль (частота до 2 МГц)

Рисунок 11.4 – По ширення сигналу уздовж лінії видимості (частота понад 30 МГц)

Розсіювання електромагнітних хвиль зазначеного діапазону в атмосфері відбувається таким чином, що у верхні атмосферні шари ці хвилі не попадають.

Якщо частота радіосигналу перевищує 30 МГц, то обгинання їм земної поверхні й відбиття від верхніх шарів атмосфери стають неможливими. У цьому випадку зв'язок повинна здійснюватися в межах прямої видимості (рис. 11.4).

При зв'язку через супутник сигнал із частотою понад 30 Мгц не буде відбиватися іоносферою. Такий сигнал може передаватися від наземної станції до супутника й назад за умови, що супутник не перебуває за межами обрію. При наземному зв'язку передавальна, що й ухвалює антени повинні перебувати в межах ефективної лінії прямої видимості. Використання терміна "ефективний" пов'язане з тим, що хвилі надвисокої частоти викривляються й переломлюються атмосферою. Ступінь і напрямок скривлення залежать від різних факторів. Однак, як правило, скривлення надвисокочастотних хвиль повторюють кривизну поверхні Землі. Тому такі хвилі поширюються на відстань, що перевищує оптичну лінію прямої видимості. Тому що зв'язок між точками доступу, що працюють у стандартах 802.11a, 802.11b і 802.11g звичайно розраховується на лінію прямої видимості, то в наступній главі розглянемо, як впливає навколишнє середовище на корисний сигнал.

11.4.2. Передача сигналу в межах лінії прямої видимості

Для будь-якої системи зв'язку слушне твердження, що прийнятий сигнал відрізняється від переданого. Даний ефект є наслідком різних викривлень у процесі передачі. При передачі аналогового сигналу викривлення приводять до його випадкової зміни, що проявляється в погіршенні якості зв'язки. Якщо ж передаються цифрові дані, викривлення приводять до появи двійкових помилок – двійкова *одиниця* може перетворитися в нуль і навпаки. Розглянемо різні типи викривлень, а також їх вплив на пропускну здатність каналів зв'язки в межах *прямої* видимості. Найбільш важливими є наступні типи викривлень:

– загасання або амплітудне викривлення сигналу;

– втрати у вільному просторі;
– шум;
– атмосферне поглинання.

11.4.3. Загасання

При передачі сигналу в будь-якому середовищі його інтенсивність зменшується з відстанню. Таке ослаблення, або *загасання*, у загальному випадку логарифмічно залежить від відстані. Як правило, загасання можна виразити як постійну втрату інтенсивності (у децибелах) на одиницю довжини. При розгляді загасання важливі три фактори.

1. Отриманий сигнал повинен мати потужність, достатню для його виявлення й інтерпретації приймачем.

2. Щоб при одержанні були відсутні помилки, потужність сигналу повинна підтримуватися на рівні, у достатній мері перевищуючому шум.

3. При підвищенні частоти сигналу загасання зростає, що приводить до викривлення.

Перші два фактори пов'язані із загасанням інтенсивності сигналу й використанням підсилювачів або ретрансляторів. Для двухточкового каналу зв'язку потужність сигналу передавача повинна бути достатньої для чіткого приймання. У той же час інтенсивність сигналу не повинна бути занадто великий, тому що в цьому випадку контури передавача або приймача можуть виявитися перевантаженими, що також приведе до викривлення сигналу. Якщо відстань між приймачем і передавачем перевищує певну постійну, понад якої загасання стає неприйнятно високим, для посилення сигналу в заданих точках простору розташовуються ретранслятори або підсилювачі. Завдання посилення сигналу значно ускладнюється, якщо існує безліч приймачів, особливо якщо відстань між ними й передавальною станцією мінливо.

Третій фактор списку відомий як амплітудне викривлення. Внаслідок того, що загасання є функцією частоти, отриманий сигнал спотворюється в порівнянні з переданим, що знижує чіткість приймання. Для усунення цієї проблеми використовуються методи вирівнювання викривлення в певній

смузі частот. Одним з можливих підходів може бути використання пристроїв, що підсилюють високі частоти в більшій мері, чому низькі.

11.4.4. Втрати у вільному просторі

Для будь-якого типу бездротового зв'язку переданий сигнал розсіюється в міру його поширення в просторі. Отже, потужність сигналу, прийнятого антеною, буде зменшуватися в міру видалення від передавальної антени. Для супутникового зв'язку згаданий ефект є основною причиною зниження інтенсивності сигналу. Навіть якщо припустити, що всі інші причини загасання й ослаблення відсутні, переданий сигнал буде загасати в міру поширення в просторі. Причина цього – поширення сигналу по все більшій площі. Даний тип загасання називають *втратами у вільному просторі* й обчислюють через відношення потужності випромененого сигналу до потужності отриманого сигналу. Для обчислення того ж значення в децибелах слід побрати десятковий логарифм від зазначеного відношення, після чого помножити отриманий результат на 10.

$$\frac{P_t}{P_r} = \frac{(4\pi)^2 d^2}{G_r G_t \lambda^2}$$

де P_t – потужність сигналу передавальної антени;

P_r – потужність сигналу, що надходить на антену приймача;

λ – довжина хвилі несучої;

d – відстань, пройдене сигналом між двома антенами;

G_t – коефіцієнт підсилення передавальної антени;

G_r – коефіцієнт підсилення антени приймача.

Отже, якщо довжина хвилі несучої і їх рознесення в просторі залишаються незмінними, збільшення коефіцієнтів підсилення передавальної й приймальні антен приводить до зменшення втрат у вільному просторі.

11.4.5. Шуми

Для будь-якої передачі даних слушне твердження, що отриманий сигнал складається з переданого сигналу,

модифікованого різними викривленнями, які вносяться самою системою передачі, а також з додаткових небажаних сигналів, взаємодіючих з вихідною хвилею під час її поширення від точка передачі до точка приймання. Ці небажані сигнали прийнято називати *шумом*. Шум є основним чинником, що обмежують продуктивність систем зв'язки.

Шуми можна розділити на чотири категорії:

- тепловий шум;
- інтермодуляційні шуми;
- перехресні перешкоди;
- імпульсні перешкоди.

Тепловий шум є результатом теплового руху електронів. Даний тип перешкод впливає на всі електричні прилади, а також на середовище передачі електромагнітних сигналів.

Якщо сигнали різної частоти передаються в одному середовищі, може мати місце інтермодуляційний шум. Інтермодуляційним шумом є перешкоди, що виникають на частотах, які являють собою суму, різницю або добуток частот двох вихідних сигналів. Наприклад, змішування двох сигналів, переданих на частотах f_1 і f_2 відповідно, може привести до передачі енергії на частоті $f_1 + f_2$. При цьому даний паразитний сигнал може интерферировать із сигналом зв'язку, переданим на частоті $f_1 + f_2$.

З *перехресними перешкодами* зустрічався кожний, хто під час використання телефону змінно чула розмова сторонніх людей. Даний тип перешкод виникає внаслідок небажаного об'єднання трактів передачі сигналів. Таке об'єднання може бути викликане зчепленням близько розташованих кручених пар, по яких передаються множинні сигнали. Перехресні перешкоди можуть виникати під час приймання сторонніх сигналів антенами. Незважаючи на те, що для зазначеного типу зв'язку використовують високоточні спрямовані антени, втрат потужності сигналу під час поширення уникнути все-таки неможливо. Як правило, потужність перехресних перешкод рівна один по одному (або нижче) потужності теплового шуму. Усі зазначені вище типи перешкод є передбачуваними й характеризуються відносно постійним рівнем потужності. Таким

чином, цілком можливо спроектувати систему передачі сигналу, яка була б стійкої до зазначених перешкод.

Однак крім перерахованих вище типів перешкод існують так звані *імпульсні перешкоди*, які по своїй природі є переривчастими й складаються з нерегулярних імпульсів або короткочасних шумових пакетів з відносно високою амплітудою. Причин виникнення імпульсних перешкод може бути безліч, у тому числі зовнішні електромагнітні впливи (наприклад, блискавки) або дефекти (поломки) самої системи зв'язки.

11.4.6. Атмосферне поглинання

Причиною додаткових втрат потужності сигналу між передавальної, що й ухвалює антенами є атмосферне поглинання, при цьому основний внесок в ослаблення сигналу вносять водні пари й кисень. Дощ і туман (краплі води, що перебувають у зваженому стані в повітрі) приводять до розсіювання радіохвиль і в остаточному підсумку до ослаблення сигналу. Зазначені фактори можуть бути основною причиною втрат потужності сигналу. Отже, в областях, для яких характерно значне випадання опадів, необхідно або скорочувати відстань між приймачем і передавачем, або використовувати для зв'язку більш низькі частоти.

12. ВІДНОШЕННЯ «СИГНАЛ-ШУМ» У ЦИФРОВИХ СИСТЕМАХ ЗВ'ЯЗКУ

12.1. Побудова антенно-фідерних трактів

Дуже важливою характеристикою продуктивності цифрових систем зв'язки є *відношення* «сигнал-шум».

Відношення «сигнал-шум» – це *відношення* енергії сигналу на 1 *біт* до щільності потужності шумів на 1 герц (E_b/N_0). Розглянемо сигнал, що містить двійкові цифрові дані, передані з певною швидкістю – *R біт*/с. Нагадаємо, що 1 Вт = 1 Дж/з, і обчислимо питому енергію одного біта сигналу: $E_b = St_b$ (де S – *потужність* сигналу; T_b – час передачі одного біта). *Швидкість передачі* даних *R* можна виразити у вигляді $R=1/T_b$. Враховуючи, що тепловий шум, який присутній у смузі шириною 1 Гц, для будь-якого пристрою або провідника становить

$$N_0=kT \text{ (Вт/Гц)} \qquad (12.1)$$

де N_0 – щільність потужності шумів у ватах на 1 Гц смуги;

k – постійна Больцмана, k=1.3803 x 10^{-23} Дж/К;

Т – температура в Кельвінах (абсолютна температура), то, отже,

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR} \qquad (12.2)$$

Відношення E_b/N_0 має велике практичне *значення*, оскільки швидкість появи помилкових бітів є (убутної) функцією даного відношення. При відомому значенні E_b/N_0, необхідному для одержання бажаного рівня помилок, можна вибирати всі інші параметри в наведеному рівнянні. Слід зазначити, що для збереження необхідного значення E_b/N_0 при підвищенні швидкості передачі даних R прийде збільшувати *потужність* переданого сигналу стосовно шуму.

Досить часто рівень потужності шуму достатній для зміни значення одного з бітів даних. Якщо ж побільшати *швидкість*

передачі даних удвічі, біти будуть «упаковані» у два рази щільніше, і той же сторонній сигнал приведе до втрати двох бітів інформації. Отже, при незмінній потужності сигналу й шуму збільшення швидкості передачі даних спричиняє зростання рівня виникнення помилок.

Приклад 12.1

Розглянемо метод кодування сигналу, для якого необхідно, щоб відношення E_b/N_0 рівнялося *8,4 дБ* при частоті виникнення помилок 10-4 (помилковим є 1 біт з кожних 10000). Якщо ефективна температура теплового шуму рівна *290 ДО*, а швидкість передачі даних – 1 Мбіт/с, який повинна бути потужність сигналу, щоб подолати тепловий шум?

Розв'язок:

По формулі (12.2) знаходимо S:

$$S = \frac{E_b}{N_0} kTR$$

Для спрощення розрахунків переведемо це вираження в логарифми:

$$S_{\text{дБВт}} = 10log_{10}\left(\frac{E_b}{N_0} kTR\right) = \left(\frac{E_b}{N_0}\right)_{\text{дБ}} + 10log_{10}(kTR)$$

Тому що 1 Мбіт = 1048576 біт, те

$$S_{\text{дБВт}} = 8.4 + 10\log_{10}(1.38 \cdot 10^{-23} \cdot 290 \cdot 1048576) = -135.37$$

або

$$S = 10^{\frac{\text{S}_{\text{дБВт}}}{10}} = 2.904 \cdot 10^{-14}\text{Вт}$$

Отже, для того щоб подолати тепловий шум, необхідна потужність *35,37 дБВт*.

12.2. Розрахунки зони дії сигналу

12.2.1. Розрахунки дальності роботи бездротового каналу зв'язки

Без виводу приведемо формулу розрахунків дальності. Вона береться з інженерної формули розрахунків втрат у вільному просторі:

$$FSL = 33 + 20(\lg F + \lg D)$$

FSL (*Free Space Loss*) – втрати у вільному просторі (*дБ*);

F – центральна частота каналу, на якому працює система зв'язку (*МГц*);

D – відстань між двома точками (*км*).

FSL визначається сумарним посиленням системи. Воно вважається в такий спосіб:

$$Y_{\text{дБ}} = P_{t,\text{дБмВТ}} + G_{t,\text{дБи}} + G_{r,\text{дБи}} - P_{min.\text{дБмВТ}} - L_{t,\text{дБ}} - L_{r,\text{дБ}}$$

де $P_{t,\text{дБмВТ}}$ – потужність передавача;

$G_{t,\text{дБи}}$ – коефіцієнт підсилення передавальної антени;

$G_{r,\text{дБи}}$ – коефіцієнт підсилення приймальної антени;

$P_{min.\text{дБмВТ}}$ – чутливість приймача на даній швидкості;

$L_{t,\text{дБ}}$ – втрати сигналу в коаксіальному кабелі й роз'ємах передавального тракту;

$L_{r,\text{дБ}}$ – втрати сигналу в коаксіальному кабелі й роз'ємах приймального тракту.

Таблиця 12.1 – Залежність чутливості від швидкості передачі даних

Швидкість	**Чутливість**
54 Мбіт/с	-66 дБмВт
48 Мбіт/с	-71 дБмВт
36 Мбіт/с	-76 дБмВт
24 Мбіт/с	-80 дБмВт
18 Мбіт/с	-83 дБмВт
12 Мбіт/с	-85 дБмВт
9 Мбіт/с	-86 дБмВт
6 Мбіт/с	-87 дБмВт

Для кожної швидкості приймач має певну чутливість. Для невеликих швидкостей (наприклад, 1-2 Мегабіта) чутливість найменша: від – *90 дБмВт* до – *94 дБмВт*. Для високих швидкостей чутливість набагато вище. Як приклад у таблиці 12.1 наведено кілька характеристик звичайних крапок доступу *802.11a*,b,g.

Залежно від марки радіомодуля максимальна чутливість може небагато варіюватися. Ясно, що для різних швидкостей максимальна дальність буде різною.

FSL обчислюється по формулі

$$FSL = Y_{\text{дБ}} - SOM \qquad (12.4)$$

де *SOM*(*System Operating* Margin) – запас в енергетику радіозв'язку (дБ). Ураховує можливі фактори, що негативно впливають на дальність зв'язки, такі як:

- температурний дрейф чутливості приймача й вихідної потужності передавача;
- усілякі атмосферні явища: туман, сніг, дощ;
- неузгодженість антени, приймача, передавача з антенно-фідерним трактом.

Параметр *SOM* звичайно береться рівним *10 дБ*. Уважається, що *10*-децибельний запас по посиленню достатній для інженерного розрахунків.

Центральна частота F каналу береться з таблиці 12.2.

У підсумку одержимо формулу дальності зв'язки:

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - \lg F\right)} \qquad (12.5)$$

Таблиця 12.2 – Обчислення центральної частоти

Канал	Центральна частота (МГц)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Приклад 12.2

Знайти відстань, на якому буде стабільно працювати зв'язок на швидкостях 54 Мбіт/с і 6 Мбит/із для точка доступу DWL-2100AP і бездротового адаптера DWL-G132. Їхні паспортні характеристики:

Потужність передавачів DWL-2100AP і DWL-G132: 16 дбмвт;

Чутливість DWL-2100AP на швидкості 54 Мбіт/с: -66 дбмвт;

Чутливість DWL-2100AP на швидкості 6 Мбіт/с: -88 дбмвт;

Чутливість DWL-G132 на швидкості 54 Мбіт/с: -66 дбмвт;

Чутливість DWL-G132 на швидкості 6 Мбіт/с: -87 дбмвт;

Коефіцієнт підсилення штатної антени DWL-2100AP: 2 дби.

Коефіцієнт підсилення штатної антени DWL-G132: 0 дби.

Втрат в антенно-фідерному тракті, тобто між бездротовими точками і їх антенами, немає.

Розв'язок:

1) Знайдемо відстань на швидкості 54 Мбит/с. Параметр FSL рівний

$$FSL = 16 + 2 - (-66) - 10 = 74\text{дБ}$$

По формулі (12.5) знаходимо дальність роботи бездротового встаткування на даній швидкості (як приклад поберемо шостий канал):

$$D = 10^{\left(\frac{74}{20} - \frac{33}{20} - \lg 2437\right)} = 0{,}049\text{км} \approx 50\text{м}$$

Знайдемо відстань на швидкості 6 Мбит/с. FSL рівний

$$FSL = 16 + 2 - (-88) - 10 = 96\text{дБ}$$

По формулі (12.5) знаходимо дальність роботи бездротового встаткування на даній швидкості:

$$D = 10^{\left(\frac{96}{20} - \frac{33}{20} - \lg 2437\right)} = 0{,}579\text{км} \approx 580\text{м}$$

12.2.2. Розрахунки зони Френеля

Радіохвиля в процесі поширення в просторі займає простір у вигляді еліпсоїда обертання з максимальним радіусом у середині прольоту, який називають зоною Френеля (рис. 12.1). Природні (земля, пагорби, дерева) і штучні (будинки, стовпи) перешкоди, що попадають у цей простір, послабляють сигнал.

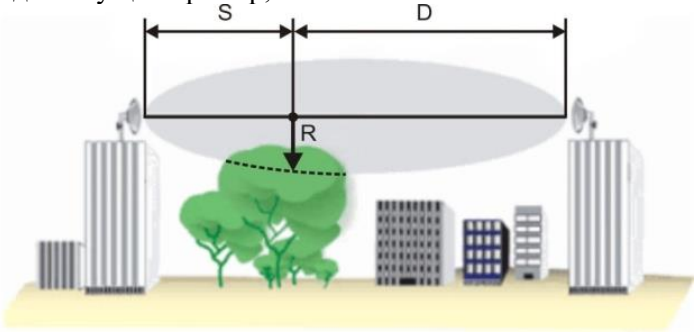


Рисунок 12.1 – Зона Френеля

Радіус першої зони Френеля над передбачуваною перешкодою може бути розрахований за допомогою формули

$$R = 17.3\sqrt{\frac{1}{f} \cdot \frac{S \cdot D}{S + D}}\ , \qquad (12.6)$$

де R – радіус зони Френеля (м);

S, D – відстань від антен до самої вищої точка передбачуваного перешкоди (км);

f – частота (ГГц).

Зауваження:

– Звичайне блокування 20% зони Френеля вносить незначне загасання в канал. При блокуванні понад 40% *загасання сигналу* буде вже значним, слід уникати влучення перешкод на шляху поширення.

– Цей розрахунки зроблений у припущенні, що земля плоска. Він не враховує кривизну земної поверхні. Для протяжних каналів слід проводити сукупний розрахунки, що враховує рельєф місцевості й природні перешкоди на шляху поширення. У випадку більших відстаней між антенами слід намагатися збільшувати висоту підвісу антен, беручи до уваги кривизну земної поверхні.

Приклад 12.1

Нехай відстань між антенами рівно 10 км (рис. 12.5), передбачувана перешкода від правої антени перебуває на відстані 7 км і бездротове встаткування працює на шостому каналі.

Розв'язок:

Підставивши дані S, D і частоту каналу з таблиці 12.2 у формулу (12.6), одержимо:

$$R = 17.3\sqrt{\frac{1}{2.4373}\cdot\frac{3\cdot 7}{3+7}} = 16.06\text{м}$$

Отже, щоб *загасання сигналу* було мінімальним, необхідно, щоб перешкода не заходила в зону Френеля з радіусом *16 м*.

12.2.3. Побудова антенно-фідерних трактів із зовнішніми антенами

Завдання по підключенню до бездротового встаткування додаткових антен, посиленню потужності передавача, включенню в систему додаткових фільтрів досить часто зустрічаються в практиці побудови бездротових мереж. І, як правило, на цю тему виникає багато питань, найпоширенішими з

яких є питання про відповідність розємів на використовуваному встаткуванні й додаткових кабелях, а також питання з розрахунку отриманих систем.

Відразу необхідно відзначити, що винос антени – справа невдячна, тому що виникаючі при цьому негативні фактори, такі як *загасання сигналу* на кабельних складаннях і збільшення рівня паразитних шумів, значно погіршують характеристики вихідної радіосистеми. Разом з тим підключені антени (особливо з більшими коефіцієнтами підсилення) багато в чому компенсують усі ці негативні фактори, але, незважаючи на це, при проектуванні все-таки намагаються максимально скоротити відстань від порту активного встаткування крапок доступу до винесеної антени й по можливості підключити антену прямо до точка доступу.

Дуже часто бувають випадки, коли необхідно побільшати зону охвату усередині приміщень, для цього використовують антени у внутрішньому (*indoor*) виконанні. Для зв'язку між будинками або районами використовують більш дороге встаткування в зовнішньому (*outdoor*) виконанні.

12.2.4. Антенно-фідерний тракт із підсилювачем

На рис. 12.6 показана бездротова система з антенно-фідерним трактом, у який включена безліч елементів. Їх може бути значно більше, але тут показані найбільше часто використовувані. Далі пояснимо, для чого використовується той або інший елемент, як він називається, і які нюанси необхідно врахувати при його використанні.

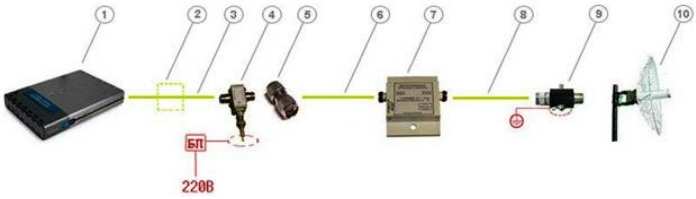


Рис. 12.6 – Антенно-фідерний тракт із підсилювачем

1. Точка доступу зі знімною антеною

Майже все бездротове встаткування D-Link комплектується знімними штатними антенами 2-5 Дбі (наприклад, DWL-2100AP, DWL-3200AP, DWL-8200AP, DWL-2700AP, DWL-7700AP, DWL-G520 і т.д.) - це означає, що штатну антену можна легко зняти й підключити замість неї могутнішу антену з необхідним коефіцієнтом підсилення й діаграмою спрямованості. У технічних характеристиках бездротового встаткування завжди сказане, яким типом антен воно комплектується за замовчуванням.

Крім підтримуваних технологій і швидкісних характеристик точка доступу має кілька важливих фізичних характеристик, які є вихідними даними для розрахунків антенно-фідерного тракту й енергетичних характеристик системи. До таких характеристик ставляться:

– потужність передавача, яка виміряється або в міліватах (*мВт*) або в децибел-міліватах (*дБмВт*).

– чутливість приймача для певної швидкості – чому вона вище, тем вище швидкість.

2. Смуговий фільтр

Він показаний пунктиром, оскільки його досить рідко включають у систему, але проте він присутній у системах професійного рівня. Прийнято думати, що кабель вносить тільки втрати, пов’язані з довжиною кабелю, і досить вибрати кабель із малим загасанням або поставити підсилювач, і всі проблеми будуть вирішені. Однак це не зовсім так. У першу чергу, довгий кабель збирає перешкоди у всьому діапазоні частот, тому роботі будуть заважати всі радіопристрої, здатні створити на вході приймача карти досить сильну перешкоду. Тому часто трапляється, що в міському середовищі, у якому є присутнім сильне зашумлення, зв’язок між точками доступу в системах з винесеної на велику відстань антеною вкрай нестабільна, і тому в кабель необхідно включати додатковий смуговий фільтр безпосередньо перед вхідним розніманням точка доступу, який внесе ще втрати не менш *1,5 дБ.*

Смугові фільтри бувають, що настроюються й з фіксованою центральною частотою, яка настроюється в процесі виробництва, наприклад як у фільтрів серії *NCS F24XXX*, тому бажане заздалегідь визначитися з вимогами по настроюванню й указати їх при замовленні. Фільтри різняться шириною смуги пропущення, що визначає діапазон частот, які не послабляються.

3. Кабельне з'єднання Sma-rp-plug ↔ N-type-male

Часто її ще називають *pigtale* – це невеликий перехідник з антенного виводу *indoor* точка доступу, який називається *SMA-RP* (реверс *SMA*), на широко використовуваний в антенно-фідерному встаткуванні високочастотне рознімання *N-type* (рис. 12.7).

Рис. 12.7 – Кабельне з'єднання pigtale

Pigtale – кабель входить у комплект поставки всіх зовнішніх (*outdoor*) антен D-Link, антени для внутрішнього використання також комплектуються необхідними кабелями. Вносить додаткове загасання близько 0,5 дБ.

4. *Інжектор живлення*

Включається в тракт між активним устаткуванням і вхідним портом підсилювача (вносить загасання не більш *0,5 дБ*) і підключається до блоку живлення, який підключається до розетки *220В*. Інжектор має 2 порту – обоє *N-type-female*. Інжектор живлення й блок живлення входять у комплект поставки підсилювачів.

5. *Перехідник Tlk-n-type-mm*

Перехідник *N-Type Male-Male* (рис. 12.8) служить для зміни конфігурації порту з *female* на *male*, тут ми його використовуємо, щоб підключити до інжектора наступну за ним кабельне складання (стандартні кабельні складання звичайно мають рознімання *N-type-male* ↔ *N-type-female*).

Рис. 12.8 – Перехідник Tlk-n-type-mm

Загальноприйнятим є, що коаксіальне з'єднання, установлюваний стаціонарно, наприклад входи або виходи підсилювачів, фільтрів, генераторів сигналів, з'єднання для підключення, установлювані на антенах, мають конфігурацію «гніздо» (*female*), а роз'єми на кабелях, що підключаються до них мають конфігурацію «штекер» (*male*). Однак дане правило не завжди дотримується, тому іноді виникають проблеми при складанні тракту на елементах від різних виробників. Розв'язати цю проблему дозволяє використання перехідника *N-type-male* ↔ *N-type-male*.

6. Кабельне з'єднання (наприклад, Hqnf-nm15)

Це 15-метрове кабельне з'єднання *N-type (female)* ↔ *N-type (male)* (рис. 12.9).

Рис. 12.9 – Кабельне з'єднання N-type (female) <=> N-type (male)

Можна також використовувати кабельні складання великої довжини, наприклад, послідовно об'єднавши дві *15* -метрові складання (або інші довжини), важливо тільки щоб:

– рівень сигналу на вхідному порту підсилювача попадав у припустимий діапазон, який зазначений у характеристиках підсилювача;

– рівень сигналу, прийнятого від вилученої точка доступу й посиленого в підсилювачі, мав достатню інтенсивність для сприйняття приймачем точка після проходження кабельного з'єднання.

7. Підсилювач *2,4 ГГц (наприклад, NCS24XX)*

Двонаправлений магістральний підсилювач (рис. 12.10) призначений для збільшення потужності переданого сигналу й підвищення чутливості каналу приймання в бездротових мережах передачі даних, а також компенсації втрат у каналі між радіомодемом і антеною.

Рис. 12.10 – Підсилювач 2,4 ГГц

Підсилювач має зовнішнє виконання й може бути встановлений безпосередньо на антенному пості. Використання підсилювача дозволяє організувати зв'язок навіть при самих несприятливих умовах з'єднання. При включенні підсилювача в радіосистему в значній мірі збільшується зона її покриття.

При використанні підсилювачів необхідно враховувати наступні моменти:

– якщо потужність передавача точка доступу занадто велика й не попадає в діапазон припустимої інтенсивності сигналу на вхідному порту підсилювача, то використовувати її з підсилювачем все-таки можна, але потрібно включити в тракт

між підсилювачем і точкою доступу кабельне складання або який-небудь спеціальний елемент, загасання на якому забезпечить необхідне ослаблення сигналу, для того щоб його інтенсивність потрапила в припустимий діапазон. Послабляючи переданий сигнал, слід також пам'ятати, що одночасно послабляється й прийнятий сигнал, тому не варто захоплюватися.

Приклад 12.4

Підключимо до точка доступу з потужністю передавача 200 мВт підсилювач NCS2405, на вході якого повинне бути 10-100 мВт, вихідна потужність – 500 мВт. Для цього необхідно послабити вихідний сигнал на 100 мВт, тобто у два рази або на 3 дБ; для цього включаємо в схему десятиметрове кабельне складання на основі кабелю із загасанням 0,3 дБ/м на частоті 2,4 ГГц.

– максимальна відстань, на яку можна винести підсилювач від порту радіомодема, залежить від загасання на використовуваних елементах тракту; при цьому необхідно, щоб рівень сигналу на вхідному порту підсилювача попадав у припустимий діапазон, який зазначений у характеристиках підсилювача, а також щоб рівень прийнятого від вилученого передавача сигналу й посиленого в підсилювачі, мав достатню інтенсивність для сприйняття приймачем після проходження даного кабельного складання.

Приклад 12.5

Порахуємо максимальну відстань від активного порту indoor точка доступу (потужність 16 дБмВт) до вхідного порту підсилювача *NCS2401* для схеми на рис. 12.6. Погонне загасання на кабелі на частоті *2,4 ГГц*візьмем по *0,3 дБ/м.*

Розв'язок:

Знайдемо сумарне загасання тракту до порту підсилювача (уважаємо схему без фільтра):

Y = 0,5 дБ (pigtale) + 0,5 дБ (інжектор) + 6 дБ (15-метрове кабельне складання (загасання на кабелі 0,3 дБ/м) + 3 рознімання по 0,75 дБ) = 7,75 дБ.

Отже, потужність, яка потрапить на вхід підсилювача, буде рівнятися

16 – 7,75 = 8,25 дБмВт.

Таблиця 12.3 – Загасання від середовища поширення сигналу

Найменування	Од.виміру	Значення
Вікно в цегельній стіні	дБ	2
Скло в металевій рамі	дБ	6
Офісна стіна	дБ	6
Залізні двері в офісній стіні	дБ	7
Скловолокно	дБ	0,5-1
Скло	дБ	3-20
Дощ і туман	дБ/км	0,02-0,05
Дерева	дБ/м	0,35
Кабельне з'єднання - pigtale	дБ	0,5
Смуговий фільтр *NCS* F24XXX	дБ	1,5
Коаксіальний кабель	дБ/м	0,3
Роз'єм N-type	дБ	0,75
Інжектор живлення	дБ	0,5

Для підсилювача *NCS2401* нижня границя припустимої інтенсивності сигналу на вхідному порту рівняється *4 мВт* (*6 дБмВт*). Отже, можна ще побільшати довжину кабельного складання:

8,25 – 6=2,25 дБмВт; 2,25/0,3 = 7,5 м,

т.е. ще приблизно на 7,5 метрів. Отже, максимальна відстань кабельного складання буде 22,5 метра.

Тепер подивимося, що відбувається із прийнятим сигналом. Припустимо, що від вилученого передавача на підсилювач надходить сигнал потужністю – *98 дБмВпт* ; у режимі приймання коефіцієнт підсилення підсилювача рівний *30 дБ*. Загасання тракту до порту радіомодема рівно *10 дБ* (7,75 дБ + 2,25 дБ). Знайдемо інтенсивність сигналу, що зробив на приймач точку доступу: – 98 + 30 – 10 = (– 78 дБмВпт). У таблиці 12.1 дивимося чутливість приймача й знаходимо швидкість, на якій він може працювати:

(– 78 дБмВт) < (– 76 дБмВт),

отже, при такій довжині кабельного складання точка доступу може працювати на швидкості 24 Мбіт/с. Якщо потрібна більша швидкість, необхідно або зменшити довжину кабельного

складання, або побрати підсилювач із більшим коефіцієнтом підсилення.

У таблиці 12.3 зведені всі величини загасання від середовища поширення сигналу.

8. Кабельне з'єднання (наприклад, Hqnf-nml,5)

Hqnf-nml,5 – кабель (перехідник) N-type(female) ↔ N-type(male) довгої 1,5 м.

9. Модуль грозового захисту

В устаткуванні D-Link іде з усіма зовнішніми антенами. Має роз'єм N-type(female) ↔ N-type(male).

10. Зовнішня спрямована (наприклад, ANT24-2100)

Антена з коефіцієнтом підсилення 21 дБі. Антени мають роз'єм N-type-female.

12.2.5. Простий антенно-фідерний тракт

На рис. 13.11 представлена проста бездротова система, у якій відсутній підсилювач, і антенно-фідерний тракт полягає тільки з пасивних елементів.

На рис. 12.11 показані:

- точка доступу DWL-2100AP;
- *pigtale* (у комплекті з антеною);
- кабельне з'єднання;
- модуль грозового захисту (у комплекті з антеною);
- антена *ANT24-1400*.

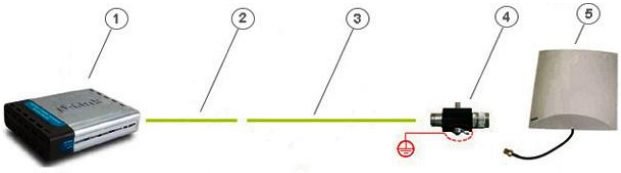


Рис. 12.11 – Простий антенно-фідерний тракт

Відстань, на яку можна винести антену в цьому випадку, обмежується потужністю передавача точка доступу й загасанням, внесеним пасивними елементами. При виносі антени на велику

відстань як прийнятий, так переданий сигнал може повністю поглинутися кабельними з'єднанням й перехідниками.

При використанні навіть самого короткого кабельного з'єднання до антени підводить потужність, значно менша вихідної, що негайно відіб'ється на дальності дії радіосистеми. Тому ми рекомендуємо використовувати в таких схемах кабельні з'єднання не довше 6 метрів і, по можливості, антени з максимальним коефіцієнтом підсилення.

12.2.6. Точка доступу, підключена прямо до антени

Якщо підключити точку доступу прямо до антени, як показано на рис. 12.12, виключивши проміжне кабельне з'єднання, буде досягнута максимальна можлива для даного комплекту встаткування дальність зв'язки.

На рис. 12.12 показані:

- точка доступу DWL-2100AP;
- *pigtale* (у комплекті з антеною);
- модуль грозового захисту (у комплекті з антеною);
- антена *ANT24-1400*.

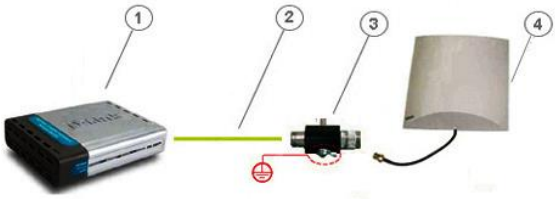


Рис. 12.12 – Точка доступу, підключена прямо до антени

У принципі, заради дальності іноді можна пожертвувати й модулем грозового захисту, щоб виключити внесене їм загасання, але краще цього не робити. Така схема досить широко використовується – це дозволяє встановити *indoor* точку доступу в безпосередній близькості від антени й мінімізувати втрати потужності сигналу.

Найбільше часто використовувані антени представлені в Додатку В. Огляд антен D-Link.

ЛІТЕРАТУРА

1. Чистяков В. А., Миктибаев Б. Є., Жанбеков А. Б. Аналіз технологій бездротової передачі даних. *Журнал наукових і прикладних досліджень*. 2016. №1. С. 166–169.
2. Джим, Г. Бездротові мережі. Перший крок (Cisco). М. : Вільямс, 2005. 192 с.
3. Беделл, П. Мережі. Бездротові технології. М. : НТ Пресс, 2008. 448 с.
4. Широкосмугові бездротові мережі передачі інформації / В.М. Вишневський та ін. М. : Техносфера, 2005. 591 с.
5. An overview and assessment of wireless technologies and coexistence of ZigBee, Bluetooth and Wi-Fi devices. R. Challoo and etc. *Procedia Computer Science*. 2012. Т. 12. С. 386–391.
6. JS Lee, YW Su, CCA Shen. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *Industrial Electronics Society*, 2007. IECON 2007. 33rd Annual Conference of the IEEE. IEEE, 2007. С. 46–51.
7. Стрельников А. Ю., Страмоусова С. А. Технологія бездротової передачі даних Wi-Fi. *Молодий вчений*. 2016. № 9-4 (113). С. 67–69.
8. Нікольський В.В., Нікольська Т.І. Електродинаміка та поширення радіохвиль. М. : Наука, 1989. 543 с.
9. Мережі на радіомодемах. *Sdamzavas*. URL: https://sdamzavas.net/1-6931.html (дата звернення: 23.11.2020).
10. Технологія SST. *Wikipedia*. URL: https://en.wikipedia.org/wiki/SST (дата звернення: 23.11.2020).
11. Бездротові мережі передачі данних. *Netwave*. URL: https://netwave.ua/bezdrotovi-merezhi-peredachi-danyh (дата звернення: 23.11.2020).
12. Мережа передачі данних Wi-Fi. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Wi-Fi (дата звернення: 23.11.2020).
13. Стандарт передачі данних Code Division Multiple Access. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/Code_Division_ Multiple _Access (дата звернення: 23.11.2020).
14. Стандарт передачі даних GPRS. *Wikipedia*. URL: https://uk.wikipedia.org/wiki/GPRS (дата звернення: 23.11.2020).

15. Бездротові системи безпеки. *Worldvision*. URL: https://worldvision.com.ua/ua/provodnye-i-besprovodnyesistemy-bezopasnosti-za-i-protiv (дата звернення: 23.11.2020).
16. Види та стандарти безпровідних мереж. *Calameo*. URL: https://ru.calameo.com/books/002206302b75f73dbbad5 (дата звернення: 23.11.2020).
17. Параметри Wi-Fi. *Ruba*. URL: https://wifi.kz/articles/radius-wi-fi-routera (дата звернення: 24.11.2020).
18. Семенко А. І. Сучасний стан створення безпровідних телекомунікаційних мереж. Львів : Львівська політехніка, 2015. 134 с.
19. Wi-Fi Plug. *Diy smart home solutions*. URL: https://www.diysmarthomesolutions.com/what-is-a-smart-plug-how-they-work-andhow-to-use-them (дата звернення: 24.11.2020).
20. Connectivity Technologies for IoT. In: Demystifying Internet of Things Security. Cheruvu S. end ect. 2020. P. 347–411. Access mode: https://doi.org/10 .1007/978-1-4842-2896-8_5.

Додаток А.

Огляд бездротового встаткування D-Link

Бездротове встаткування компанії D-Link презентовано наступними серіями продуктів:

– Серія Airplusg – призначена для створення економічних бездротових мереж стандарту *802.11g* у діапазоні частот 2,4 ГГц;

– Серія Airplusxtremeg – призначена для створення високошвидкісних бездротових мереж стандарту *802.11g* у діапазоні частот 2,4 ГГц;

– Серія Airplusxtremeg з підтримкою технології *MIMO* – призначена для створення високошвидкісних бездротових мереж стандарту *802.11g* у діапазоні частот 2,4 ГГц зі збільшеним радіусом дії;

– Серія Airpremierag – призначена для створення бездротових мереж масштабу підприємства стандартів *802.11a*/b/g у діапазоні частот 2,4/5 ГГц;

– Серія Airpremier – призначена для створення бездротових мереж масштабу підприємства й зовнішніх мереж стандартів *802.11b*/g у діапазоні частот 2,4 ГГц.

Устаткування серії Airplusg є економічно ефективним розв'язком для створення бездротових мереж удома або малого офісу. Дана серія продуктів включає бездротову крапку доступу, бездротові маршрутизатори, принт-сервери й PCI/Cardbus/ Usb-Адаптери. Усе встаткування функціонує на базі стандарту 802.11g на швидкості до 54 Мбіт/с і назад сумісне із пристроями стандарту 802.11b. Для забезпечення захисту бездротової мережі в пристроях реалізована підтримка сучасних протоколів шифрування даних WPA/WPA2. Настроювання й керування здійснюються через зручний web-інтерфейс.

DWL-G700AP Airplusg бездротова точка доступу 802.11g, до 54 Мбіт/с

Рисунок А1 – Бездротова точка доступу DWL-G700AP

- Підтримка стандартів *802.11b*/g
- 1 порт 10/*100Base-tx*
- Режими роботи: точка доступу, бездротовий повторювач
- Шифрування *WEP, WPA* і *WPA2*
- Підтримка протоколу 802.1x
- Фільтрація Mac-Адрес
- Функція відключення *широкомовлення SSID*
- Dhcp-Клієнт/сервер
- Web-Інтерфейс керування

DI-524/524UP Airplusg бездротові маршрутизатори 802.11g, до 54 Мбіт/с

Рисунок А2 – Бездротовий маршрутизатор DI-524UP

- Підтримка стандартів *802.11b*/g
- 4 порту 10/*100Base-tx* LAN
- 1 порт USB 1.1 для підключення принтера (DI-524UP)
- Шифрування *WEP*, *WPA* і *WPA2*
- Підтримка протоколу 802.1x
- NAT, VPN pass-through, фільтрація MAC/IP/URL
- Dhcp-Клієнт/сервер
- Web-Інтерфейс керування

Обгрунтування для створення високошвидкісних бездротових мереж стандарту 802.11g

Для бізнес-додатків D-Link пропонує сімейства встаткування Airplusxtremeg, Airpremierag і Airpremier, що дозволяють забезпечити високий рівень захисту інформації й підтримуючі швидкість з'єднання в обох діапазонах до 108 Мбит/с. Кожна серія бездротових пристроїв представлена точкою доступу, багатофункціональним шлюзом доступу й мережними адаптерами для шин *PCI*, *PCMCIA*, *USB*. Точка доступу, що входять у сімейства Airpremier і Airpremierag, підтримують стандарт 802.3af *Power* over *Ethernet*(*Poe*). На *додаток* до цього всі точки доступу підтримують протокол мережного керування *SNMP* v.3, який дозволяє здійснювати настроювання й

віддалений *моніторинг* пристроїв у режимі реального часу з будь-якого зручного місця.

Швидкість з'єднання до 108 Мбіт/с досягається при роботі в турбо-режимі (*Turbo mode*). Цей режим може використовуватися у двох підрежимах – *Dynamic Turbo* і *Static Turbo*.

При роботі в режимі *Dynamic Turbo* пристрою відслідковують ефір і аналізують можливі режими роботи взаємодіючих один з одним клієнтів. У випадку якщо умови навколишнього середовища дозволяють, радіолінія переводиться в режим розширеної смуги частот, і пристрою періодично відслідковують, не з'явився чи не підтримуючий турбо-режими клієнт *802.11g*. Якщо так, то система вертається у звичайний режим роботи зі швидкістю з'єднання до 54 Мбіт/с.

При роботі в *Static Turbo* режим розширеного використання радіочастотного діапазону включений постійно, при цьому встаткування без підтримки турбо-режимів таку *мережу* виявити не зможе. Швидкість з'єднання в такій бездротовій мережі буде максимально можливої, тому що пристроям не доводиться постійно перемикатися у звичайний режим функціонування.

Функція Super G without Turbo mode містить у собі наступні *механізми* підвищення продуктивності (максимальна швидкість з'єднання залишається рівної 54 Мбіт/с):

Packet Bursting (Пакетна *передача даних*): техніка пакетної передачі, що дозволяє побільшати пропускну здатність завдяки відправленню більшої кількості кадрів за те ж час і зменшенню стандартних накладних витрат за рахунок відмови від проміжних періодів очікування *DIFS* (*Distributed Interframe Space*).

Fast Frames (Швидкі кадри): технологія пакетної агрегації підвищує пропускну здатність шляхом збільшення розміру переданих кадрів і зменшення міжкадрових інтервалів.

Hardware Compression and Encryption (Апаратний стиск і *шифрування*): застосування апаратного стиску по алгоритму Lempel-Ziv і шифрування даних. Збільшення пропускної

здатності здійснюється за рахунок попереднього стиску інформації.

Функція Super G with Turbo mode містить у собі наступні *механізми* підвищення продуктивності: *Packet Bursting, Fast Frames, Hardware Compression and Encryption* і Multi-Channel *Bonding*.

Multi-Channel Bonding (*Об'єднання* каналів): максимальне збільшення пропускної здатності здійснюється за рахунок використання декількох (двох) каналів передачі одночасно.

DWL-2100AP Airplusxtremeg бездротова точка доступу 802.11g, до 108 Мбіт/с

Рисунок А3 – Бездротова точка доступу DWL-2100AP

– Підтримка стандартів *802.11b*/g 1
– порт 10/*100Base-tx*
– Режими роботи: точка доступу, *WDS* із точкою доступу, *WDS* (міст), бездротової повторювач, бездротової клієнт
– Шифрування *WEP, WPA* і *WPA2*

– Підтримка протоколу 802.1x
– Фільтрація Mac-Адрес
– Поділ *WLAN STA*
– 8 *SSID* для сегментації мережі
– Функція відключення *широкомовлення SSID*
– 802.1Q VLAN Tagging
– Підтримка WMM (Wi-Fi *Multimedia*)
– Dhcp-Клієнт/сервер
– Web-Інтерфейс керування, протокол SNMP v.1, v.3, Telnet

DI-624/624S Airplusxtremeg бездротові маршрутизатори 802.11g, до 108 Мбіт/с

Рисунок А4 – Бездротової маршрутизатор DI-624S

– Підтримка стандартів *802.11b*/g
– 4 порту 10/*100Base-tx* LAN
– 2 порту USB 2.0 (DI-624S)
– Шифрування *WEP*, *WPA* і *WPA2*
– Ip-Маршрутизація
– NAT, *SPI*, *DMZ*, VPN pass-through, фільтрація MAC/IP/URL
– Підтримка Qos (DI-624S)
– 6 вбудованих серверів (DI-624S)
– Web-Інтерфейс керування

DGL-4300 Gamerlounge ігровий маршрутизатор 802.11g, до 108 Мбіт/с

Рисунок А5 – Ігровий маршрутизатор DGL-4300

– Підтримка стандартів *802.11b*/g
– 4 порту 10/100/1000Base-T LAN
– 1 порт 10/*100Base-tx* WAN
– Антена з коефіцієнтом підсилення 5 *dbi*
– Підтримка *WDS*
– Підтримка технології Gamefuel™ Priority
– Шифрування *WEP*, *WPA* і *WPA2*
– NAT, VPN у режимі pass-through
– До 256 конфігурацій міжмережевих екранів для портів
– Політики контролю доступу ("батьківський" контроль)
– Ведення журналу подій на самому пристрої й зовнішньому сервері
– Статична/*динамічна маршрутизація*
– Повідомлення по електронній пошті
– Високопродуктивний центральний процесор для підтримки до 1000 одночасних з'єднань

– Web-Інтерфейс керування

DWL-2200AP Airpremier керована точка доступу 802.11g з підтримкою Poe, до 108 Мбіт/с

Рисунок А6 – Бездротова точка доступу DWL-2200AP

– Підтримка стандартів *802.11b*/g
– 1 порт 10/*100Base-tx*
– Антена з коефіцієнтом підсилення 5 *dbi*
– Підтримка стандарту 802.3af *Poe*
– Режими роботи: точка доступу, *WDS* із точкою доступу, *WDS* (міст)
– Шифрування *WEP*, *WPA* і *WPA2*
– Підтримка шифрування AES

– Фільтрація Mac-Адрес
– Функція відключення *широкомовлення SSID*
– 802.11i-ready
– Dhcp-Клієнт/сервер
– Web-Інтерфейс керування, протокол SNMP v.3, Telnet

DWL-3200AP Airpremier керована точка доступу 802.11g з підтримкою Poe, до 108 Мбіт/с

Рисунок А7 – Бездротова точка доступу DWL-3200AP

– Підтримка стандартів *802.11b*/g
– 1 порт 10/*100Base-tx*
– 2 антени з коефіцієнтом підсилення 5 *dbi*
– Підтримка стандарту 802.3af *Poe*
– Металевий корпус із вентиляцією
– Режими роботи: точка доступу, міст " точка-точка", міст "точка - багато крапок"
– Шифрування *WEP*, *WPA* і *WPA2*

– Підтримка протоколу 802.1x
– Фільтрація Mac-Адрес
– 8 *SSID* для сегментації мережі
– Функція відключення *широкомовлення SSID*
– 802.11i-ready
– Dhcp-Клієнт/сервер
– Web-Інтерфейс керування, протокол SNMP v.3, Telnet

DWL-7100AP Airpremier AG трехрежимная дводіапазонна бездротова точка доступу 802.11a/b/g, до 108 Мбіт/с

Рисунок А8 – Бездротова точка доступу DWL-7100AP

– Підтримка стандартів 802.11a/b/g
– 1 порт 10/*100Base-tx*
– Режими роботи: точка доступу, *WDS* із точкою доступу, *WDS* (міст), бездротової повторювач, бездротової клієнт
– Шифрування *WEP*, *WPA* і *WPA2*
– Підтримка протоколу 802.1x
– Фільтрація Mac-Адрес
– Поділ *WLAN STA*

– Функція відключення *широкомовлення SSID*
– DHCP клієнт/сервер
– Web-Інтерфейс керування, протокол SNMP v.3, Telnet

DI-784 Airpremier AG трьохрежимний дводіапазонний бездротової маршрутизатор 802.11a/b/g, до 108 Мбіт/с

Рисунок А9 – Бездротової маршрутизатор DI-784

– Підтримка стандартів 802.11a/b/g 4 порту
– 10/*100Base-tx* LAN 1 порт 10/*100Base-tx* WAN з підтримкою *Pppoe* Шифрування *WEP*, *WPA* і
– *WPA2 Ip*-Маршрутизація
– NAT, *SPI*, *DMZ*, VPN pass-through, фільтрація MAC/IP/URL, *віртуальний сервер*
– Підтримка протоколу Network Timing Protocol (*NTP*)
– Web-Інтерфейс керування

Рішення на базі технології MIMO

Завдяки підтримці технології *MIMO* (Multiple *Input* Multiple *Output*) можна в 8 разпобільшати дальність передачі бездротового сигналу.

Міmo-Пристрою, які представлені бездротовим маршрутизатором DI-634M і бездротовими *PCI*- і Cardbus-*Адаптерами* DWL-G520M і DWL-G650M, передають інформацію через безліч антен з високим коефіцієнтом підсилення. У процесі поширення радіосигнали звичайно відбиваються від об'єктів, що зустрічаються на їхньомушляху, створюючи безліч маршрутів, що приводить до їхньої інтерференції й загасанню. Пристрою використовують ефект багатопроменевого поширення для збільшення дальності передачі інформації, поєднуючи сигнали, прийняті декількома антенами на різних частотах і підвищуючи за рахунок цього *потужність вихідного* сигналу. У результаті скорочується кількість «мертвих» зон і здійснюється передача потужних сигналів на більші відстані з високими швидкостями, достатніми для роботи потокових додатків і передачі більших файлів.

Крім технології *MIMO* DI-634M, DWL-G520M і DWL-G650M підтримують технологію 108G, завдяки чому на їхній основі можна будувати надійні бездротові мережі, що забезпечують високу *продуктивність* і великий *радіус* дії. *Підтримка пристроями розширених функцій* мережної безпеки забезпечує захист бездротового з'єднання й доступу в *Internet*.

DI-634M Airplusxtremeg бездротової маршрутизатор 802.11g з підтримкою технології MIMO, до 108 Мбіт/с

Рисунок А10 – Бездротової Mimo-Маршрутизатор DI-634M

- Підтримка стандартів 802.11b/g
- Підтримка технології MIMO
- 4 порту 10/100Base-tx LAN
- 1 порт 10/100Base-tx WAN
- Шифрування WEP, WPA і WPA2
- Підтримка протоколу 802.1x
- NAT, DMZ, VPN pass-through, DHCP, віртуальний сервер
- Web-Інтерфейс керування

Рішенняя для створення зовнішніх бездротових мереж

Бездротове встаткування, призначене для зовнішнього використання, спеціально розроблене для роботи в складних кліматичних умовах і обладнане міцним водонепроникним корпусом із вбудованим обігрівачем і температурним датчиком. Крім того, дане встаткування підтримує стандарт IEEE 802.3af, що дозволяє здійснювати його установку в місцях, де немає доступних силових розеток.

Сімейство бездротових пристроїв для зовнішнього використання представлено двома точками доступу – DWL-2700AP і DWL-7700AP Пристрою мають розширені функції

забезпечення безпеки, мережного керування, включаючи протокол SNMP, і підтримують кілька режимів роботи, що дозволяє задіяти їх для створення надійних і добре керованих бездротових магістралей.

При об'єднанні двох вилучених офісів або з'єднанні двох локальних мереж дальність дії, забезпечувана зовнішніми точками доступу зі штатними антенами, може виявитися недостатньою. Відстань передачі в цьому випадку можна значно побільшати за допомогою спрямованих і всеспрямованих антен, призначених для зовнішнього використання.

DWL-2700AP Airpremier зовнішня бездротова точка доступу 802.11b/g, до 54 Мбіт/с

Рисунок А11 – Зовнішня бездротова точка доступу DWL-2700AP

- Підтримка стандартів *802.11b*/g
- 1 порт 10/*100Base-tx*
- 2 антени з коефіцієнтом підсилення 5 *dbi*
- Підтримка стандарту 802.3af *Poe*
- Міцний корпус із вбудованим обігрівачем

– Режими роботи: точка доступу, *WDS* із точкою доступу, *WDS* (міст)
– Шифрування *WEP*, *WPA* і *WPA2*
– Підтримка протоколу 802.1x
– Фільтрація Mac-Адрес
– Multiple SSID для сегментації мережі
– Поділ WLAN STA
– Функція відключення широкомовлення SSID
– 802.1Q VLAN Tagging
– Web-Інтерфейс керування, протокол SNMP v.3, Telnet

DWL-7700AP Airpremier зовнішня трьохрежимна дводіапазонна бездротова точка доступу/міст 802.11a/b/g, до 108 Мбіт/с

Рис. А12 – Зовнішня бездротова точка доступу DWL-7700AP

– Підтримка стандартів *802.11a*/b/g
– 1 порт 10/*100Base-tx*
– 2 антени з коефіцієнтом підсилення 5 *dbi*
– Підтримка стандарту 802.3af *Poe*
– Міцний корпус із вбудованим обігрівачем

– Режими роботи: точка доступу, *WDS* із точкою доступу, *WDS* (міст)
– Шифрування *WEP*, *WPA* і *WPA2*
– Підтримка протоколу 802.1x
– Фільтрація Mac-Адрес
– Multiple *SSID* для сегментації мережі
– Поділ *WLAN STA*
– Функція відключення *широкомовлення SSID*
– 802.1Q VLAN Tagging
– Підтримка WMM (Wi-Fi *Multimedia*)
– Web-Інтерфейс керування, протокол SNMP v.3, Telnet

Додаток Б.

Правила використання радіочастотного спектра

Витримка з Закону України «Про радіочастотний ресурс України»:

Цей Закон встановлює правову основу користування радіочастотним ресурсом України, визначає повноваження держави щодо умов користування радіочастотним ресурсом України, права, обов'язки і відповідальність органів державної влади, фізичних і юридичних осіб в цій сфері.

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

Автоматизована інформаційна система управління радіочастотним спектром – система надання, збирання, накопичення, захисту, обліку, обробки та використання інформації що дозволяє проводити заходи з радіочастотного планування, розподілу та використанню радіочастотного ресурсу України, оцінювати електромагнітну сумісність та здійснювати радіочастотні присвоєння;

введення в експлуатацію – перше використання радіоелектронного засобу;

введення радіоелектронних засобів та випромінювальних пристроїв в обіг на ринку України – перше забезпечення доступності радіоелектронних засобів та випромінювальних пристроїв на ринку України;

виділення радіочастот – надання відповідним записом у Плані використання радіочастотного ресурсу України права використовувати певні смуги радіочастот для застосування в Україні визначених цим Планом радіотехнологій;

вимірювання параметрів радіоелектронного засобу – частина приймальних випробувань на місці експлуатації нового радіоелектронного засобу, під час проведення яких здійснюється експериментальне визначення відповідності параметрів радіоелектронного засобу;

випромінювальний пристрій – технічний пристрій, що призначений для генерування і локального використання

радіочастотного випромінювання у промислових, наукових, медичних, побутових потребах за винятком потреб радіозв'язку;

заплановане присвоєння радіочастот – присвоєння радіочастот, для якого було виконано процедуру розрахунку електромагнітної сумісності з позитивними результатами;

заявлене присвоєння радіочастот - присвоєння радіочастот, для якого було розпочато процедуру розрахунку електромагнітної сумісності;

забезпечення електромагнітної сумісності (радіоелектронних засобів і випромінювальних пристроїв) – сукупність організаційно-технічних та технічних заходів, що проводяться власником (користувачем) радіоелектронного засобу з метою сумісного використання радіочастотного ресурсу, зменшення або виключення радіозавад між радіоелектронними засобами;

електромагнітна сумісність – здатність радіоелектронних засобів і випромінювальних пристроїв одночасно функціонувати з обумовленою якістю в реальних умовах експлуатації з урахуванням впливу ненавмисних радіозавад і не створювати шкідливих (неприпустимих) радіозавад іншим радіоелектронним засобам;

ефективне використання радіочастотного ресурсу – досягнення оптимального результату при користуванні певною технологією в межах певних смуг, номіналів радіочастот, які видані користувачу радіочастотного ресурсу, відповідно до ліцензії за тією ж технологією;

користування радіочастотним ресурсом – діяльність, пов'язана із застосуванням радіоелектронних засобів та/або випромінювальних пристроїв, що випромінюють електромагнітну енергію в навколишній простір у межах радіочастотного ресурсу;

користувач радіочастотного ресурсу - юридична, фізична особа – підприємець або фізична особа, діяльність якої безпосередньо пов'язана з користуванням радіочастотним ресурсом;

конвергентна мережа зв'язку – сукупність поєднаних між собою різних мереж технологій та інтерфейсів, таких як наземна

мережа рухомого (мобільного) зв'язку, дротова широкосмугова мережа зв'язку, мережа фіксованого телефонного зв'язку, широкосмуговий супутниковий зв'язок, канали електрозв'язку тощо, яка забезпечує доступ абонентів до широкого спектру послуг електронних комунікацій з низькою та/або високою мобільністю термінального обладнання, широким діапазоном швидкостей передавання в залежності від потреб абонентів і служб, широким спектром служб і платформ застосування послуг електронних комунікацій, незалежно від того, до якої мережі та за яким інтерфейсом підключене термінальне обладнання абонента до мережі;

конверсія радіочастотного ресурсу України – виконання комплексу заходів, яким передбачена зміна радіослужб та/або радіотехнологій чи категорії користувачів радіочастотного ресурсу України для подальшого використання певної смуги або смуг радіочастот;

ліцензія на користування радіочастотним ресурсом України – документ, що засвідчує право суб'єкта господарювання на користування радіочастотним ресурсом України протягом визначеного терміну в конкретних регіонах та в межах певних смуг, номіналів радіочастот з виконанням ліцензійних умов;

натурні випробування – експериментальне підтвердження забезпечення електромагнітної сумісності заявленого радіоелектронного засобу з іншими радіоелектронними засобами загальних та/або спеціальних користувачів радіочастотного ресурсу України;

Національна таблиця розподілу смуг радіочастот України – нормативно-правовий акт, яким регламентується розподіл смуг радіочастот радіослужбам в Україні і розподіл на смуги спеціального та загального призначення;

незаконно діючий радіоелектронний засіб, випромінювальний пристрій – радіоелектронний засіб або випромінювальний пристрій будь-якого призначення, експлуатація якого не дозволена (заборонена) в Україні або він експлуатується без визначеного законодавством відповідного замовленого, запланованого або існуючого присвоєння радіочастот, у тому числі загального дозволу;

приймальні випробування запланованого радіоелектронного засобу на місці експлуатації (первинний технічний контроль) – комплекс робіт, що складається з перевірки на місці експлуатації запланованого радіоелектронного засобу відповідності його характеристик розрахункам вимірювання та інструментальної оцінки параметрів випромінювання з метою визначення їх відповідності висновкам, стандартам, нормам випромінювання;

присвоєння радіочастоти (смуги, номіналу або радіочастотного каналу) – внесення параметрів та визначених умов експлуатації радіоелектронного засобу із статусом задіяної радіочастоти до Реєстру присвоєнь радіочастот загальних користувачів або до Реєстру присвоєнь спеціальних користувачів автоматизованої інформаційної системи управління радіочастотним спектром;

радіоаматор – фізична особа, яка здійснює користування радіочастотним ресурсом радіозавада – електромагнітне випромінювання будь-якого походження, яке перешкоджає прийманню радіосигналів;

радіозв'язок – передавання та/або приймання інформації за допомогою радіохвиль;

радіоелектронний засіб – технічний засіб, призначений для передавання та/або приймання радіосигналів радіослужбами;

радіоелектронний засіб спеціального призначення – радіоелектронний засіб, призначений для здійснення діяльності спеціальних користувачів відповідно до їх функціональних обов'язків;

радіочастотний моніторинг – комплекс організаційно-технічних заходів, що здійснюється на замовлення національного регулятора, спрямованих на контроль параметрів випромінювання радіоелектронних засобів, завчасне виявлення радіозавад;

радіохвилі – електромагнітні хвилі, частоти коливання яких не вищі за 3 ТГц, що розповсюджуються в просторі без штучного хвилеводу;

радіочастота (частота) – одиниця радіочастотного спектру, визначена певним номіналом;

радіочастотний ресурс – частина радіочастотного спектра, придатна для передавання та/або приймання електромагнітної енергії радіоелектронними засобами і яку можливо використовувати на території України та за її межами відповідно до законів України та міжнародного права, а також на виділених для України частотно-орбітальних позиціях;

радіочастотний спектр – безперервний інтервал радіочастот, не вищий за 3 ТГц;

Реєстр ліцензій на користування радіочастотним ресурсом України – інформаційний ресурс, що створений за допомогою автоматизованої системи надання, збирання, накопичення, захисту, обліку, оброблення та використання інформації, щодо виданих ліцензій на користування радіочастотним ресурсом України;

розрахунок електромагнітної сумісності – технічний розрахунок щодо можливості застосування конкретного радіоелектронного засобу з заявленими технічними характеристиками і параметрами випромінювання у визначеному місці без радіозавад для радіоелектронних засобів, що вже мають заявлені, заплановані та існуючі присвоєння радіочастот;

смуга радіочастот – безперервна сукупність частот, що розміщуються між двома визначеними граничними частотами;

сигнал розпізнавання радіоелектронного засобу – позивний сигнал або номер вибірного виклику (літерно-цифрове сполучення (слово, мелодія), який присвоюється для ідентифікації радіоповідомлень абонента електрозв'язку при проведенні сеансу радіозв'язку із використанням конкретного радіоелектронного засобу у випадках, передбачених Регламентом радіозв'язку Міжнародного союзу електрозв'язку, або міжнародний ідентифікатор термінального обладнання (IMEI, ESN, MEID, BSIC, MAC address тощо), що присвоюється виробником (виготовлювачем) цього радіоелектронного засобу для його автоматичної ідентифікації в радіомережі (мережі електронних комунікацій) або при його підключенні до неї (міжнародний ідентифікатор кінцевого обладнання) з метою забезпечення інформаційної безпеки мереж електронних комунікацій (радіомереж), розшуку;

тестове включення запланованого радіоелектронного засобу – включення запланованого радіоелектронного засобу для його перевірки і налагоджування перед та під час проведення первинного технічного контролю, а також для проведення натурних або тестових випробувань;

тестові випробування запланованого радіоелектронного засобу – експериментальне визначення забезпечення необхідної якості зв'язку в телекомунікаційній мережі і умов виконання електромагнітної сумісності з іншими радіоелектронними засобами у місці розташування та/або зоні використання;

технологічний користувач радіочастот – особа, яка здійснює користування радіочастотами для власної господарської діяльності, не пов'язаної з наданням послуг електронних комунікацій;

шкідлива радіозавада – втручання у роботу користувача радіочастотного ресурсу за допомогою радіозавади;

ширина смуги радіочастот – числова різниця між номіналами граничних частот смуги радіочастот.

Використання в Україні радіочастотного спектра здійснюється у відповідності з наступними принципами: дозвільний порядок доступу користувачів до радіочастотного спектра; платність використання радіочастотного спектра; неприпустимість безстрокового виділення смуг радіочастот, присвоєння радіочастот або радіочастотних каналів; прозорість і відкритість процедур розподілу й використання радіочастотного спектра.

Засобу зв'язку, інші радіоелектронні засоби й високочастотні пристрої, що є джерелами електромагнітного випромінювання, підлягають реєстрації. Перелік радіоелектронних засобів і високочастотних пристроїв, що підлягають реєстрації, і порядок їх реєстрації визначаються Урядом України. Радіоелектронні засоби, використовувані для індивідуального приймання програм телевізійного віщання й радіомовлення, сигналів персональних радиовызовов (радиопейджеры), електронні вироби побутового призначення й засобу персональної радіонавігації, що не містять радиоизлучающих пристроїв, використовуються на території

Україні з урахуванням обмежень, передбачених законодавством Україні, і реєстрації не підлягають. Використання без реєстрації радіоелектронних засобів і високочастотних пристроїв, що підлягають реєстрації відповідно до правил справжньої статті, не допускається.

У відповідності Законом України «Про радіочастотний ресурс України» право на використання радіочастотного спектра надається за допомогою виділення смуг радіочастот і присвоєння радіочастот або радіочастотних каналів. Використання радіочастотного спектра без відповідного дозволу Державного підприємства «Український державний центр радіочастот» не допускається.

Стаття 15. Концепція формування та реалізації національної політики у сфері користування радіочастотним ресурсом України.

1. Державне підприємство «Український державний центр радіочастот» (далі – Державне підприємство) утворено відповідно до Закону, віднесено до сфери управління національного регулятора для виконання завдань відповідно до цього Закону і здійснює свою діяльність на підставі статуту, який затверджується національним регулятором.

2. Державне підприємство здійснює такі види діяльності у сфері користування радіочастотним ресурсом України:

1) проведення розрахунків електромагнітної сумісності;

2) проведення радіочастотного моніторингу використання радіочастотного ресурсу України загальними користувачами;

3) надання технічних обґрунтувань щодо можливості застосування заявленого типу радіоелектронних засобів на території України загальними користувачами в смугах радіочастот загального користування;

4) прийняття участі у проведенні приймальних випробувань радіоелектронних засобів на місці експлуатації;

5) здійснення заходів щодо виявлення дії джерел радіозавад;

6) ведення автоматизованої інформаційної системи управління радіочастотним спектром;

7) здійснення заходів щодо забезпечення електромагнітної сумісності радіоелектронних засобів, випромінювальних пристроїв щодо присвоєння радіочастот, призначення позивних сигналів радіоелектронним засобам;

8) інші види діяльності, не заборонені чинним законодавством.

3. Державне підприємство виконує роботи на підставі господарських договорів. За рахунок розпорядників коштів Державного бюджету України виконуються роботи, пов'язані з розрахунком мереж цифрового наземного мовлення, а також роботи, пов'язані з виявленням джерел радіозавад у смугах частот загального користування за заявою спеціальних користувачів, а також на безпосереднє замовлення національного регулятора роботи, пов'язані з проведенням радіочастотного моніторингу у смугах радіочастот загального користування.

4. Докладна інформація про перелік робіт (послуг), що виконуються Державним підприємством, а також тарифи на них публікуються в офіційному бюлетені національного регулятора та розміщуються на його офіційній сторінці в мережі Інтернет.

5. Державне підприємство за дорученням національного регулятора:

надає технічну допомогу щодо проведення необхідних вимірювань під час здійснення державного нагляду за користуванням радіочастотним ресурсом України загальними користувачами;

здійснює міжнародний захист, координацію радіочастот, бере участь у роботі Міжнародного союзу електрозв'язку.

Стаття 16. Національна таблиця розподілу смуг радіочастот України

1. Національна таблиця розподілу смуг радіочастот регламентує розподіл смуг радіочастот радіослужбам в Україні та визначає смуги радіочастот спеціального та загального користування.

2. Національна таблиця розподілу смуг радіочастот України розробляється ЦОВЗ на основі Регламенту радіозв'язку Міжнародного союзу електрозв'язку та Концепції формування та

реалізації національної політики України у сфері користування радіочастотним ресурсом України, на підставі пропозицій і за участю національного регулятора, Національної ради України з питань телебачення і радіомовлення, Генерального штабу Збройних Сил України, інших заінтересованих органів державної влади. ЦОВЗ подає зазначену Таблицю на затвердження Кабінету Міністрів України після її погодження національним регулятором, Національною радою України з питань телебачення і радіомовлення та Генеральним штабом Збройних Сил України.

До розгляду питання про затвердження Національної таблиці розподілу смуг радіочастот України на засідання Кабінету Міністрів України обов'язково запрошуються члени національного регулятора, Національної ради України з питань телебачення і радіомовлення та представники Генерального штабу Збройних Сил України.

3. Національна таблиця розподілу смуг радіочастот України визначає:

1) розподіл смуг радіочастот між радіослужбами відповідно до Регламенту радіозв'язку Міжнародного союзу електрозв'язку;

2) розподіл смуг радіочастот на смуги спеціального та загального користування.

4. Зміни до Національної таблиці розподілу смуг радіочастот України вносяться у порядку визначеному цим Законом для її розробки та затвердження.

5. ЦОВЗ, з урахуванням національних інтересів, організовує діяльність щодо зближення розподілу смуг радіочастот, визначеного Національною таблицею розподілу смуг радіочастот, з розподілом смуг радіочастот, рекомендованим Міжнародним союзом електрозв'язку та Європейським Союзом.

6. ЦОВЗ публікує Національну таблицю розподілу смуг радіочастот України на своїй офіційній сторінці в мережі Інтернет.

Національний регулятор публікує Національну таблицю розподілу смуг радіочастот України в своєму офіційному бюлетені та розміщує на офіційній сторінці в мережі Інтернет.

Стаття 17. План використання радіочастотного ресурсу України

1. Радіочастотний ресурс України використовується відповідно до Плану використання радіочастотного ресурсу України.

2. План використання радіочастотного ресурсу України та зміни до нього розробляються із врахуванням та дотриманням принципів:

1) Концепції формування та реалізації національної політики у сфері користування радіочастотним ресурсом України;

2) державної політики щодо розвитку сфер електронних комунікацій;

3) національної таблиці розподілу смуг радіочастот України;

4) рекомендацій Міжнародного союзу електрозв'язку, Європейської конференції адміністрацій пошти та електрозв'язку, інших міжнародних організацій, членом яких є або має намір стати Україна;

5) дотримання вимог щодо електромагнітної сумісності;

6) дотримання вимог, що стосуються національної безпеки, оборони та охорони громадського правопорядку;

7) забезпечення міжнародної координації радіочастот;

8) необхідності розробки та впровадження заходів, спрямованих на забезпечення ефективного використання радіочастотного ресурсу України;

9) необхідності забезпечення принципу технологічної нейтральності (з дотриманням принципів ефективного розподілу радіочастотного ресурсу України та підтримання конкуренції на ринку);

10) дотримання принципу зменшення обмежень на шляху доступу до радіочастотного ресурсу України та його використання.

2. План використання радіочастотного ресурсу України визначає:

1) перелік радіотехнологій, що використовуються в Україні, з визначенням смуг радіочастот та радіослужб, яким

вони відповідають, а також терміни припинення їх розвитку та використання;

2) перелік перспективних для впровадження в Україні радіотехнологій із визначенням смуг радіочастот та радіослужб, яким вони відповідають, а також терміни їх впровадження.

3. План використання радіочастотного ресурсу України є постійно діючим нормативно-правовим актом, що затверджується Кабінетом Міністрів України за поданням ЦОВЗ.

4. План використання радіочастотного ресурсу України розробляється ЦОВЗ згідно з Національною таблицею розподілу смуг радіочастот України на підставі пропозицій і за участю національного регулятора, Національної ради України з питань телебачення і радіомовлення, Генерального штабу Збройних Сил України, інших заінтересованих органів державної влади, а також громадських організацій та суб'єктів підприємницької діяльності. ЦОВЗ подає зазначений План на затвердження Кабінету Міністрів України після його погодження національним регулятором, Національною радою України з питань телебачення і радіомовлення та Генеральним штабом Збройних Сил України. До розгляду питання про затвердження Плану використання радіочастотного ресурсу України на засідання Кабінету Міністрів України обов'язково запрошуються керівники ЦОВЗ, члени національного регулятора, та представники Генерального штабу Збройних Сил України.

5. Перегляд Плану використання радіочастотного ресурсу України здійснюється не рідше одного разу на рік. Зміни до Плану вносяться за необхідністю у порядку, визначеному цим Законом для розробки та затвердження Плану.

6. ЦОВЗ розглядає пропозиції про зміни до Плану використання радіочастотного ресурсу України та вносить їх із своїми висновками до Кабінету Міністрів України протягом одного місяця від дня надходження пропозицій.

7. Кабінет Міністрів України розглядає внесені ЦОВЗ пропозиції про зміни до Плану використання радіочастотного ресурсу України протягом місяця від дати їх подання.

8. Порядок та терміни розробки Плану використання радіочастотного ресурсу України визначаються Кабінетом Міністрів України відповідно до вимог цього Закону.

9. Контроль за виконанням Плану використання радіочастотного ресурсу України покладається на національного регулятора.

Стаття 18. Конверсія радіочастот

1. Конверсія радіочастотного ресурсу України передбачає комплекс заходів, у результаті виконання яких відбувається зміна умов користування частиною радіочастотного ресурсу України (радіочастот та/або смуг радіочастот) для подальшого його використання користувачами інших категорій та/або впровадження інших технологій.

2. Конверсія радіочастотного ресурсу України здійснюється на виконання та відповідно до Плану конверсії радіочастотного ресурсу України, а також згідно із стратегічними завданнями держави щодо впровадження сучасних технологій електронних комунікацій.

3. Проект Плану конверсії радіочастотного ресурсу України розробляє ЦОВЗ відповідно до Плану використання радіочастотного ресурсу України, на підставі пропозицій і за участю національного регулятора, Національної ради України з питань телебачення і радіомовлення, Генерального штабу Збройних Сил України, інших заінтересованих державних органів.

4. ЦОВЗ, національний регулятор, Генеральний штаб Збройних Сил України забезпечують проведення конверсії радіочастотного ресурсу України та несуть відповідальність за здійснення конверсії в обсягах та у терміни, передбачені Планом конверсії радіочастотного ресурсу України.

5. Конверсія радіочастотного ресурсу України в інтересах спеціальних та загальних користувачів здійснюється за рахунок Державного бюджету України. Кабінет Міністрів України в установленому порядку для проведення конверсії радіочастотного ресурсу України може залучати додаткові позабюджетні кошти.

Додаток В.

Обладнання радіодоступу
(радіоінтерфейс передачі даних IEEE802.11n)

Відповідно до Додаток 10до рішення НКРЗІ від 12.01. 2012 № 18 (у редакції рішення НКРЗІ від 20.10.2015 № 545)

Таблиця В.1 – Узагальнені умови застосування в смузі радіочастот 2400-2483,5 МГц:

	Найменування параметру	Опис	Примітка
1.	Служба радіозв'язку	Фіксована	Радіозв'язок у системі передавання даних з використанням шумоподібних сигналів
2.	Радіотехнологія	Широкосмуговий радіодоступ	Обладнання радіодоступу (адаптери, безпроводові картки, радіомодулі, приєднувальні пристрої, тощо) для безпроводових мереж передачі даних (WLAN), включаючи локальні безпроводові обчислювальні мережі (WAS/RLANs); технічні засоби телекомунікацій (базові станції, точки безпроводового доступу) для організації мережі передачі даних з використанням шумоподібних сигналів, термінальне (кінцеве) радіообладнання (абонентські станції радіодоступу) та обладнання фіксованого радіодоступу
3.	Смуга радіочастот	2400-2483,5 МГц*	

Таблиця В.1 (Продовження)

4.	Сітка (центральних частот)	5 МГц	Формула утворення сітки центральних частот каналів: f_n=2412+5*(n-1), де n=1,2, …,13. 1) Центральні частоти каналів з шириною каналу 20 МГц: 2412 МГц, 2417 МГц, 2422 МГц, 2427 МГц, 2432 МГц, 2437 МГц, 2442 МГц, 2447 МГц, 2452 МГц, 2457 МГц, 2462 МГц, 2467 МГц, 2472 МГц; 2) Центральні частоти каналів з шириною каналу 40 МГц: 2422 МГц, 2427 МГц, 2432 МГц, 2437 МГц, 2442 МГц, 2447 МГц, 2452 МГц, 2457 МГц, 2462 МГц.
5.	Тип модуляції/клас випромінювання	20M0G1W (22M0G1D) 20M0D1W (22M0D1D) 40M0G1W (40M0G1D) (40M0D1D) **	BPSK, QPSK, 16QAM, 64QAM з використанням технології ортогонального мультиплексування частотних каналів (OFDM)

Таблиця В.1 (Продовження)

6.	Метод радіодоступу/дуплексу	CSMA-CA/TDD	Багатостанційний доступ з контролем несучої і попередженням колізії
7.	Максимальна потужність передавача (передавачів)	100 мВт ЕІВП ≤ 100 мВт (для використання на бездозвільній основі)	Максимальне середнє значення спектральної щільності ЕІВП до 10 мВт/МГц. Мінімальна потужність передавача 1 мВт При використанні режиму роботи з багатоелементними антенними системами (технологія MIMO) з двома та більше просторовими каналами передачі, сумарна ЕІВП усіх передавачів, які формують різні просторові канали передачі і використовуються у відповідній схемі технології MIMO, не повинна перевищувати вказаних припустимих значень ЕІВП та спектральної щільності ЕІВП

Таблиця В.1 (Продовження)

8.	Порядок використання*	На бездозвільній основі всередині приміщень	Відповідно до пункту 4 розділу 1 або пункту 3 розділу 2 Норм, що регулюють використання деяких типів РЕЗ або ВП для їх експлуатації відповідно до вимог частин другої та восьмої статті 30 Закону України «Про радіочастотний ресурс України» (на бездозвільній та безоплатній основі) (далі – Норми) додатку до Переліку радіоелектронних засобів та випромінювальних пристроїв, на експлуатацію яких потрібен дозвіл на експлуатацію радіоелектронного засобу або випромінювального пристрою, затвердженого рішенням НКРЗІ від 23.12.2014 № 844, зареєстрованого в Міністерстві юстиції України 19.02.2015 за № 201/26646 (далі – Перелік)
		На бездозвільній основі	Відповідно до пункту 8 розділу 1 Норм Переліку
		За дозволом на експлуатацію радіоелектронного засобу	На кожний РЕЗ видається дозвіл на експлуатацію в залежності від виду (місця у радіомережі) згідно з позицією 24 Вимог щодо отримання дозволу на експлуатацію видів РЕЗ (ВП) залежно від радіотехнології, в якій його застосовується (розділ ІІ Переліку).

Таблиця В.1 (Продовження)

9.	Основні загальні вимоги до РЕЗ (національні стандарти або європейські гармонізовані чи між - народні стандарти)	ДСТУ ETSI EN 300 328:2008[1]	
11.	Додаткові вимоги щодо умов застосування		При застосуванні всередині приміщень набездозвільній основі щільність потоку потужності, що створюється антеною цього РЕЗ навідстані 100 м. від зовнішніх стін будівель, неповинна перевищувати мінус 110 дБ (Вт/м^2×1 МГц)
12.	Вимоги щодо антени	Ненаправлена інтегрована/конструктивна антена	При застосуванні всередині приміщень з коефіцієнтом підсилення до 6 дБі

[1]ДСТУ ETSI EN 300 328:2008Електромагнітна сумісність і радіочастотний спектр. Системи з радіодоступом у діапазоні частот 2,4 ГГц. Загальні вимоги до радіоінтерфейсу (ETSIEN 300 328:2006, IDT)

*Користування смугою радіочастот 2400-2483,5 МГц для надання телекомунікаційних послуг здійснюється на підставі ліцензій на користування радіочастотним ресурсом України

**Огинаюча спектру випромінювання передавача (спектральна маска) (спектральні характеристики випромінювання РЕЗ (радіоінтерфейс IEEE 802.11n)

Таблиця В.2. Узагальнені умови застосування в смугах радіочастот 5150-5350 МГц:

№	Найменування параметру	Опис	Примітка
11	Служба радіозв'язку	Рухома, за винятком повітряної рухомої	Радіозв'язок у багатоканальних розподільчих системах для передавання та ретрансляції телевізійного зображення, передавання звуку, цифрової інформації
2	Радіотехнологія	Широкосмуговий радіодоступ	Обладнання радіодоступу (адаптери, безпроводові картки, радіомодулі, приєднувальні пристрої, тощо) для безпроводових мереж передачі даних (WLAN), включаючи локальні безпроводові обчислювальні мережі (WAS/RLANs); технічні засоби телекомунікацій базові станції дступу.
3	Смуга радіочастот	5150-5250 МГц 5250-5350 МГц*	

Таблиця В.2 (Продовження)

4	Сітка (центральних) частот	5 МГц	Формула утворення сітки центральних частот каналів: f_n=5000+5*n, де 1) для ширини каналу 20 МГц n=32, 36, 40, 44, 48, 52, 56, 60, 64; Центральні частоти каналів з шириною каналу 20 МГц: 5160 МГц, 5180 МГц, 5200 МГц, 5220 МГц, 5240 МГц, 5260 МГц, 5280 МГц, 5300 МГц, 5320 МГц; 2) для ширини каналу 40 МГц n=38, 46, 56, 64; Центральні частоти каналів з шириною каналу 40 МГц: 5190 МГц, 5230 МГц, 5280 МГц, 5320 МГц.
5	Тип модуляції/клас випромінювання	20M0G1W (20M0G1D) 20M0D1W (20M0D1D) 40M0G1W (40M0G1D) 40M0D1W (40M0D1D) **	BPSK, QPSK, 16QAM, 64QAM з використанням технології ортогонального мультиплексування частотних каналів (OFDM)

Таблиця В.2 (Продовження)

6	Метод радіо-доступу	CSMA-CA/TDD	Багатостанційний доступ з контролем несучої і попередженням колізії
7	Максимальна потужність передавача (передавачів)	ЕІВП ≤ 200 мВт	У смузі радіочастот 5150-5350 МГц максимальне значення спектральної щільності ЕІВП не повинне перевищувати 10 мВт/МГц у будь-якій смузі шириною 1 МГц. При використанні режиму роботи з багатоелементними антенними системами (технологія MIMO) з двома та більше просторовими каналами передачі, сумарна ЕІВП усіх передавачів, які формують різні просторові канали передачі і використовуються у відповідній схемі технології MIMO, не повинна перевищувати вказаних припустимих значень ЕІВП та спектральної щільності ЕІВП
		ЕІВП ≤ 100 мВт (для використання на бездозвільній основі)	
8	Вимоги щодо завадозахищеності та забезпечення ЕМС	-	Наявність алгоритмів контролю потужності випромінювання та динамічного вибору частоти згідно з вимогами стандарту ETSIEN 301 893 (ДСТУ 7115:2009)

Таблиця В.2 (Продовження)

9	Порядок використання*	На бездозвільній основі всередині приміщень	Відповідно до пункту 4 розділу 1 та пункту 3 розділу 2 Норм, що регулюють використання деяких типів РЕЗ або ВП для їх експлуатації відповідно до вимог частин другої та восьмої статті 30 Закону України «Про радіочастотний ресурс України» (на бездозвільній та безоплатній основі) (далі – Норми) додатку до Переліку радіоелектронних засобів та випромінювальних пристроїв, на експлуатацію яких потрібен дозвіл на експлуатацію радіоелектронного засобу або випромінювального пристрою, затвердженого рішенням НКРЗІ від 23.12.2014 № 844, зареєстрованого в Міністерстві юстиції України 19.02.2015 за № 201/26646 (далі – Перелік)
		На бездозвільній основі абонентські станції радіодоступу	Відповідно до пункту 8 розділу 1 Норм Переліку

Таблиця В.2 (Продовження)

		За дозволом на експлуата-цію радіоелек-тронного засобу	На кожний РЕЗ видається дозвіл на експлуатацію в залежності від виду (місця у радіомережі) згідно з позицією 24 Вимог щодо отримання дозволу на експлуатацію видів РЕЗ (ВП) залежно від радіотехнології, в якій його застосовується (розділ II Переліку).
10	Основні загальні вимоги до РЕЗ (націо-нальні стандар-ти.	ДСТУ 7115:2009[2]	-

[2] ДСТУ 7115:2009 Обладнання радіодоступу діапазону частот 5 ГГц. Загальні технічні вимоги та методи випробування (ETSI EN 301 893:2008, MOD)

Таблиця В.2 (Продовження)

11	Додатко-ві вимоги щодо умов засто-сування	-	Призастосуванні всередині приміщень набездозвільній основі щільність потоку потужності, що створюється антеною цього РЕЗ навідстані 100м. від зовнішніх стін будівель, неповинна перевищувати мінус 110 дБ (Вт/м^2×1 МГц)
12	Вимоги щодо антени	Ненаправ-лена інтегрована/ конструк-тивна антена	При застосуванні всередині приміщень з коефіцієнтом підсилення до 6 дБі
14	Посила-ння	ДСТУ 7115:2009[1], ETSIEN 301 893[3]/ / ERC/DEC/(04)08[4]/ Резолюція 229 (перегл. ВКР-12)[5],	Ефективне використання спектру / / ECC Рішення / Інші посилання

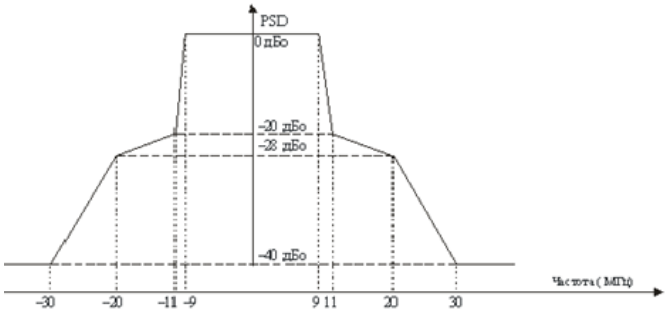
[3]ETSI EN 301 893 V1.6.1 (2011-11) Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

[4] ECC/DEC/(04)08. ECC Decision of 09 July 2004 on the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)

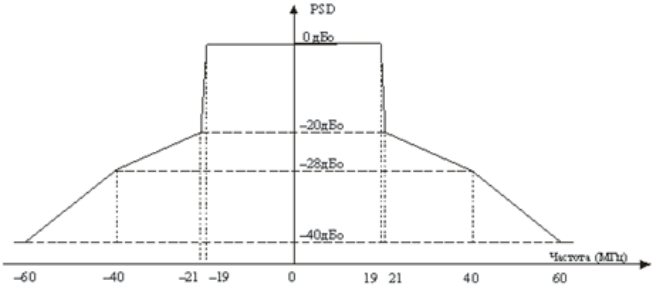
[5]Резолюція 229 (переглянута ВКР-12) Использование полос частот 5150-5250 МГц, 5250-5350 МГц и 5470-5725 МГц подвижной службой для внедрения беспроводного доступа, включая локальные радиосети

*Користування смугою радіочастот 5250-5350 МГц для надання телекомунікаційних послуг здійснюється на підставі ліцензій на користування радіочастотним ресурсом України. Смуга радіочастот 5150-5250 МГц згідно з Планом використання радіочастотного ресурсу України, затвердженого постановою Кабінету Міністрів України від 09.06.2006 № 815, призначена для використання технологічними користувачами

** Огинаюча спектру випромінювання передавача (спектральна маска) (спектральні характеристики випромінювання РЕЗ (радіоінтерфейс IEEE 802.11n)



Для ширини смуги випромінювання каналу 20 МГц



Для ширини смуги випромінювання каналу 40МГц

Таблиця В.3 Узагальнені умови застосування в смузі радіочастот 5470-5670 МГц:

№	Найменування параметру	Опис	Примітка
11	Служба радіозв'язку	Рухома, за винятком повітряної рухомої	Радіозв'язок у багатоканальних розподільчих системах для передавання та ретрансляції телевізійного зображення, передавання звуку, цифрової інформації
2	Радіотехнологія	Широкосмуговий радіодоступ	Обладнання радіодоступу (адаптери, безпроводові картки, радіомодулі, приєднувальні пристрої, тощо) для безпроводових мереж передачі даних (WLAN), включаючи локальні безпроводові обчислювальні мережі (WAS/RLANs); технічні засоби телекомунікацій (базові станції, точки безпроводового доступу), термінальне (кінцеве) радіообладнання (абонентські станції радіодоступу) та обладнання фіксованого радіодоступу
3	Смуга радіочастот	5470-5670 МГц*	-

Таблиця В.3 (Продовження)

4	Сітка частот	5 МГц	Формула утворення сітки центральних частот каналів: f_n=5000+5*n, де 1) для ширини каналу 20 МГц n=100, 104, 108, 112, 116, 120, 124, 128, 132; Центральні частоти каналів шириною смуги випромінювання 20 МГц: 5500 МГц, 5520 МГц, 5540 МГц, 5560 МГц, 5580 МГц, 5600 МГц, 5620 МГц, 5640 МГц, 5660 МГц; 2) для ширини каналу 40 МГц n=98, 106, 114, 122, 130; Центральні частоти каналів: шириною смуги випромінювання 40 МГц: 5490 МГц, 5530 МГц, 5610 МГц, 5650 МГц.

Таблиця В.3 (Продовження)

5	Тип модуляції/ клас випромінювання	20M0G1W (20M0G1D) 20M0D1W (20M0D1D) 40M0G1W (40M0G1D) 40M0D1W (40M0D1D) **	BPSK, QPSK, 16QAM, 64QAM з використанням технології ортогонального мультиплексування частотних каналів (OFDM)
6	Метод радіодоступ	CSMA-CA/TDD	Багатостанційний доступ з контролем несучої і попередженням колізії
7	Максимальна потужність передавача	250 мВт та ЕІВП ≤ 1 Вт	При застосуванні поза межами (ззовні) будівель. Максимальне значення спектральної щільності ЕІВП не повинне перевищувати 50 мВт/МГц у будь-якій смузі шириною 1 МГц. При використанні режиму роботи з багатоелементними антенними системами (технологія MIMO) з двома та більше просторовими каналами передачі, сумарна ЕІВП усіх передавачів, які формують різні просторові канали передачі і використовуються у відповідній схемі технології MIMO, не повинна перевищувати вказаних припустимих значень ЕІВП та спектральної щільності ЕІВП
		ЕІВП ≤ 100 мВт (для використання на бездозвільній основі)	

Таблиця В.3 (Продовження)

8	Порядок використання*	На бездозвільній основі всередині приміщень	Відповідно до пункту 4 розділу 1 та пункту 3 розділу 2 Норм, що регулюють використання деяких типів РЕЗ або ВП для їх експлуатації відповідно до вимог частин другої та восьмої статті 30 Закону України «Про радіочастотний ресурс України» (на бездозвільній та безоплатній основі) (далі – Норми) додатку до Переліку радіоелектронних засобів та випромінювальних пристроїв, на експлуатацію яких потрібен дозвіл на експлуатацію радіоелектронного засобу або випромінювального пристрою, затвердженого рішенням НКРЗІ від 23.12.2014 № 844, зареєстрованого в Міністерстві юстиції України 19.02.2015 за № 201/26646 (далі – Перелік)
		За дозволом на експлуатацію радіоелектронного засобу	На кожний РЕЗ видається дозвіл на експлуатацію в залежності від виду (місця у радіомережі) згідно з позицією 24 Вимог щодо отримання дозволу на експлуатацію видів РЕЗ (ВП) залежно від радіотехнології, в якій його застосовується (розділ ІІ Переліку).

Таблиця В.3 (Продовження)

9	Основні агальні вимоги до РЕЗ (національні стандарти.	ДСТУ 7115:2009	-
10	Додаткові вимоги щодо умов застосування		При застосуванні всередині приміщень на бездозвільній основі щільність потоку потужності, що створюється антеною цього РЕЗ на відстані 100 м від зовнішніх стін будівель, не повинна перевищувати мінус 110 дБ (Вт/м^2×1 МГц)
11	Вимоги щодо антен.	Ненаправлена інтегрована/конструктивна антена	При застосуванні всередині приміщень з коефіцієнтом підсилення до 6 дБі

Таблиця В.3 (Продовження)

12	Посилання	ДСТУ 7115:2009[1],ETSIEN 301 893[6]/ / ERC/DEC/(04)08[7]/ Резолюція 229 ((перегл. ВКР-12)[8], IEEE Std 802.11n-2009[9]	Ефективне використання спектру / / ЕСС Рішення / Інші посилання

*Користування смугою радіочастот 5470-5670 МГц для надання телекомунікаційних послуг здійснюється на підставі ліцензій на користування радіочастотним ресурсом України.

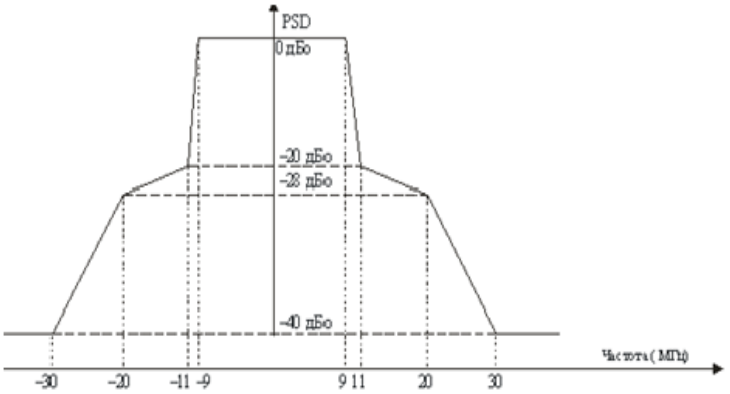
** Огинаюча спектру випромінювання передавача (спектральна маска) (спектральні характеристики випромінювання РЕЗ (радіоінтерфейс IEEE 802.11n)

[6]ETSI EN 301 893 V1.6.1 (2011-11) Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

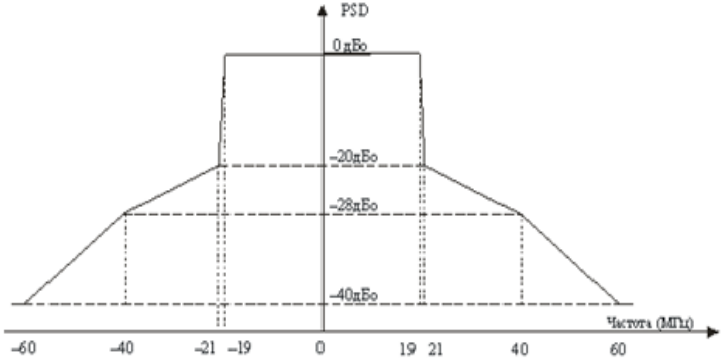
[7] ECC/DEC/(04)08. ECC Decision of 09 July 2004 on the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)

[8]Резолюція 229 (переглянута ВКР-12) Використання смуг частот 5150-5250 МГц, 5250-5350 МГц та 5470-5725 МГц рухомою службою для впровадження бездротового доступу, включаючи локальні радіомережі

[9] IEEE Std 802.11n-2009 Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput



Для ширини смуги випромінювання каналу 20 МГц



Для ширини смуги випромінювання каналу 40МГц

Таблиця В.4 Узагальнені умови застосування в смузі радіочастот 5725-5850 МГц:

№	Найменування параметру	Опис	Примітка
1	Служба радіозв'язку	Фіксована	Радіозв'язок у системі передавання даних з використанням шумоподібних сигналів
2	Радіотехнологія	Широко-смуговий радіодоступ	Обладнання радіодоступу (адаптери, безпроводові картки, радіомодулі, приєднувальні пристрої, тощо) для безпроводових мереж передачі даних (WLAN), включаючи локальні безпроводові обчислювальні мережі (WAS/RLANs); технічні засоби телекомунікацій (базові станції, точки безпроводового доступу) та обладнання фіксованого радіодоступу

Таблиця В.4 (Продовження)

3	Смуга радіочастот	5725-5850 МГц*	-
4	Сітка (центральних) частот	5 МГц	Формула утворення сітки центральних частот каналів: f_n=5000+5*n, де 1) для каналів з шириною смуги випромінювання 20 МГц n=148 – 168. Центральні частоти каналів шириною смуги випромінювання 20 МГц: 5740 МГц, 5745 МГц, 5750 МГц, 5755 МГц, 5760 МГц, 5765 МГц, 5770 МГц, 5775 МГц, 5780 МГц, 5785 МГц, 5790 МГц, 5795 МГц, 5800 МГц, 5805 МГц, 5810 МГц, 5815 МГц, 5820 МГц, 5825 МГц, 5830 МГц, 5835 МГц, 5840 МГц; 2) для каналів з шириною смуги випромінювання 40 МГц де n=156, 160, 162.

Таблиця В.4 (Продовження)

5	Тип модуляції/клас випромінювання	20M0G1W (20M0G1D) 20M0D1W (20M0D1D) 40M0G1W (40M0G1D) 40M0D1W (40M0D1D) **	BPSK, QPSK, 16QAM, 64QAM з комбінованим використанням технології ортогонального мультиплексування частотних каналів (OFDM)
6	Метод радіодоступу/дуплексу	CSMA-CA/TDD	Багатостанційний доступ з контролем несучої і попередженням колізії
7	Максимальна потужність передавача	250 мВт та ЕІВП ≤ 2 Вт ЕІВП ≤ 100 мВт (для використання на бездозвільній основі)	При застосуванні всередині будівель. Максимальне значення спектральної щільності ЕІВП не повинне перевищувати 50 мВт/МГц у будь-якій смузі шириною 1 МГц. При використанні режиму роботи з багатоелементними антенними системами (технологія MIMO) з двома та більше просторовими каналами передачі, сумарна ЕІВП усіх передавачів.

Таблиця В.4 (Продовження)

8	Вимоги щодо завадозахище-ності та забезпечення ЕМС	-	Наявність алгоритмів контролю потужності випромінювання та динамічного вибору частоти згідно з вимогами стандарту ETSIEN 301 893 (ДСТУ 7115:2009) Максимальна середня щільність ЕІВП до 200 мВт/МГц у будь-якій смузі шириною 1 МГц.
9	Порядок використання*	На бездозвільній основі всередині приміщень	Відповідно до пункту 4 розділу 1 та пункту 3 розділу 2 Норм, що регулюють використання деяких типів РЕЗ або ВП для їх експлуатації відповідно до вимог частин другої та восьмої статті 30 Закону України «Про радіочастотний ресурс України» (на бездозвільній та безоплатній основі) (далі – Норми) додатку до Переліку радіоелектронних засобів та випромінювальних пристроїв.

Таблиця В.4 (Продовження)

		На бездозвільній основі абонентські станції радіодоступу	Відповідно до пункту 8 розділу 1 Норм Переліку
		За дозволом на експлуатацію радіоелектронного засобу	На кожний РЕЗ видається дозвіл на експлуатацію в залежності від виду (місця у радіомережі) згідно з позицією 24 Вимог щодо отримання дозволу на експлуатацію видів РЕЗ (ВП) залежно від радіотехнології, в якій його застосовується (розділ ІІ Переліку).
10	Основні загальні вимоги до РЕЗ (національні стандарти або європейські гармонізовані чи міжнародні стандарти)	ДСТУ 7115:2009[10]	-

[10]ДСТУ 7115:2009 Обладнання радіодоступу діапазону частот 5 ГГц. Загальні технічні вимоги та методи випробування (ETSI EN 301 893:2008, MOD)

Таблиця В.4 (Продовження)

11	Додаткові вимоги щодо умов застосування	-	При застосуванні всередині приміщень на бездозвільній основі щільність потоку потужності, що створюється антеною цього РЕЗ на відстані 100 м від зовнішніх стін будівель, не повинна перевищувати мінус 110 дБ (Вт/м^2×1 МГц)
12	Вимоги щодо антени	Ненаправлена інтегрована/конструктивна антена	При застосуванні всередині приміщень з коефіцієнтом підсилення до 6 дБі
13	Посилання	ДСТУ 7115:2009[1], ETSI EN 302 502[11]/ / IEEE Std 802.11n-2009[12],	Ефективне використання спектру / / ECC Рішення / Інші посилання

*Користування смугою радіочастот 5725-5850 МГц для надання телекомунікаційних послуг здійснюється на підставі ліцензій на користування радіочастотним ресурсом України

[11]ETSI EN 302 502 V1.2.1 (2008-07) Broadband Radio Access Networks (BRAN);5,8 GHz fixed broadband data transmitting systems; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

[12] IEEE Std 802.11n-2009 Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput

**Огинаюча спектру випромінювання передавача (спектральна маска) (спектральні характеристики випромінювання РЕЗ (радіоінтерфейс IEEE 802.11n)

Таким чином відповідноДСТУ 7115:2009 та «Загальним технічним вимогам та методам випробування» (ETSI EN 301 893:2008, MOD)і Узагальненим умовам застосування в смузі радіочастот 2400-2483,5МГц, 5150-5350 МГц, 5470-5670 МГц, 5725-5850 МГц.

Дозволити громадянам України та юридичним особам використання на вторинній основі радіочастот у межах смуги радіочастот 2400-2483,5 Мгц для експлуатації усередині-офісних систем передачі даних на території Україні без оформлення дозволів на використання радіочастот, при виконанні наступних умов:

- експлуатації РЕЗ внутрішнофісних систем передачі даних тільки усередині будинків, закритих складських приміщень і виробничих територій;
- реєстрації РЕЗ внутрішнофісних систем передачі данихустановленим у Україні порядком.

У Додаток 10 до рішення НКРЗІ від 12.01. 2012 № 18 (у редакції рішення НКРЗІ від 20.10.2015 № 545) включене, зокрема внутрішньо офісне встаткування, що випливає, D-Link:

DWL-1000AP+, DWL-1040AP+, DWL-900AP+, DWL-650+, DWL-520+, DWL-120+, DI-714P+, DI-614+, DWL-G520, DWL-G650, DWL-2100AP, DI-624, DWL-G520+, DWL-G650+, DWL-2000AP+, DI-624+, DI-724P+, DI-824VUP+, *DSL-G*604T, DWL-G120, DWL-G122, DWL-G510, DWL-G630, DWL-G730AP, DI-524, DWL-3200AP.

3) Bluethooth.

Порядок використання на території Україні радіоелектронних засобів технології Bluetooth, що працюють у смузі частот 2400-2483,5 Мгц. визначає можливість використання, придбання й експлуатації радіоелектронних засобів технології Bluetooth з максимальною випромінюваною потужністю не більш 2,5 мВт без оформлення дозволів органів державної радіочастотної служби й без наступної реєстрації цихРЕЗ у зазначених органах.

Додаток Г.

Огляд антен D-Link

Антена ANT24-0700

Це всеспрямована антена з високим коефіцієнтом підсилення *7 дБи* (рис. В.1(а)).Діаграма спрямованості показано на рис. Г.1(б))

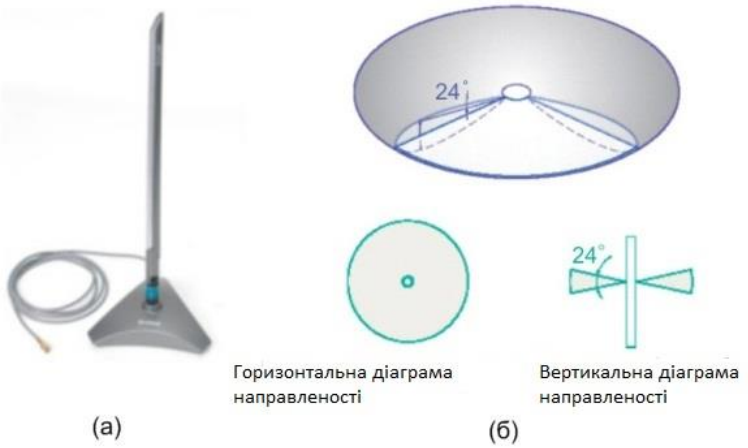


Рисунок Г.1 – Антена ANT24-0700

Антена *D-Link ANT24-0700* – це всеспрямована антена з високим коефіцієнтом підсилення, призначена для використання в приміщенні в діапазоні частот *2,4 ГГц*. Її можна застосовувати з бездротовими пристроями *802.11b* і *802.11g*, такими як точка доступу й вилучені маршрутизатори. Антену можна використовувати для заміни стандартної антени бездротового пристрою з метою збільшення радіуса дії. Вона може бути підключена до бездротового пристрою через кабель (вхідний у комплект поставки антени) або прямо.

Антена ANT24-0800

Це всеспрямована антена для внутрішнього й зовнішнього використання з коефіцієнтом підсилення 8 *дБі* (рис. Г.2 (а)).Діаграма спрямованості показано на рис. Г.2 (б).
діаграма направленості

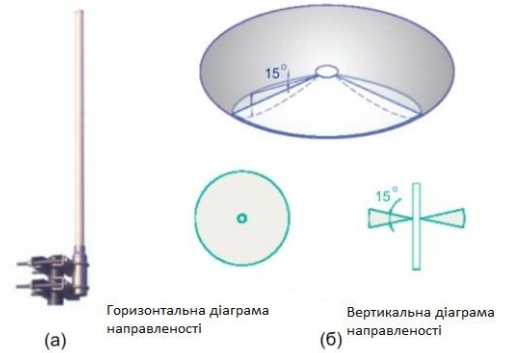


Рисунок Г.2 – Антена ANT24-0800

D-Link ANT24-0800 підключається до бездротових пристроїв, що працюють у частотному діапазоні 2,4 ГГц для збільшення площі покриття бездротової мережі. Дана модель має 360-градусну зону охвату (у горизонтальній площині) і 15-градусну зону охвату по вертикалі. *D-Link ANT24-0800* поставляється з кабелем-перехідником, що дозволяють підключати антену до бездротових пристроїв з реверсним розніманням *Sma-rp-plug*. Комплект поставки містить у собі набір кріплення, модуль грозового захисту й заземлення, кабель-перехідник. Корпус антени стійкий до погодних явищ, що дозволяє використовувати її не тільки усередині приміщень. Антена також має шарнірне з'єднання, що дозволяє точніше настроїти кут нахилу антени для гарного приймання.

Додаток Д.

Основи передачі QAM

QAM – (Quadrature Amplitude Modulation – Модуляція методом Квадратичних Амплітуд) – це технологія передачі цифрового інформаційного потоку у вигляді аналогового сигналу. Це досягається шляхом поділу несучої хвилі на дві несучі однакової частоти зрушені відносно друг-друга на 90 про, кожна з яких промодулирована по одному із двох або більш дискретних рівнів амплітуди. Комбінація всіх рівнів амплітуди на цих дві несучі являє собою бінарну бітову картину.

I і **Q** компоненти – це дві половини бітової картини цифрового потоку передані одночасно, як рівні напруги двох ідентичні частотні несучі зрушених на 90°. Компонента **I** (incident) модулює несучу без зрушення фази. Компонента **Q** (quadrature) модулює несучу зі зрушенням 90 про (дивися Рисунок Д1).

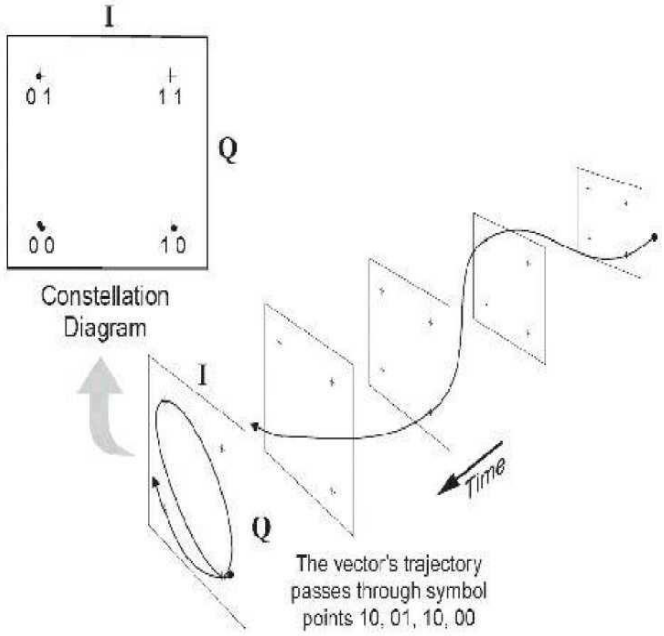


Рисунок Д.1 – Констеляційна діаграма відображаюча I /Q вектор

Траєкторія вектора, описуючи криву в часі, проходить через точки 10, 01, 10, 00.

QPSK - (**Quadraturephaseshiftkeying**- Кодування методом Квадратичного Фазового Зсуву) – це найпростіша форма **QAM** (також відома як **4-QAM**). **QPSK** використовує дві несучі однакової частоти, зрушені на 90 ^{про}, і два можливі рівні амплітуди. Один рівень амплітуди відповідає 0, інший – 1 (рисунок Д.1).

Констеляційна **діаграма** (або діаграма-сузір'я) – це карта, або квадратна матриця, у якій рівні амплітуди **I** і **Q** компонент **QAM** сигналу відображені у вигляді значущих точок у квадратній системі координат**I** і **Q.**

Координата **I** визначає горизонтальну позицію точки, а **Q** – вертикальну (рис. Д.2). Констеляційна діаграма в цій матриці утворюється з горизонтальних і вертикальних ліній (будь то промальованих або ж просто уявлюваних) з'єднуючих можливі значення компонентів **I** і **Q**. Цілочислене значення кожної отриманої точки визначається осередком матриці в яку вона попадає. Помилка визначається як випадання вимірюваної точки з осередка.

16-QAM діаграма – це 4X4 матриця, у якій кожна з 16 осередків представляє одну з 16 можливих бінарних комбінацій. Вертикальне й горизонтальне положення кожної точки відповідає **I** і **Q** рівням амплітуди сигналу переданого протягом одного циклу. **64-QAM** діаграма представлено на рисунку Д.2.

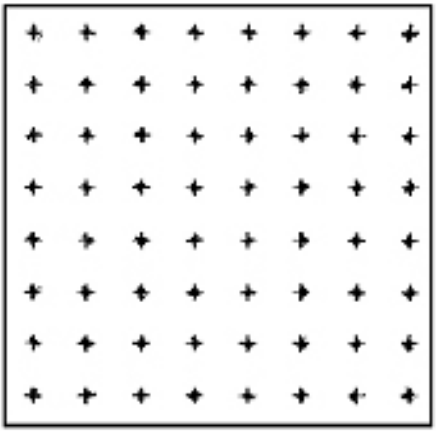


Рисунок Д.2 – 64-QAM Констеляційна діаграма

Аналіз Констеляційної діаграми QAM

Зовнішній вигляд значущих точок у осередках констеляційної діаграми може дати ключову інформацію про те що відбувається при передачі сигналу. Далі наведено перелік типових діаграм і відповідний їм діагностика.

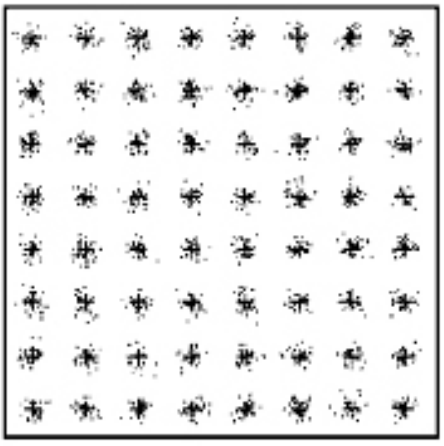


Рисунок Д.3 – 64-QAM Констеляційна діаграма при поганому відношення Сигнал/Шум

При поганому відношенні Сигнал/Шум – картинка поки відмінна, але подальша деградація сигналу приведе до повної втрати картинки. Розпливчастий образ точки займає практично весь осередок.

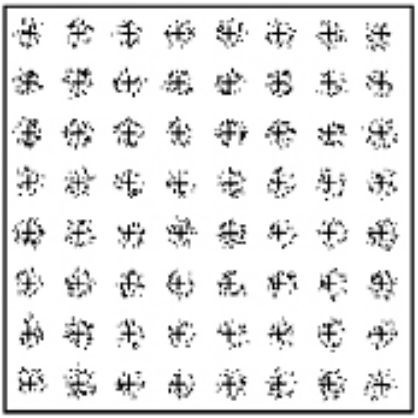


Рисунок Д.4 – Інтермодуляційна картина 64-QAM Констеляційна діаграма(«шуми інгресії»)

Інтермодуляційна картина («шуми інгресії») отримується через когерентний шум у кожному осередку утворюються концентричні картинки.

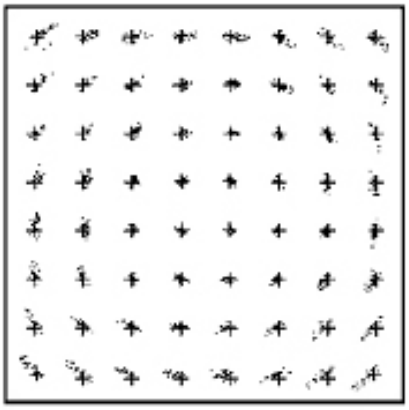


Рисунок Д.5 – 64-QAM Констеляційна діаграма

Фазовий Зсув

Фазовий Зсув – виникає через залишкові радіочастотні перешкоди, які звичайно є проблемою головного встаткування. Точки в осередках перекручені в такий спосіб що виникає візуальний ефект сферичної симетрії щодо центру діаграми.

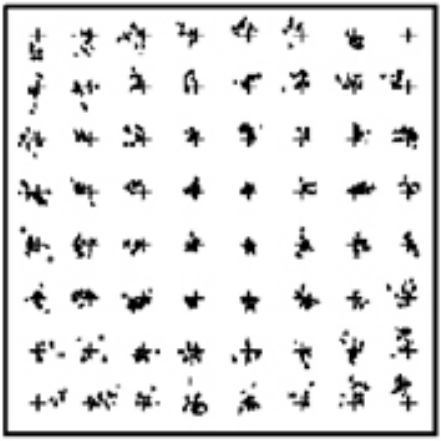


Рисунок Д.6 – 64-QAM Констеляційна діаграма. Вплив Нелінійності амплітудної характеристики

Нелінійність амплітудної характеристики – викликана нелінійністю проміжних і високочастотних підсилювачів, фільтрів, конвертерів і еквалайзерів. Точки зміщені щодо центру осередка по осях **I** і **Q** пропорційно відстані осередка від центру діаграми.

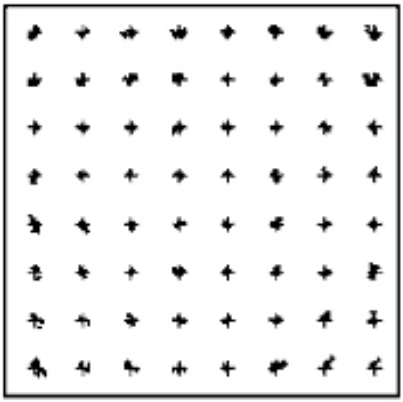


Рисунок Д.7 – 64-QAM Констеляційна діаграма.
IQ нестабільність

IQ нестабільність – пов'язана із проблемами підсилювачів несучої частоти, фільтрів і цифрових модуляторів головних станцій.

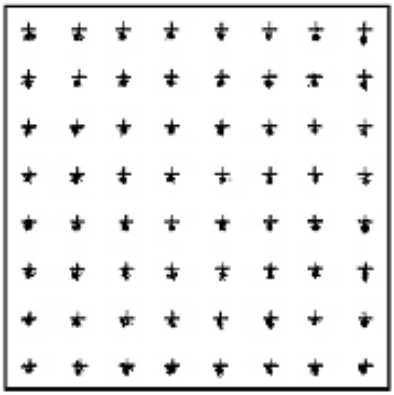


Рисунок Д.8 – 64-QAM Констеляційна діаграма.
Відхилення несучої

Відхилення несучої - є наслідком дисбалансу в змішувачі модулятора або наявності паразитного постійного струму в системі передачі. Уся картинка зміщена в одному напрямку.

Вимоги до відношення Сигнал/Шум при високій швидкості передачі

Переваги високих значень номера QAM – це підвищена швидкість передачі даних, оскільки в такий спосіб більша кількість бітів інформації може бути передано протягом одного циклу. Однак, з іншого боку, у цьому випадку більше число рівнів амплітуди сигналу розташовуються близько один до одного, підвищуючи тим самим імовірність нерозрізненості двох рівнів, і як наслідок – підвищуючи чутливість системи до шуму. Таким чином, високі значення номера QAM більш вимогливі до параметра CNR (Carrier Noise Ratio – Відношення Сигнал/Шум). На малюнку 3 представлене відношення параметра CNR до іншого параметра – BER (Bit Error Rate – Відношення Біт/Помилка)

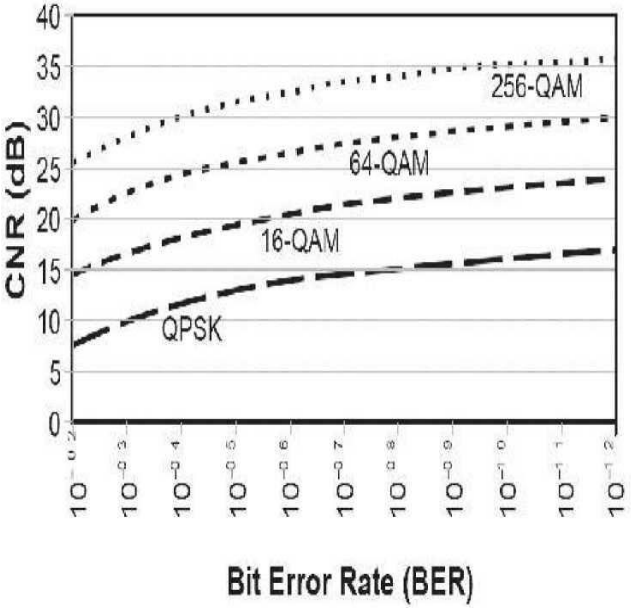


Рисунок Д.9 – Відношення CNR до BER

BER, NPR, FEC, MER

BER (Bit Error Rate – Відношення Біт/Помилка) – це підрахунок неправильно отриманих бітів інформації. Якщо точніше – це кількість помилково прийнятих бітів розділене на загальну кількість переданих бітів. Воно може бути виражене й у дБ, але звичайно виражається у форматі 10 – X. Наприклад, 10 – 9 означає що один помилковий біт був прийнятий у при одержанні потоку інформації обсягом в 1 мільярд бітів.

NPR (Noise Power Ratio – Відношення Шум/Потужність) це технологія виміру співвідношення Сигнал/Шум в аналогових пристроях, що працюють у режимах QAM або QPSK. Оскільки ці режими мають частотний спектр у вигляді Гаусового шуму, NPR-тест проводиться шляхом підміни сигналу еквівалентною смугою білого шуму. Ближче до середини смуги ця шумова «засічка» (звичайно 4 МГц) опускається. Коли смуга шуму пускається через пристрій, глибина «засічки» визначається декількома факторами: термічним шумом, «шумоподобными продуктами» сигналу й т.п. (дивися Рис. Д10).

Typical NPR Curve

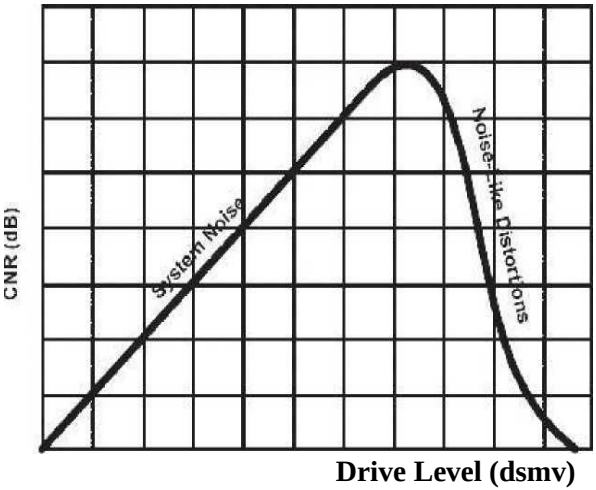


Рисунок Д.10 – Типовий вид кривій NPR

FEC (Forward Error Correction – Упереджувальна Корекція Помилок) – це програмна технологія для визначення й усунення помилок у цифровій передачі даних. Це складне й затратомістке (по потужності процесора), однак необхідне завдання – упереджати втрату бітів інформації, що дозволяє поліпшити якість картинки.

MER (Modulation Error Ratio – Відношення Модуляція/Помилка) – це величина відхилення отриманої модуляції (по амплітуді й/або фазі) від переданої (рис. Д.11).

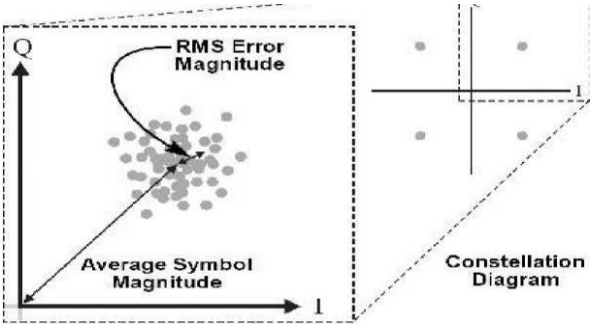


Рисунок Д.11 – Визначення MER

При збільшенні MER до величини при якій точки попадають на границі осередка або за них, BER різко зростає. Далі, коли BER перевищить здатність FEC коректувати помилки, відбудеться збій передачі. Практично на точці зриву, якість картинки усе ще буде відмінною, не передвіщаючи збій, що наближається. Це явище відоме як «ефект зриву», коли всі добре аж до того. Це характерна складність для **J** непередбаченого моменту, коли все вже погано цифрової передачі – коли ви дивитеся на картинку, неможливо знати коли відбудеться зрив.

Додаток Е.

Метод OFDM

Вивчаючи теорію технологій бездротових мереж доступу або мереж стільниковому зв'язка, неминуче, так чи інакше, можна зіштовхнутися з такою абревіатурою, як OFDM.OFDM (англ. *Orthogonal frequency-division multiplexing*) – мультиплексування з ортогональним частотним поділом каналів, є цифровою схемою модуляції, яка використовує велику кількість близько розташованих ортогональних, що піднесуть. Кожна, що піднесе модулюється за звичайною схемою модуляції (наприклад, квадратурна амплітудна модуляція) на низькій символьній швидкості, зберігаючи загальну швидкість передачі даних, як і у звичайних схем модуляції однієї несучої в тій же смузі пропущення. На практиці сигнали OFDM виходять шляхом використання ШПФ (швидке перетворення Фур'є)".

Думаю після прочитання даного пояснення для більшості читачів тема OFDM як була незрозумілої, так їй і залишилася. Це не дивно, оскільки при описі використовуються досить нетривіальні й непрості терміни. Рядовий читач запитає, що це ще за ортогональний частотний поділ каналів? Той, хто хоча б частково знаком зі спектральним аналізом може здивуватися, звідки тут узялося швидке перетворення Фур'є?

Коротка біографія OFDM

Паралельна передача даних із частотним поділом була придумана ще в середині 60-х років минулого століття й використовувалася, як і більшість відомих сьогодні технологій, спочатку тільки у військових системах. У ті часи військові, використовуючи OFDM, уже здійснювали паралельну передачу даних з використанням 34, що піднесуть.

В 1980-х стали розглядати застосування OFDM у комерційних системах: у першу чергу у високошвидкісних модемах і цифрових мобільних мережах. В 1990-х OFDM модуляцію стали використовувати в цифровому радіомовленні (DAB), у наземному телемовленні, при передачі відео високої

чіткості HDTV, а також у відомих технологіях останньої милі ADSL, HDSL.

Довгий час OFDM не знаходила досить широкого поширення в інших системах зв'язку через складну технічну реалізацію. Розв'язок завдання формування OFDM сигналу аналоговими методами досить проблематично. Розвиток обчислювальних систем і методів цифрової обробки сигналів дозволяє застосовувати сьогодні OFDM модуляцію у всіляких системах – від радіо до провідних ліній і навіть волоконно-оптичних.

У чому ж зміст OFDM?

Незважаючи на те, що метод дослівно розшифровується як мультиплексування з ортогональним частотним поділом, його все-таки в першу чергу відносять до методів цифрової модуляції. Справа в тому, що метод OFDM використовує одночасно й модуляцію й мультиплексування, але мультиплексування особливе. Звичайне мультиплексування має на увазі об'єднання різних сигналів від різних джерел, тут же відбувається об'єднання складових частин того самого сигналу.

Постараємося пояснити все на простому прикладі. Представте, що нам треба передати з одного пункту в інший скляний вітраж. Для цього в нашому розпорядженні є деякий ресурс, допустимо 4 візка (у випадку передачі інформації як ресурсу можна було б уважати доступний для передачі діапазон частот).

У випадку OFDM ми розбираємо наш скляний вітраж на деяку певну кількість частин, для прикладу нехай їх буде 4. Далі кожний візок перевозить свою частину посилки (вітража), при цьому візки котяться одночасно паралельно один одному. Допустимо на шляху в нас зустрічається одна перешкода у вигляді каменю (у випадку передачі інформації – вузькополосна перешкода). Одна з візків наїжджає на камінь, відповідно одна із частин посилки не доходить до пункту приймання.

Однак більша кількість частин вітража все-таки була коректно отримане, тому за допомогою інтуїції й чарівництва

(завадостійкого кодування), їсти шанс відновити відсутню в результаті падіння одному візка частина посилки.

Як би все було, не застосовуючи OFDM? При традиційному підході для найшвидшої передачі всієї посилки ми також задіємо всі доступні ресурси, але будемо транспортувати вітраж цілком на всіх 4 візках (використовуємо високошвидкісний метод модуляції, що займає всю смугу каналу). Допустимо, на шляху в нас також зустрічається одна перешкода у вигляді каменю. У результаті одна з візків наїжджає на камінь, вітраж падає й розбивається вщент.

Алгоритму, по якому в цьому випадку розпався на частині наш вітраж, ми не знаємо, тому зібрати по шматочках заново ми його не можемо. Підсумок: цілий вітраж не доїхав до пункту приймання (загублений чималий обсяг даних, тут навіть завадостійке кодування нас не врятує). Таким чином, можна сказати, що один з основних девізів OFDM: «не треба класти всі яйця в один кошик».

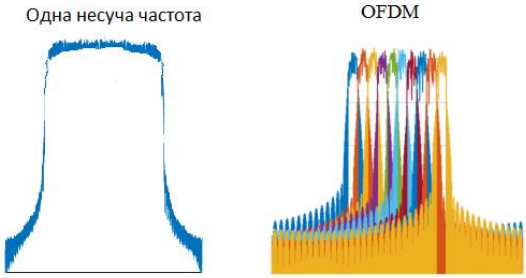


Рисунок Е.1 – Частотний спект сигналу з однією несучою та OFDM

Однієї з особливістю OFDM є те, що всі візки можуть рухатися паралельно практично впритул і при цьому не заважати один одному. При передачі інформації роль візків виконують сигнали, що піднесуть, тобто безліч несучих коливань (якщо забули, що це таке, почитайте в будь-якому підручнику основи модуляції). Згадаємо фільм Термінатор 2 і представимо, що візки зроблені з рідкого металу. У зв’язку із цим навіть якщо при русі

шляху візків частково перекриваються, вони не заважають один одному, комфортно співіснують разом і рухаються далі. Існує аналогічний ефект стосовно передачі сигналів – ортогональність сигналів. Звичайно для пояснення терміна ортогональність сигналів приводять інтегральне математичне вираження. Однак оскільки була дана обіцянка пояснювати все на пальцях, можна просто усвідомити наступне. Ортогональні сигнали мають чудову властивість – їх взаємна енергія дорівнює нулю. Ортогональність, що піднесуть дозволяє на прийманні виділити кожну з них із загального сигналу навіть у випадку часткового перекриття їх спектрів. Оскільки, що піднесуть розташовуються впритул друг до друга й навіть частково накладаються один на одного (рис. Е.2) спектральна ефективність модульованого OFDM сигналу виходить високої.

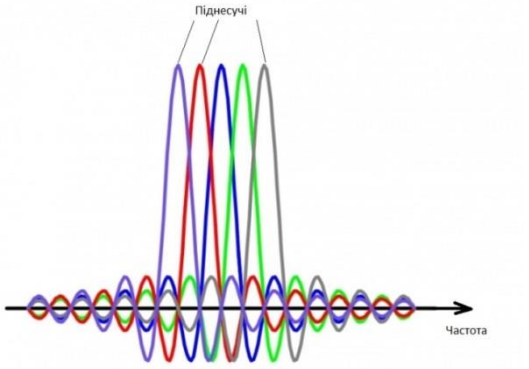


Рисунок Е.2 – Зображення піднесучіх на частотній осі

Як видне з малюнка кожна піднесуча представлена окремим піком. Зверніть увагу, що в точці піка кожної піднесучої має значення, а інших піднесучіх дорівнює нулю. На осі часу кожної кривій відповідає свій модульований сигнал. Сума всіх цих сигналів дає складний за формою OFDM-сигнал.

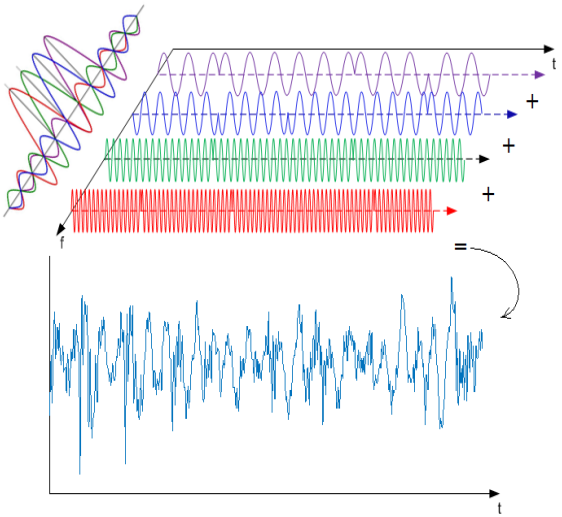


Рисунок Е.3 – Зображення піднесучіх на осяхчастоти та часу

Параметри сигналів, що піднесуть (наприклад, синусоїди) підбираються таким чином, щоб вони були по відношенню одне до одного ортогональні. Для швидкої реалізації даного дії за допомогою обчислювальних пристроїв використовують алгоритм зворотного швидкого перетворення Фур'є (ЗШПФ). Тобто ми навмисно представляємо, що значення сигналу перед блоком ЗШПФ ставляться до частотної області. Тоді на виході блоку ЗШПФ ми одержуємо значення сигналу на осі часу. Поєднуючи всі значення, ми одержуємо складний складовий OFDM сигнал.

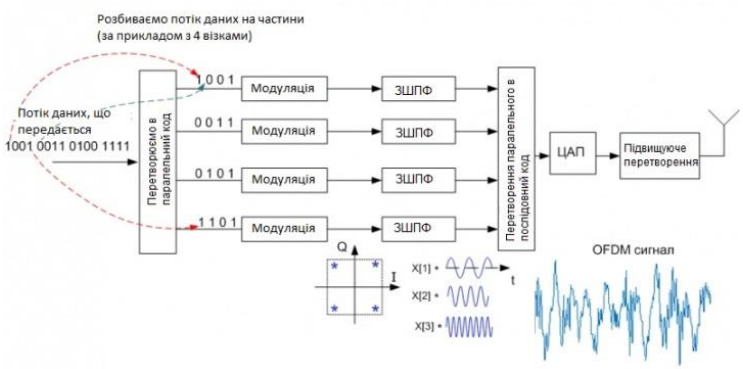


Рисунок Е4 – Схема перетворень з використанням ЗШПВ

Важливо відзначити, що в даній спрощеній схемі представлені не всі блоки, наявні в реальних системах з OFDM. Тут для спрощення схеми не наведені блоки додавання захисних біт і циклічного префікса, що є невід'ємною частиною технології.

Враховуючи те, що ЗШПВ працює ефективно з масивами розмірності 2k, кількість, що піднесуть вибирається аналогічної кратності. Наприклад, в Wimax число, що піднесуть вибирається від 128 до 2048 і може займати смуги частот від 1,25 Мгц до 20 Мгц (Таблиця Е.1).

Таблиця Е.1 – Відповідність числа піднесучих до ширини каналу

Ширина каналу	Число піднесучих
1,25 МГц	128
2,5 МГц	256
5 МГц	512
10 МГц	1024
20 МГц	2048

Для кожної з, піднесучих використовується свій формат модуляції залежно від вимог і величини перешкод у каналі.

На прийомному кінці всі блоки наведеної вище схеми інвертуються(замість ЦАП ставиться АЦП, замість зворотного ШПФ – пряме ШПФ) і ставляться у зворотному порядку.

У чому ж полягає родзинка OFDM, що обумовило його популярність у всіх сучасних системах зв'язку?

Переваги OFDM:

– здатність протистояти складним умовам у радіоканалі, у першу чергу усувати міжсимвольну інтерференцію й боротися з вузькополосними перешкодами (як у прикладі ми втратили одну з візків і в наступні моменти часу можемо поки змінити даний шлях з перешкодою на іншій);

– висока спектральна ефективність. Якщо число, що піднесуть наближається до нескінченності, OFDM системи показують майже подвоєну спектральну ефективність у порівнянні із традиційними системами із частотним поділом каналів.

– адаптивність методу – можливість використання різних схем модуляції для різних, що піднесуть, що дозволяє адаптуватися до умов поширення сигналу й до різних вимог до якості прийнятого сигналу;

– проста реалізація методами цифрової обробки (стала простою з розвитком потужності обчислювальних пристроїв);

– здатність протистояти інтерференції між, що піднесуть, що обумовлює гарні показники при багатопроменевому поширенні.

Недоліки OFDM:

– потрібна високоточна синхронізація за часом і по частоті;

– OFDM сигнал має відносно високе значення пік-фактора, що приводить до надмірних енергетичних витрат;

– використання захисних інтервалів знижує спектральну ефективність методу;

– метод чутливий до ефекту Доплера, що накладає додаткові труднощі при його застосуванні в мобільних мережах.

Поточне застосування OFDM. На сьогоднішній день найбільш відоме застосування OFDM модуляції в бездротових системах зв'язку Wi-Fi, Wimax, LTE, у наземних системах

цифрового телебачення DVB-T, у системах кабельного телебачення DVB-C, у технології ADSL і це далеко не всі приклади.

Важливо відзначити, що тут були розглянуті тільки деякі основні моменти OFDM. Якщо ви прагнете розібратися в цій темі більш серйозно, то варто звернути увагу також на такі моменти як додавання циклічного префікса для усунення перешкод і боротьби із завмираннями, процедури тактової й фазової синхронізації, використання пілотних, що піднесуть і ін.

Додаток Ж
Модель OSI (The Open Systems Interconnection model)

Модель OSI (The Open Systems Interconnection model) – мережева модель стека (магазину) мережевих протоколів ISO/OSI. За допомогою цієї моделі різні мережеві пристрої можуть взаємодіяти один з одним. Модель визначає різні рівні взаємодії систем. Кожен рівень виконує певні функції при такій взаємодії. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання й програмного забезпечення може бути набагато простішою, прозорішою й зрозумілішою.

Однако, на даний час основним використовуваним стеком протоколів є TCP/IP, розробка якого не пов'язана з моделлю OSI і до того ж була здійснена до її прийняття. За увесь час існування моделі OSI вона не була реалізована, і, очевидно, не буде реалізована ніколи. Сьогодні використовується тільки деяка підмножина моделі OSI. Вважається, що модель занадто складна, а її реалізація візьме занадто багато часу.

Модель складається з семи рівнів, а саме *фізичний, канальний, мережевий, транспортний, сеансовий, представницький та прикладний рівні***,** кожен з яких взаємодіє між своїми сусідами й виконує лише функції, які йому відводиться. Так:

Фізичний рівень має справи з передачею бітів по фізичних каналах зв'язку, таким, як коаксіальний кабель, кручена пара, оптоволоконий кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, таку як крутість фронтів імпульсів, рівні напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів. Крім того, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня:

- передача бітів по фізичних каналах;

- формування електричних сигналів;
- кодування інформації;
- синхронізація;
- модуляція.

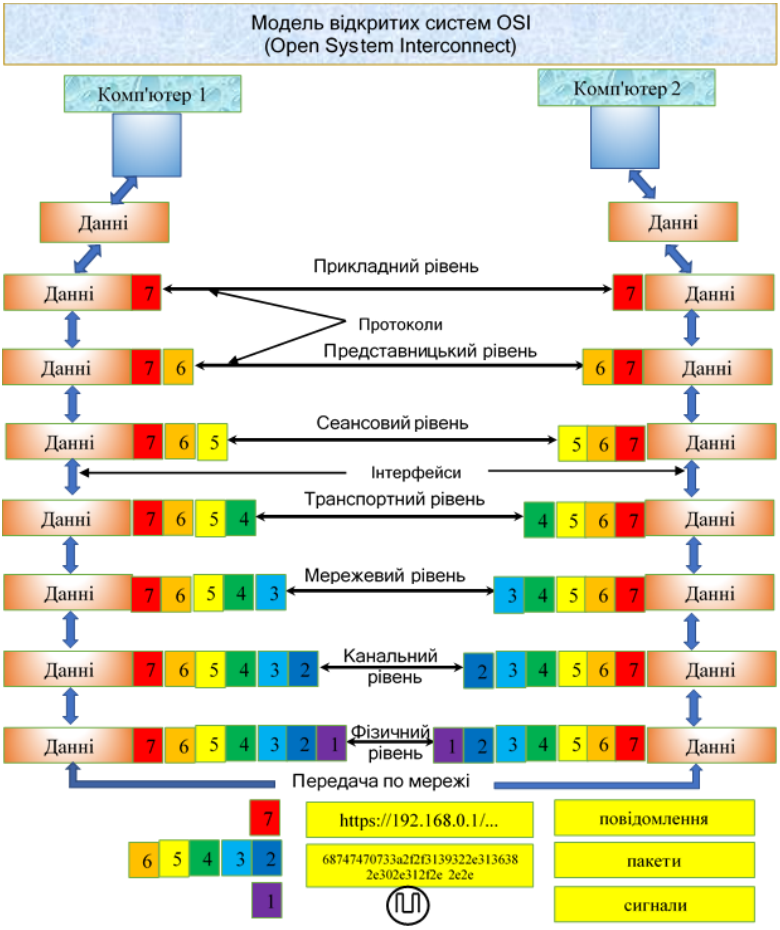


Рисунок Ж.1 – Модель взаємодії відкритих систем ISO/OSI

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп’ютера функції фізичного

рівня виконуються мережним адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 100Base-TX технології Ethernet, що визначає в якості середовища передачі даних неекрановану кручену пару категорії 5 із хвильовим опором 100 метрів, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, а також деякі інші характеристики середовища й електричних сигналів.

Для канального рівня характерні таке: на фізичному рівні просто пересилаються біти. При цьому не враховується, що в тих мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте.

Тому однієї із завдань канального рівня (Data Link layer) є перевірка доступності середовища передачі. Інше завдання канального рівня – реалізація механізмів виявлення й корекції помилок. Для цього на канальному рівні біти групуються в набори, називані кадрами (frames).

Канальний рівень забезпечує коректність передачі кожного кадру поміщаючи спеціальну послідовність біт у початок і кінець кожного кадру, для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом, і додає контрольну суму до кадру. Канальний рівень може не тільки виявляти помилки, але й виправляти їх за рахунок повторної передачі ушкоджених кадрів. Необхідно відзначити, що функція виправлення помилок для канального рівня не є обов'язкової, тому в деяких протоколах цього рівня вона відсутня, наприклад в Ethernet і Frame Relay.

Мережевий рівень (Network layer) служить для утворення єдиної транспортної системи, що поєднує кілька мереж, причому ці мережі можуть використовувати зовсім різні принципи передачі повідомлень між кінцевими вузлами й мати довільну структуру зв'язків. Функції мережного рівня досить різноманітні.

На мережевому рівні сам термін мережа наділяють специфічним значенням. У цьому випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних типових топологій і, що

використовують для передачі даних один із протоколів канального рівня, певний для цієї топології.

Повідомлення мережевого рівня прийнято називати пакетами (packets). При організації доставки пакетів на мережному рівні використовується поняття «номер мережі». У цьому випадку адреса одержувача складається зі старшої частини – номера мережі й молодшої – номера вузла в цій мережі. Всі вузли однієї мережі повинні мати ту саму старшу частину адреси, тому терміну «мережа» на мережному рівні можна дати й інше, більше формальне визначення: мережа – це сукупність вузлів, мережна адреса яких містить той самий номер мережі.

На мережному рівні визначаються два види протоколів:

- мережеві протоколи (routed protocols) – реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережного рівня. Однак часто до мережного рівня відносять і інший вид протоколів, називаних протоколами обміну маршрутною інформацією або просто протоколами маршрутизації (routing protocols);
- протоколи вирішення адрес – Address Resolution Protocol, ARP, які відповідають за відображення адреси вузла, використовуваного на мережному рівні, у локальну адресу мережі.

Прикладами протоколів мережевого рівня є протокол міжмережної взаємодії IP стека TCP/IP і протокол межмережевого обміну пакетами IPX стека Novell.

Транспортний рівень забезпечує додаткам або верхнім рівням стека – прикладному й сеансовому – передачу даних з тим ступенем надійності, що їм потрібно. Модель OSI визначає п’ять класів сервісу, надаваних транспортним рівнем. Ці види сервісу відрізняються якістю надаваних послуг: терміновістю, можливістю відновлення перерваного зв’язку, наявністю засобів націлити декількох з’єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення й виправлення помилок передачі, таких як перекручування, втрата й дублювання пакетів.

Основні завдання транспортного рівня:

- розбивка повідомлення сеансового рівня на пакети, їхня нумерація;
- буферизація прийнятих пакетів;
- впорядочення пакетів, що прибувають;
- адресація прикладних процесів;
- керування потоком.

Як правило, всі протоколи, починаючи із транспортного рівня й вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережних операційних систем. Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Сеансовий рівень (Session layer) забезпечує керування діалогом: фіксує, яка зі сторін є активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у випадку відмови можна було повернутися назад до останньої контрольної точки, а не починати все спочатку. На практиці деякі додатки використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто поєднують із функціями прикладного рівня й реалізують в одному протоколі.

Основні завдання сеансового рівня:

- встановлення способу обміну повідомленнями (дуплексний або напівдуплексний);
- синхронізація обміну повідомленнями;
- організація «контрольних точок» діалогу.

Представницький рівень (Presentation layer) має справу з формою подання переданої по мережі інформації, не міняючи при цьому її змісту. За рахунок рівня подання інформація, передана прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть перебороти синтаксичні розходження в поданні даних або ж розходження в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування й дешифрування даних, завдяки якому таємність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол

Secure Socket Layer (SSL), що забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Основні завдання представницького рівня:

- перетворення даних із зовнішнього формату у внутрішній;
- шифрування й розшифровка даних.

Прикладний рівень – це в дійсності просто набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ ресурсів, що розділяються, таким як файли, принтери або гіпертекстові Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, який оперує прикладний рівень, звичайно називається повідомленням (message).

Основні завдання прикладного рівня:

- ідентифікація, перевірка прав доступу;
- принт–і файл–сервіс, пошта, вилучений доступ і т.д.

Найпопулярнішим стеком протоколів комунікації через розповсюдження Інтернету є стек TCP/IP. Цей стек є вихідним з операційних систем Unix та Linux, а також є основним стеком для систем Windows. Приклади інших окулярів протоколів зв'язку можна назвати стек IPX/SPX, розроблений Novell та NetBiOS/SMB, розробленими спільно IBM та Microsoft. Слід зазначити, що стек протоколів зв'язку зазвичай включають не всі рівні моделі OSI (часто немає сеансового рівня та рівня подання даних).

Крім моделі OSI, існує також модель IEEE Project 802, прийнята в лютому 1980 року (звідси й число 802 у назві), яку можна розглядати як модифікацію, розвиток, уточнення моделі OSI. Стандарти, обумовлені цією моделлю (так звані 802-специфікації), діляться на дванадцять категорій, кожної з яких привласнений свій номер:

- 802.1 – об'єднання мереж.
- 802.2 – керування логічним зв'язком.
- 802.3 – локальна мережа з методом доступу CSMA/CD і топологією «шина» (Ethernet).

- 802.4 – локальна мережа з топологією «шина» і маркерним доступом.
- 802.5 – локальна мережа з топологією «кільце» і маркерним доступом.
- 802.6 – міська мережа (Metropolitan Area Network, MAN).
- 802.7 – широкомовна технологія.
- 802.8 – оптоволоконна технологія.
- 802.9 – інтегровані мережі з можливістю передачі мови й даних.
- 802.10 – безпека мереж.
- 802.11 – бездротова мережа.
- 802.12 – локальна мережа із централізованим керуванням доступом по пріоритетах запитів і топологією «зірка» (100VG–AnyLAN).

Стандарти 802.3, 802.4, 802.5, 802.12 прямо ставляться до підрівню MAC другого (канального) рівня еталонної моделі OSI. Інші 802—специфікації вирішують загальні питання мереж.

ГЛОСАРІЙ

801.11 – стандарт *IEEE*, у якому визначається порядок доступу до передавального середовища й приводяться специфікації фізичного рівня для бездротових локальних мереж зі швидкістю до 2 Мбит/с. Стандарт *802.11* поширюється на високочастотні радіоканали *DSSS* і *FHSS*, а також на інфрачервоні канали.

802.11a – редакція стандарту *802.11 IEEE*, у якій розглядаються мережі, що працюють зі швидкостями до 54 Мбит/із за технологією *DSSS*.

802.11b – редакція стандарту *802.11 IEEE*, у якій розглядаються мережі, що працюють зі швидкостями до 11 Мбит/із за технологією *DSSS*.

802.11g – редакція стандарту *802.11 IEEE*, у якій розглядаються мережі, що працюють зі швидкостями до 54 Мбит/із за технологією *DSSS*, назад сумісні зі стандартом *802.11b*.

802.11i – стандарт *IEEE*, що ставиться до безпеки бездротових мереж. У ньому об'єднані протоколи 802.1x і *TKIP*/CCMP, що дозволяє забезпечити автентифікацію користувачів, *конфіденційність* і *цілісність* даних у бездротових локальних мережах.

802.1x – стандарт *IEEE* автентифікації й контролю доступу на канальному рівні.

Access point (*точка доступу*) – тип базової станції, яку бездротова локальна *мережа* використовує для забезпечення взаємодії бездротових користувачів із провідною мережею й здійснення роумінгу в межах будинку.

Ad Hoc mode (режим *одноранговой мережі*) – *конфігурація* бездротової мережі, при якій користувачі можуть безпосередньо встановлювати з'єднання між своїми пристроями, обходячись без послуг базової станції. У цьому режимі можуть працювати бездротові персональні й *локальні мережі*.

Autentificator (Автентифікатор) – у протоколі 802.1x посередник між сервером автентифікації, наприклад *RADIUS*, і претендентом. У бездротових мережах звичайно розміщається на

крапці доступу; у провідних мережах цю функцію можуть виконувати висококласні комутатори.

Bluetooth – частина специфікації *802.15* для бездротових персональних мереж, розроблена й підтримувана групою *Bluetoothsig*, яка була заснована компаніями Ericsson, Nokia, *IBM*, Intel і Toshiba.

BSS (Basic Service Set) (Базовий набір служб) – *базова* сота в мережі *802.11*, що полягає з однієї точка доступу клієнтів, що й приєдналися до неї.

CCMP (Counter Mode with CBC MAC) – заснований на алгоритмі *AES* протокол шифрування, який повинен замінити *WEP* і *TKIP*. Уважається обов'язковим у специфікації *WPA* версії 2.

CDMA (Code Division Multiple Access) – *множинний доступ* з кодовим *поділом каналів*. Процес, при якому кожний *користувач* модулює свої сигнали відмінним від інших кодом щоб уникнути виникнення взаємних перешкод.

Clear-To-Send (CTS) (Готовий до передачі) – керуючий *фрейм* у стандарті *802.11*, застосовуваний для виявлення віртуальної несучої. *Фрейм CTS* посилає у відповідь на *фрейм RTS*. Він дозволяє запитуючому хосту передавати дані протягом часу, зазначеного в *поле Network Allocation Vector*.

CRC (Cyclic Redundancy Check) (Код циклічної надмірності) – основний математичний *алгоритм* обчислення контрольної суми для перевірки цілісності переданих даних. Часто обчислюється шляхом розподілу довжини фрейму на *просте число*, легко може бути змінений супротивником.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) – протокол другого рівня, застосовуваний для усунення колізій у мережах *802.11* із множинним доступом з *контролем несучої*. Станції тільки тоді намагаються здійснити передачу, коли цього не робить жодна інша станція мережі. А якщо ні, то відбувається *колізія*, і станції доводиться повторно передавати дані.

dbi – децибели, віднесені до ідеальної ізотропної антени.

db – децибели, віднесені до напівхвильового диполя.

DCF (Distributed Coordination Function) – *розподілена функція* координації. Частина стандарту *802.11*, що визначає, як станції повинні конкурувати за *право доступу* до середовища передачі. Для регулювання трафіка мережі *DCF* використовує технологію *CSMA*.

DSSS (Direct Sequence Spread Spectrum) – один із двох підходів до передачі радіосигналів зі змінюваним спектром. При використанні технології *DSSS потік* переданих даних розбивається на невеликі шматочки, кожному з яких виділяється широкосмуговий канал. На передавальному кінці інформаційний сигнал комбінується з послідовністю бітов, переданих з більш високою швидкістю, яка розділяє дані відповідно до коефіцієнта зміни.

EAP (Extensible Authentication Protocol) – гнучкий протокол автентифікації, спочатку спроектований для автентифікації в протоколі PPP, а пізніше включений у стандарт 802.1x.

EAPOL (EAP over LAN EAP) – інкапсуляції фреймів протоколу EAP у провідних локальних мережах. Визначається окремо для *Ethernet* і *Token* Ring.

EIRP (Ефективна ізотропно випромінювана *потужність*) – реальна вихідна *потужність*, випромінювана антеною, що розраховується як IR + коефіцієнт підсилення антени.

ESSID (Extended Service Set ID) – ім'я, що ідентифікує *мережа 802.11*. Щоб приєднатися до бездротової локальної мережі, потрібно знати її ESSID.

ETSI (European Telecommunications Standards Institute) – Європейський інститут стандартів телекомунікацій, некомерційна організація, що випускає стандарти й правила в області телекомунікацій для всієї Європи.

FDMA (Frequency Division Multiple Access) – *множинний доступ* із частотним поділом. Процес, у ході якого відносно широкий частотний *діапазон* ділиться на вузькі піддіапазони. Кожний *користувач* передає мову й дані у виділеному для нього піддіапазоні.

FHSS (Frequency Hopping Spread Spectrum) – зміна спектра стрибкоподібною перебудовою частоти). Один із двох підходів до передачі радіосигналу зі змінюваним спектром. Характеризується тим, що несуча частота псевдовипадковим образом «скаче» у межах певного діапазону.

FSK (Frequency Shift Keying) – частотна маніпуляція. Процес модуляції, при якому злегка змінюється частота несучого сигналу, за рахунок чого здійснюється *вистава* інформації способом, що підходять для її передачі через повітряне середовище.

ICV (Integrity Check Value) (Код контролю цілісності) – проста *контрольна сума*, що обчислюється для фрейму *802.11* перед початком шифрування по протоколу *WEP*.

IV (Initialization Vectors) (*Вектор* ініціалізації) – додаткові несекретні двійкові дані для шифрування відомого або передбачуваного відкритого тексту з метою введення додаткової криптографічної мінливості. Крім того, вектори ініціалізації використовуються для синхронізації криптографічного встаткування.

Hotspot («гаряча точка») – *місце*, де розгорнута загальнодоступна бездротова локальна *мережа*. «Гарячі точки» розташовуються в зонах, де може перебувати великий кількість людей з комп'ютерними пристроями, – таких як аеропорти, готелі, палаци з'їздів і кафе.

MIC (Message Integrity Check) (Код цілісності повідомлення) – *алгоритм*, використовуваний у стандарті 802.11i для забезпечення автентифікації й цілісності пакетів.

OFDM (Orthogonal Frequency Division Multiplexing) – *мультиплексування* з поділом по ортогональних частотах. Процес, у ході якого сигнал перед передачею через повітряне середовище розподіляється по багатьом, що піднесуть. Використовується з метою підвищення характеристик бездротових локальних мереж стандартів 802.11a й *802.11g* і в деяких патентованих бездротових регіональних мережах.

Point-To-Multipoint System (система типу «точка – кілька точок») – система, що дозволяє одному користувачеві прямо зв'язуватися з декількома іншими.

Point-To-Point System (система типу «точка-*точка»*) – система, у якій *зв'язок* між двома користувачами здійснюється прямо.

Point-To-Point Tunneling Protocol (PPTP) (Двоточковий тунельний протокол) – дуже широко розповсюджений тунельний протокол, запатентований Microsoft.

PSK (Phase Shift Keying) – фазова *модуляція*. Процес модуляції, при якому для вистави інформації використовуються невеликі зміни фази несучої, у результаті чого можлива *передача даних* через радіоефір.

PSK (Pre Shared Key) (Режим з попереднім *розподілом ключів*) – описаний у специфікації *WPA* режим забезпечення безпеки, заснований на попередньому розміщенні ключів на всіх хостах, що мають *доступ* до бездротової локальної мережі. Застосовується в тих випадках, коли *розподіл ключів* по протоколу 802.1x неможливо.

QAM (Quadrature Amplitude Modulation) – квадратурна амплітудна *модуляція*. Процес модуляції, при якому для вистави інформації використовуються невеликі зміни фази й амплітуди несучої, у результаті чого *передача даних можлива* через радіоефір.

RADIUS (Remote Authentication Dial-In User Service) – служба дистанційної автентифікації користувачів по лініях, що комутируються. Система автентифікації й обліку, яку багато постачальників послуг широкосмугового доступу до *Internet* використовують для керування доступом до *Internet* і виписки рахунків за користування бездротовою мережею.

Request-To-Send (RTS) (*Запит* на передачу) – тип керуючого фрейму в стандарті *802.11*, застосовується в механізмі виявлення віртуальної несучої. Якщо такий механізм використовується в мережі *802.11*, то станція, що бажає відправити дані, повинна попередньо послати *фрейм RTS*.

Spanning Tree Protocol (STP) (Протокол покриваючого дерева) – певний у стандарті 802.*Id* протокол рівня 2, що дозволяє уникнути зациклення в мережах з декількома комутаторами й надлишковими з'єднаннями.

Supplicant (Претендент) – у протоколі 802.1x клієнтський пристрій, що бідує в автентифікації.

TDMA (Time Division Multiple Access) *множинний доступ* з тимчасовим *поділом каналів*. Процес, що дозволяє тільки одному користувачеві здійснювати передачу в даний проміжок часу. Кожний *користувач* займає всю смугу каналу протягом виділеного для нього тимчасового інтервалу.

TKIP (Temporal Key Integrity Protocol) (Протокол цілісності тимчасових ключів) – заснований на алгоритмі *RC4* протокол шифрування, який урятований від багатьох слабостей оригінального статичного протоколу *WEP*. Протокол *TKIP* – це необов'язкова частина стандарту 802.11i. Він назад сумісний з *WEP* і не вимагає заміни встаткування.

VPN (Virtual Private Network) – віртуальна приватна *мережа*, що використовує спеціальне *програмне забезпечення* на клієнтському пристрої, який управляє доступом до віддалених додатків і забезпечує *безпека* з'єднання за рахунок наскрізного шифрування.

WDS (Wireless Distribution System) (Бездротова розподілена система) – елемент бездротової системи, що полягає із взаємозалежних базових наборів служб, які утворюють розширений набір служб.

WEP (Wired Equivalent Privacy) – у стандарті *802.11* необов'язковий механізм забезпечення безпеки, у якому для шифрування трафіка в бездротовій мережі застосовується *алгоритм RC4*.

Wi Fi (Wireless Fidelity) – процедура сертифікації, розроблена організацією Wi-Fi Alliance, яка гарантує можливість спільної роботи різних продуктів, що реалізують стандарт *802.11*.

Wi-Fi Protected Access (WPA) – захищений *доступ* до Wi-Fi. Протокол безпеки, певний Альянсом Wi-Fi, що дозволяє комп'ютерним пристроям періодично одержувати нові ключі шифрування. В *WPA* версії 1 застосовуються тимчасовий протокол цілісності ключа *TKIP* і *WEP*; в *WPA* версії 2 використовується стандарт 802.11i, що включає *AES*.

WLAN (Wireless Local Area Network) (Бездротова локальна *мережа*) – *локальні мережі* стандарту *802.11*.

АВТОРИ

БЄДНЯК Олег Григорійович – завідувач навчальною лабораторією комп'ютерних систем і мереж Національного університету «Запорізька політехніка».

ВОСКОБОЙНИК Володимир Олександрович – кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки і наноелектроніки Національного університету «Запорізька політехніка».

САВЧЕНКО Юрій Володимирович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів.

ТІМЕНКО Артур Валентинович – старший викладач кафедри комп'ютерних систем і мереж Національного університету «Запорізька політехніка».

КІЦЕЛЬ Наталія Василівна – науковий співробітник відділу організації наукової діяльності Кременчуцького льотного коледжу Харківського національного університету внутрішніх справ.

ШАПОВАЛ Олександр Олександрович – доктор технічних наук, професор, професор кафедри машинобудування Кременчуцького національного університету імені Михайла Остроградського.

Наукове видання

БЄДНЯК Олег Григорійович
САВЧЕНКО Юрій Володимирович
ВОСКОБОЙНИК Володимир Олександрович
ТІМЕНКО Артур Валентинович
КІЦЕЛЬ Наталія Василівна
ШАПОВАЛ Олександр Олександрович

ОСНОВИ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

Монографія

Підписано до друку 25.04.2025
Формат 60x84 1/16. Умовн. друк. арк. 17,3.
Наклад 300 прим. Замовлення № 21-25.
Папір офсетний. Гарнітура Times.
Електрографічний друк.

Видавець ПП «Видавництво «НОВАБУК»
Свідоцтво суб'єкта видавничої справи
ДК №7598 від 10.02.2025р.
www.novabook.com.ua
097 555 10 72

Віддруковано ФОП Щербатих О.В.
вул. Софіївська, 36-Б, м. Кременчук, 39601
Свідоцтво суб'єкта видавничої справи
ДК №2129 від 17.03.2005 р.

ISBN 978-617-639-525-6