ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження питань безпеки бездротової мережі малого офісу»

на здобуття освітнього ступеня магістра
зі спеціальності __125_____
Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Михайло ШУЛЬГА

Виконав: здобувач вищої освіти групи СЗДМ-61

_____ ШУЛЬГА Михайло

Керівник: _____ ПЕПА Юрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Систем інформаційного та кібернетичного захисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ШУЛЬЗІ Михайлу Анатолійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Дослідження питань безпеки бездротової локальної мережі малого офісу».
Керівник кваліфікаційної роботи: ПЕПА Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «____» 2023 р. №_____.

2. Строк подання кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
__Аналіз загроз в комп'ютерній мережі.
__Оцінка саособів захисту інформації.
__Способи і методи безпечної роботи в локальній мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд стандартів Wi-Fi.
2. Протокольна безпека.
3. Апаратна безпека.
4. Програмна безпека.

5. Перелік графічного матеріалу: _____Презентаційний матеріал на слайдах_____
_____

6. Дата видачі завдання _____15.10.2023 р._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літературних джерел		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання четвертого розділу роботи		
6	Написання висновків по роботі		
7	Підготовка демонстраційних матеріалів		
8	Підготовка доповіді		

Здобувач вищої освіти _____ Михайло ШУЛЬГА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи містить: 75 стор., 38 рис., 11 табл. та 26 джерел.

Об'єкт дослідження – локальна бездротова мережа.

Предмет дослідження – методи та технології захисту передачі інформації через радіоканал.

Мета роботи – дослідити безпеку передачі інформації в межах малого офісу між хостами та запропонувати механізми надійного захисту інформації.

Методи дослідження: аналіз сучасних технологій захисту даних, порівняння алгоритмів шифрування, експериментальні дослідження, системний аналіз.

У роботі проаналізовано сучасні методи та технології захисту передачі цифрової інформації. Враховуючи специфіку передачі даних в межах малого офісу автором запропоновано систему безпечної роботи в мережі і протестовано її експериментально на вразливість і ефективність роботи.

Галузь використання – безпека передачі даних в бездротових мережах, захист інформації в мережах.

Ключові слова: ПАКЕТИ ДАНИХ, БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ, ШИФРУВАННЯ, АДМІНІСТРУВАННЯ, ДОСТУП, ВРАЗЛИВІСТЬ, МЕРЕЖЕВА БЕЗПЕКА.

ABSTRACT

The text part of the master's qualification work contains: 75 pages, 38 figures, 11 tables and 26 sources.

The object of research - a local wireless network.

Subject of research - methods and technologies for protecting the transmission of information over the radio channel.

Purpose - to investigate the security of information transmission within a small office between hosts and to propose mechanisms for reliable information protection.

Research methods: analysis of modern data protection technologies, comparison of encryption algorithms, experimental studies, system analysis.

The paper analyzes modern methods and technologies for protecting the transmission of digital information. Taking into account the specifics of data transmission within a small office, the author proposes a system of secure networking and tests it experimentally for vulnerability and efficiency.

Field of application - data transmission security in wireless networks, information security in networks.

Keywords: DATA PACKETS, DATA TRANSMISSION SECURITY, ENCRYPTION, ADMINISTRATION, ACCESS, VULNERABILITY, NETWORK SECURITY.

ЗМІСТ

ВСТУП

Одна з характерних прикмет початку XXI століття – це стрімкий розвиток і проникнення в усі сфери нашого життя засобів радіозв'язку різного призначення, що вже перетворилися в предмети першої необхідності. За дуже короткий термін вони стали могутнім інструментом обміну й одержання інформації, будучи інтегрованими у високотехнологічні системи і мережі, завдяки постійно зростаючим потребам і можливостям оплати послуг їх користувачами.

Бездротові мережі стали цілою індустрією, у якій зайнята величезна кількість компаній. Затверджуються нові стандарти, з'являється сумісне з ними устаткування. Будуються корпоративні WLAN-мережі і точки публічного доступу (“хот-споти”). Не відстають виробники ноутбуков і кишенькових комп'ютерів, що випускають все більш легкі й ультра портативні моделі, однаково придатні для роботи в офісі і на природі.

Зв'язати офіс, готель, аеропорт або кафе з зовнішнім світом можна самими різними способами. Компанії із солідними офісами, охороною, системами спостереження цілком можуть дозволити собі оптоволокно. Провідні технології перевірені часом, недорогі, безпечні і продуктивні. Десяти, стомегабітними і навіть гігабітними мережами Ethernet нині вже нікого не здивуєш, мережні контролери коштують досить дешево і нерідко входять у стандартне постачання ПК і ноутбуков. Проте вони не вирішують головне питання – не дають користувачеві настільки необхідної йому мобільності. Чи то справа технології бездротових мереж, що уже давно почали боротьбу за масового споживача.

Публічна мережа WLAN (PWLAN) звичайно складається з розставлених по будинку точок доступу (базових станцій), підключених до IP мережі оператора, і мобільних клієнтів, що підключаються до своєї базової станції за допомогою мережевих карт. Усе, що потрібно для роботи

в такому місці, - ноутбук с картою бездротового доступу або PDA з підтримкою 802.11.

Оскільки радіус дії устаткування WLAN виміряється десятками метрів, ці рішення економічно вигідно використовувати тільки в зонах підвищеного попиту на послуги бездротового доступу до мереж передачі даних - так званих "hot spots".

Серед послуг, що можуть запропонувати мандрівникам оператори мобільного зв'язку і сервіс-провайдери - доступ в інтернет, користування поштовою скринькою, чатом, перегляд відеофільмів і, звичайно, послуга доступу до корпоративної мережі.

У сучасному українському телекомунікаційному співтоваристві не припиняються дискусії про можливу долю комерційних зон беспроводного доступу («хот спотов»), створених на базі беспроводных мереж стандарту IEEE 802.11 (Wi-Fi).

Скептики пророкують швидку ринкову загибель технології Wi-Fi і не бачать особливої вигоди для операторів у будівництві публічних зон доступу. Їхні опоненти, навпроти, прагнуть довести перспективність і конкурентноздатність мереж Wi-Fi на ринку послуг бездротової передачі інформації. Однак, як це часто трапляється з новими технологіями, не чекаючи вердикту місцевих «маркетологів», ця технологія поступово приживається на українському телекомунікаційному ринку.

На відміну від мереж стільникового зв'язку, у Wi-Fi один, навіть дуже великий оператор не може забезпечити значне локальне і тим більше глобальне покриття в силу самої природи даної технології. Майбутнє ринку Wi-Fi послуг виглядає саме як безліч учасників – операторів з різними бізнес моделями надання послуг. Ця ситуація створює передумови для виникнення ринку послуг Wi-Fi-роумінгу в беспроводных мережах стандарту IEEE 802.11.

Для масового приватного користувача Wi-Fi-роумінг найближчим часом швидше за все не буде критичною послугою, оскільки він

орієнтований на стандартну й найбільш економічну схему одержання послуг по попередньо оплачених картах, за аналогією зі звичайною послугою Dial-up доступу. У той же час по мірі розвитку цього ринку варто очікувати, що роумінг буде затребуваний і цією категорією користувачів.

У числі основних задач, що встають на шляху розвитку нової технології, - інтеграція з мережами GPRS (а в майбутньому - 5G), мережна безпека і білінг.

1 ОГЛЯД ІСНУЮЧИХ ТЕХНОЛОГІЙ ПОБУДОВИ БЕЗДРОВТОВИХ МЕРЕЖ

1.1 Підходи до побудови бездротових локальних мереж

Бездротові локальні мережі класифікуються відповідно до використаного в них технології передачі (табл. 1.1). Усі сучасні продукти ринку локальних мереж відносяться до однієї з наступних категорій:

- *Інфрачервоні (Infrared - IR) Локальні мережі.*

Окремий осередок мережі, що використовує передачу в інфрачервоному діапазоні, обмежена розмірами однієї кімнати, оскільки інфрачервоне випромінювання не проходить крізь непрозорі стіни.

- *Вузькосмугова НВЧ - передача.*

Ці локальні мережі працюють на НВЧ, але не використовують розширений спектр. Деякі з цих продуктів працюють на частотах, що вимагає ліцензії.

- *Локальні мережі з розширеним спектром.*

Даний тип локальних мереж використовує при передачі технологію розширеного спектра. У більшості випадків ці локальні мережі працюють на діапазонах ISM (Industrial, Scientific and Medical Radio Frequency Band – радіочастотні діапазони для промислового, наукового і медичного застосування).

Таблиця 1.1 - Порівняльні характеристики бездротових локальних мереж

	Інфрачервоне випромінювання		Розширений спектр		Радіо
	Розсіяне	З направленим променем	Перебудова частоти	Пряма послідовність	Вузькосмугова НВЧ-передача
Швидкість передачі даних Мбіт/с	1-4	1-10	1-3	2-20	10-20
Діапазон (м)	15-60	25	30-100	30-250	10-40
Довжина хвилі/частота	800-900 нм		902 – 928 МГц 2,4 – 2,483 ГГц 5,725 – 5,85 ГГц		902 – 928 МГц 5,2 – 5,775 ГГц 18,825– 9,205 ГГц
Схема модуляції	ASK		FSK	QPSK	FS/QPSK
Випромінювана потужність	----		< 1 Вт		25 мВт

В даний час найбільш популярні бездротові локальні мережі використовують технологію розширеного спектра.

1.2 Вибір системи широсмугового бездротового доступу

Під терміном "доступ" розуміється мережний доступ, що має масовий характер, тобто мережа доступу. Радіомодемні з'єднання типу "крапка - крапка", а також радіорелейні станції і лінії зв'язку, що є традиційними засобами рішення проблеми "останньої милі" за допомогою радіозасобів, мають численні приклади реалізації, однак не забезпечують масовий характер підключень. Тому в даному проекті розглядаються системи бездротового доступу, що є функціонально закінченим набором апаратно-програмних засобів, що реалізують з'єднання типу "крапка - багато крапок" і утворюючу мережу доступу.

Попит на послуги телефонії і доступу в Інтернет існує. Він народжує пропозицію, реалізована на основі різнотипного устаткування

бездротового доступу, що тією чи іншою мірою дозволяє вирішувати існуючі задачі. Перелік основних класів систем бездротового доступу в табл. 1.2.

Таблиця 1.2 - Основні класи систем бездротового доступу

Тип системи	Діапазон частот/ швидкість передачі	Основна область використання	Переваги	Недоліки
WLL DECT	1,88 - 1,90 ГГц/до 56 кбіт/с	Доступ до ТФОП. Низькошвидкісний доступ до Інтернет	Простота легалізації мережі. Високоякісна телефонія	Низька швидкість модемного підключення до Інтернет
WLL за фірмовими стандартами	0,9 – 5,8 ГГц	Доступ до ТФОП. Низкошвидкісний доступ до Інтернет	Гнучкість у виборі діапазону. Великий вибір устаткування	Фірмові протоколи і несумісність устаткування від різних виробників
LMDS	26-38 ГГц	Надання виділених каналів. Високошвидкісна передача даних. Доступ до Інтернет	Висока пропускна здатність	Висока вартість устаткування. Відсутність єдиного стандарту. Мала дальність
MMDS	2,3-2,5 ГГц	Високошвидкісна передача даних. Доступ до Інтернет. Цифрове телемовлення	Висока пропускна здатність. Велика дальність	Висока вартість устаткування і частотних дозволів.Немає единогостандарту

Продовження таблиці 1.2

Тип системи	Діапазон частот/ швидкість передачі	Основна область використання	Переваги	Недоліки
Системи широкосму-гового бездротового доступу (BWA)	2,4 – 10,5 ГГц	Високошвидкісна передача даних. Доступ до Інтернет. Пакетна телефонія	Великий вибір устаткування і частотних діапазонів.	Несумісність устаткування різних виробників
Bluetooth	2,4 ГГц/780 кбіт/с	Бездротовий зв'язок ближньої дії	Дешевина і простота використання. Мале енергоспоживання	Переважна більшість Bluetooth-пристроїв обмежена радіусом дії 10-30 м. Несумісність продуктів різних виробників між собою
GPRS	< 50 кбіт/с	Пакетна передача даних по бездротовим телефонним мережам і Інтернету. Низкошвидкісний доступ до Інтернет	Забезпечує мобільний, порівняно дешевий доступ в Інтернет. Велика зона покриття	Нестабільна швидкість передачі даних, мала надійність з'єднання

Продовження таблиці 1.2

Radio Ethernet стандарту IEEE 802.11b	2,4 ГГц/11 Мбіт/с	Високошвидкісний доступ до Інтернет. Корпоративні мережі	Дешевина і приступність устаткування. Висока пропускна здатність – до 11 Мбіт/с на сектор. Велика дальність. Великий досвід використання устаткування. Сумісність устаткування від різних виробників	Висока завантаженість діапазону, перешкоди від піратських радіозасобів. Неможливість подальшого розвитку у великих містах через вичерпання діапазону. Проблеми передачі трафіка реального часу (голосу) через використовування колізійного протоколу
Radio Ethernet стандарту IEEE 802.11 a	5 ГГц, 54-108 Мбіт/с	Високошвидкісний доступ до Інтернет. Корпоративні мережі	Мала завантаженість діапазону. Висока пропускна здатність – до 54 Мбіт/с (у turbo режимі 108 Мбіт/с) на сектор	Пристрої дорожче, ніж 802.11b і g. Мала дальність передачі. Великі складності з одержанням ліцензії. Проблеми передачі трафіка реального часу (голосу) через використовуваний колізійний протокол.

1.2.1 Джерела технології

Перший - це системи фіксованого радіодоступу (WLL - Wireless Local Loop), що з'явилися як альтернатива провідної телефонії. До рішень цього класу можна віднести MultiGain Wireless (Innowave ECI Wireless Systems), де передача даних обмежується смугою 64 Кбит/з ISDN BRI, або, фактично, модемним з'єднанням 56 Кбит/з, а також WLL DECT (Digital Enhanced Cordless Telecommunications – цифрові розширені бездротові телекомунікації) , тут передача даних, організована через модемне з'єднання, має швидкість ще менше.

Слідом за мережами кабельного телебачення з'явилися системи бездротового телемовлення на базі технологій MMDS (Multichannel Multipoint Distribution Service – багатоканальна багатоточкова розподільна служба) і LMDS (Local Multipoint Distribution Service). Їх можна вважати другим джерелом BWA.

Комп'ютерна ера, що супроводжувалася розвитком локальних обчислювальних мереж, обумовила появу бездротових систем типу Wireless LAN, що пізніше були стандартизовані комітетом IEEE 802.11 як мережі радіо-Ethernet. Саме на базі цих трьох, що стали вже традиційними, технологій останнім часом одержали розвиток нові технічні засоби.

Різниця між пристроями WLL і BWA досить умовна і полягає в наступному. Системи WLL орієнтовані переважно на надання послуг класичної телефонії; передача даних, як правило, здійснюється на рівні модемного підключення. Устаткування BWA, навпроти, споконвічно створювалося для високошвидкісної передачі даних і дозволяє формувати телефонні канали поверх пакетного протоколу, у якості якого звичайно застосовується IP.

1.2.2 Радіочастоти і характеристики систем

Устаткування широкосмуговового доступу використовує цілком визначений частотний діапазон. Насамперед, - це діапазон 2,4 ГГц.

Обумовлено це тим, що в багатьох країнах цей діапазон вільний від ліцензування й інсталяції устаткування, що працює в цьому діапазоні, мають масовий характер.

За вільним від ліцензування діапазоном випливають смуга радіочастот 2,5 - 2,7 ГГц, використовувана MMDS, діапазони 3,5 ГГц, 5,8 ГГц. Як правило, у цих діапазонах працює устаткування операторського класу, що має велику абонентську ємність і розширений набір послуг (передача даних, мультимедіа, телефонії). Далі випливають частоти в діапазонах від 10 до 38 ГГц. Смуга радіочастот 27,5 - 29,5 ГГц використовується системами LMDS. Ці системи спеціалізовані для цілей телевізійного мовлення.

Системи широкосмугового бездротового доступу типу "крапка - багато крапок", що працюють у мікрохвильовому діапазоні до 38 ГГц, мають унікальну ємність. Інформаційні потоки, якими оперують подібного роду системи, дозволяють характеризувати їхній радіо інтерфейс як ATM в ефірі.

Використовувані частоти забезпечують роботу систем в умовах прямої видимості. Можливості систем, характеристики, а також умови їхнього застосування обумовлюють фіксований доступ.

1.2.3 Компоненти й архітектура

Подібні системи мають дуже важливу якість, як легка розширюваність і масштабируемость. Будучи утворюючим елементом мережі беспроводного доступу, базова станція (БС) відіграє важливу роль у класифікації систем широкополосного беспроводного доступу. Інформаційна ємність БС дозволяє умовно розділити всі системи беспроводного доступу по групах.

Абонентські пристрої (Subscriber Units, SU), що обслуговуються БС і встановлювані в користувача, мають різний користувальницький інтерфейс. Для телефонії використовується абонентська лінія (FXS),

цифровий інтерфейс E1, ISDN. Для передачі даних - Ethernet, Frame Relay із синхронним інтерфейсом, ISDN.

Абонентські пристрої мають або убудовану, або зовнішню спрямовану антену, що приєднується. Кожен абонентський пристрій або пристрій передплатника (SU) працює на свою БС.

З'єднання між БС різних стільник виконуються за допомогою технологій провідного (найчастіше оптичні лінії зв'язку) або бездротового доступу (радіорелейні, або радіомодемні лінії зв'язку).

1.2.4 Мобільність сучасних бездротових технологій

Не всі існуючі в даний час бездротові технології дійсно мобільні. Наприклад, досить дешевий супутниковий зв'язок, що по кишені навіть приватним особам, мобільної не назвеш – не брати ж із собою усюди немаленьку параболічну антену.

1.2.4.1 GPRS (General Packet Radio Service)

Можливості GSM-мереж обмежені пропускною здатністю. GPRS з її піковими швидкостями в 53,6 кбіт/с для прийому і 26,8 кбіт/с для передачі на практиці виявляється досить примхливої, а мережа 3G досить неспішно рухається до споживача і найчастіше теж неприйнятна для передачі великих обсягів інформації. Найбільший у Кореї оператор мобільного зв'язку SK Telekom надає доступ до мереж 3G, що працює на швидкості всього 256 кбіт/с.

GPRS (пакетний радіозв'язок загального призначення) — це стандарт бездротового високошвидкісного зв'язку, що дозволяє обмінюватися пакетними даними, наприклад, електронною поштою або інформаційним наповненням web-сайтів, по бездротовим телефонним мережам і Інтернету. Технологію GPRS часто називають технологією покоління 2,5 (2.5G) (за аналогією з технологією бездротового зв'язку першого покоління (1G), що застосовувалася для зв'язку аналогових

стільникових телефонів, а також технологією бездротового зв'язку другого покоління (2G), що застосовується в цифрових мобільних телефонах). Підтримка технології GPRS реалізована не тільки в мобільних телефонах: мобільні ПК також можуть бути обладнані адаптером GPRS, що забезпечує підключення до Інтернету.

1.2.4.2 Bluetooth

Bluetooth — технологія короткохвильового радіозв'язку (2,4 ГГц), що діє на досить близькій відстані (найчастіше працює в межах однієї кімнати і не дозволяє передавати дані на великі відстані: переважна більшість Bluetooth-пристроїв обмежена радіусом дії 10–30 м) і спрощує взаємодію мережних пристроїв один з одним, а також доступ за допомогою мережних пристроїв в Інтернет. Ця технологія спрощує синхронізацію даних між мережними пристроями й іншими комп'ютерами. Оскільки технологія Bluetooth не призначена для передачі великих обсягів даних, вона не підходить у якості заміни локальних або глобальних мереж.

2 ТЕХНОЛОГІЇ WI-FI

2.1 Особливості технології

На зорі розвитку радіотехніки термін "бездротовий" *(wireless)* використовували для позначення радіозв'язку в широкому розумінні цього слова, тобто буквально у всіх випадках, коли передача інформації здійснювалася без дротів. Пізніше це тлумачення практично вийшло з обігу, і "бездротовий" стало вживатися як еквівалент терміну "радіо" (*radio*) або "радіочастота" (*RF - radio frequency*). Зараз обидва поняття вважаються взаємозамінними в тому разі, якщо йдеться про діапазон частот від 3 кГц до 300 ГГц. Проте термін "радіо" частіше використовується для опису вже давно існуючих технологій (радіомовлення, супутниковий зв'язок, радіолокація, радіотелефонний зв'язок тощо). А термін "бездротовий" у наші дні заведено відносити до нових технологій радіозв'язку, таких, як мікростільникова і стільникова телефонія, пейджинг, абонентський доступ тощо.

Розрізняють три типи бездротових мереж (рис. 2.1): *WWAN (Wireless Wide Area Network), WLAN (Wireless Local Area Network) і WPAN (Wireless Personal Area Network).*

Рисунок 2.1 - Радіус дії персональних, локальних і глобальних бездротових мереж

Під час побудови мереж *WLAN* і *WPAN*, а також систем широкосмугового бездротового доступу (*BWA - Broadband Wireless Access*) застосовуються подібні технології. Ключова відмінність між ними (рис. 2.2) - діапазон робочих частот і характеристики радіоінтерфейсу. Мережі *WLAN* і *WPAN* працюють у неліцензійних діапазонах частот 2,4 і 5 ГГц, тобто під час їхнього розгортання не потрібне частотне планування та координація з іншими радіомережами, що працюють у тому самому діапазоні. Мережі *BWA* (*Broadband Wireless Access*) використовують як ліцензійні, так і неліцензійні діапазони (від 2 до 66 ГГц).

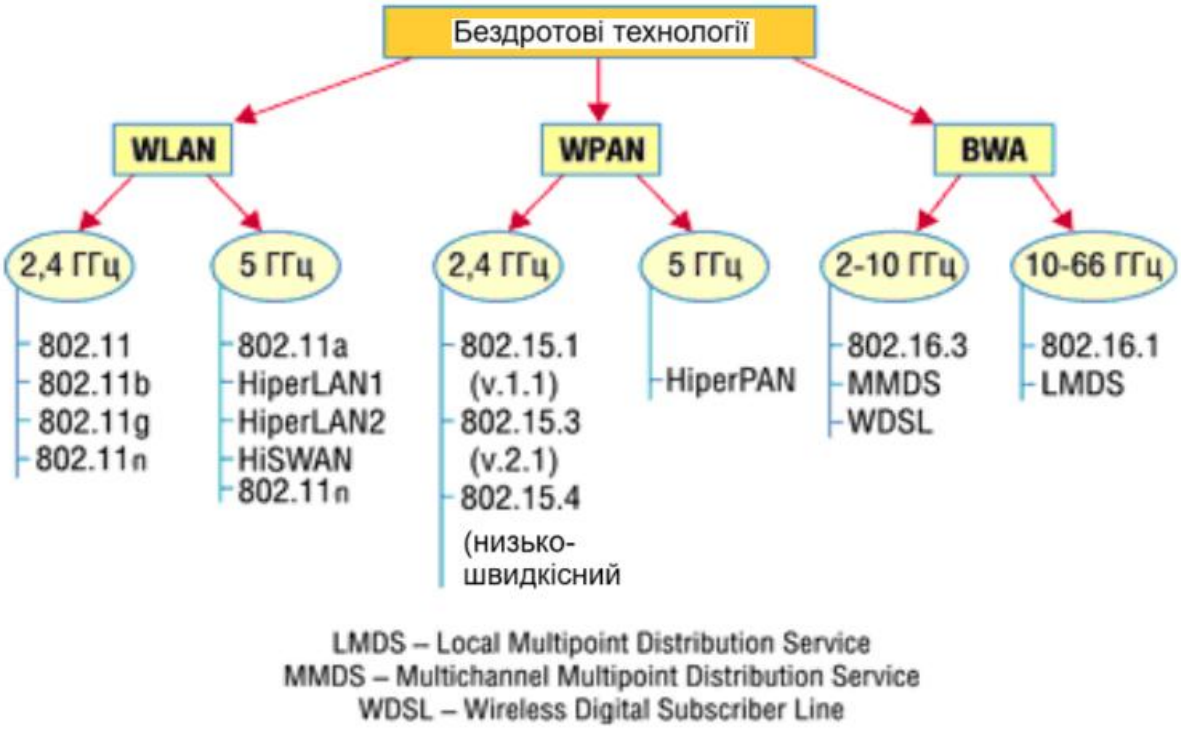

Рисунок 2.2 - Класифікація бездротових технологій

Основне призначення бездротових локальних мереж (*WLAN*) - організація доступу до інформаційних ресурсів усередині будівлі. Друга за значимістю сфера застосування - це організація громадських комерційних точок доступу (hot spots) у людних місцях - готелях, аеропортах, кафе, а також організація тимчасових мереж на період проведення заходів (виставок, семінарів).

Бездротові локальні мережі створюють на основі сімейства стандартів *IEEE* 802.11. Ці мережі відомі також як *Wi-Fi (Wireless Fidelity)*, і хоча сам термін *Wi-Fi* у стандартах явно не прописано, бренд *Wi-Fi* набув у світі найширшого поширення.

У 1990 р. Комітет зі стандартів *IEEE* 802 (*Institute of Electrical and Electronic Engineers*) сформував робочу групу зі стандартів для бездротових локальних мереж *IEEE* 802.11. Ця група зайнялася розробкою загального стандарту для радіообладнання та мереж, що працюють на частоті 2.4 ГГц зі швидкостями 1 і 2 Мбіт/с. Роботу зі створення стандарту було завершено через сім років, і в червні 1997 р. було ратифіковано першу специфікацію *IEEE* 802.11.

Стандарт *IEEE* 802.11 став першим стандартом для продуктів *WLAN* від незалежної міжнародної організації. Однак до моменту виходу стандарту в світ спочатку закладена в ньому швидкість передачі даних виявилася недостатньою. Це стало причиною подальших доопрацювань, тому сьогодні можна говорити про групу стандартів.

2.2 Основні стандарти

Нині широко використовується переважно три стандарти групи *IEEE* 802.11 (представлені в табл. 2.1).

Таблиця 2.1 - Основні характеристики стандартів групи *IEEE* 802.11

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

Стандарт *IEEE* 802.11g, ухвалений у 2003 році, є логічним розвитком стандарту *IEEE* 802.11b і передбачає передачу даних у тому самому частотному діапазоні, але з вищими швидкостями. Крім того, стандарт *IEEE* 802.11g повністю сумісний з *IEEE* 802.11b, тобто будь-який пристрій *IEEE* 802.11g має підтримувати роботу з пристроями *IEEE* 802.11b. Максимальна швидкість передавання даних у стандарті *IEEE* 802.11g становить 54 Мбіт/с. Під час розроблення стандарту *IEEE* 802.11g розглядали дві конкуруючі технології: метод ортогонального частотного поділу *OFDM*, запозичений зі стандарту 802.11a та запропонований до розгляду компанією *Intersil*, і метод двійкового пакетного згорткового кодування *PBCC,* запропонований компанією *Texas Instruments*. У результаті стандарт *IEEE* 802.11g містить компромісне рішення: як базові застосовуються технології *OFDM* і *CCK*, а опціонально передбачено використання технології *PBCC*.

Ідея згорткового кодування (*Packet Binary Convolutional Coding, PBCC*) полягає в такому. Вхідна послідовність інформаційних біт перетворюється у згортковому кодері таким чином, щоб кожному вхідному біту відповідало більше одного вихідного. Тобто згортковий

кодер додає певну надлишкову інформацію до вихідної послідовності. Якщо, приміром, кожному вхідному біту відповідають два вихідних, то говорять про згорткове кодування зі швидкістю, що дорівнює 1/2. Якщо ж кожним двом вхідним бітам відповідають три вихідні, то швидкість згорткового кодування становитиме вже 2/3.

Будь-який згортковий кодер будується на основі кількох послідовно пов'язаних комірок запам'ятовування та логічних елементів *XOR*. Кількість комірок, що запам'ятовують, визначає кількість можливих станів кодера. Якщо, наприклад, у згортковому кодері використовується шість комірок для запам'ятовування, то в кодері зберігається інформація про шість попередніх станів сигналу, а з урахуванням значення вхідного біта одержимо, що в такому кодері застосовується сім біт вхідної послідовності. Такий згортковий кодер називається кодером на сім станів.

Вихідні біти, що формуються у згортковому кодері, визначаються операціями *XOR* між значеннями вхідного біта і бітами, збереженими в комірках, що запам'ятовують, тобто значення кожного вихідного біта, який формують, залежить не тільки від вхідного інформаційного біта, а й від кількох попередніх бітів.

Головною перевагою згорткових кодерів є завадостійкість сформованої ними послідовності. Річ у тім, що в разі надмірності кодування навіть у разі виникнення помилок приймання вихідна послідовність біт може бути безпомилково відновлена. Для відновлення вихідної послідовності біт на стороні приймача застосовується декодер Вітербі.

Дибіт, сформований у згортковому кодері, використовується надалі як переданий символ, але попередньо він піддається фазовій модуляції. Причому залежно від швидкості передачі можлива двійкова, квадратурна або навіть восьмипозиційна фазова модуляція.

На відміну від технологій *DSSS* (коди Баркера, *CCK-послідовності*), у технології згорткового кодування не застосовують технологію

розширення спектра завдяки використанню шумоподібних послідовностей, однак розширення спектра до стандартних 22 МГц передбачено і в цьому випадку. Для цього застосовують варіації можливих сигнальних сузір'їв *QPSK* і *BPSK*.

Розглянутий метод *PBCC-кодування* опціонально використовується в протоколі *IEEE* 802.11b на швидкостях 5,5 і 11 Мбіт/с. Аналогічно в протоколі *IEEE* 802.11g для швидкостей передачі 5,5 і 11 Мбіт/с цей спосіб теж застосовується опціонально. Взагалі, внаслідок сумісності протоколів *IEEE* 802.11b і *IEEE* 802.11g технології кодування і швидкості, передбачені протоколом *IEEE* 802.11b, підтримуються і в протоколі *IEEE* 802.11g. У цьому плані до швидкості 11 Мбіт/с протоколи *IEEE* 802.11b і *IEEE* 802.11g збігаються один з одним, за винятком того, що в протоколі *IEEE* 802.11g передбачені такі швидкості, яких немає в протоколі *IEEE* 802.11b.

Опціонально в протоколі *IEEE* 802.11g технологія *PBCC* може використовуватися при швидкостях передачі 22 і 33 Мбіт/с.

Для швидкості 22 Мбіт/с порівняно з уже розглянутою нами схемою *PBCC* передача даних має дві особливості. Насамперед, застосовується 8-позиційна фазова модуляція (*8-PSK*), тобто фаза сигналу може приймати вісім різних значень, що дає змогу в одному символі кодувати вже три біти. Крім того, у схему, за винятком згорткового кодера, додано пунктурний кодер *(Puncture)*. Сенс такого рішення досить простий: надмірність згорткового кодера, що дорівнює 2 (на кожний вхідний біт припадає два вихідних), досить висока і за певних умов завадостійкого середовища є надлишковою, тому можна зменшити надмірність, щоб, приміром, кожним двом вхідним бітам відповідали три вихідні. Для цього можна, звісно, розробити відповідний згортковий кодер, але краще додати в схему спеціальний пунктурний кодер, який буде просто знищувати зайві біти. Припустимо, пунктурний кодер видаляє один біт із кожних чотирьох вхідних біт. Тоді кожним чотирьом вхідним бітам

відповідатимуть три вихідні. Швидкість такого кодера становить 4/3. Якщо ж такий кодер використовується в парі зі згортковим кодером зі швидкістю 1/2, то загальна швидкість кодування становитиме вже 2/3, тобто кожним двом вхідним бітам відповідатимуть три вихідні.

Технологія *PBCC* є опціональною в стандарті *IEEE* 802.11g, а технологія *OFDM* - обов'язковою. Для того щоб зрозуміти суть технології *OFDM*, розглянемо детальніше багатопроменеву інтерференцію, що виникає під час поширення сигналів у відкритому середовищі.

Ефект багатопроменевої інтерференції сигналів полягає в тому, що внаслідок багаторазових відбитків від природних перешкод один і той самий сигнал може потрапляти в приймач різними шляхами. Але різні шляхи поширення відрізняються один від одного за довжиною, а тому ослаблення сигналу буде для них неоднаковим. Отже, у точці приймання результуючий сигнал являє собою інтерференцію багатьох сигналів, які мають різні амплітуди та зміщені один відносно одного в часі, що еквівалентно складанню сигналів із різними фазами.

Наслідком багатопроменевої інтерференції є спотворення сигналу, що приймається. Багатопроменева інтерференція притаманна будь-якому типу сигналів, але особливо негативно вона позначається на широкосмугових сигналах, оскільки під час використання широкосмугового сигналу в результаті інтерференції певні частоти складаються синфазно, що призводить до збільшення сигналу, а деякі, навпаки, протифазно, спричиняючи ослаблення сигналу на даній частоті.

Говорячи про багатопроменеву інтерференцію, що виникає під час передавання сигналів, відзначають два крайні випадки. У першому з них максимальна затримка між сигналами не перевищує тривалості одного символу й інтерференція виникає в межах одного переданого символу. У другому - максимальна затримка між сигналами більша від тривалості одного символу, тому в результаті інтерференції складаються сигнали, що

представляють різні символи, і виникає так звана міжсимвольна інтерференція (*Inter Symbol Interference, ISI*).

Найбільш негативно на спотворення сигналу впливає саме міжсимвольна інтерференція. Оскільки символ - це дискретний стан сигналу, що характеризується значеннями частоти несучої, амплітуди та фази, для різних символів змінюються амплітуда та фаза сигналу, а отже, відновити вихідний сигнал вкрай складно.

З цієї причини за високих швидкостей передавання застосовується метод кодування даних, званий ортогональним частотним поділом каналів з мультиплексуванням (*Orthogonal Frequency Division Multiplexing, OFDM*). Суть його полягає в тому, що потік переданих даних розподіляється по безлічі частотних підканалів і передача ведеться паралельно на всіх таких підканалах. При цьому висока швидкість передавання досягається саме за рахунок одночасного передавання даних усіма каналами, тоді як швидкість передавання в окремому підканалі може бути й невисокою.

Завдяки тому що в кожному з частотних підканалів швидкість передавання даних можна зробити не надто високою, створюються передумови для ефективного придушення міжсимвольної інтерференції.

Під час частотного поділу каналів необхідно, щоб окремий канал був досить вузьким для мінімізації спотворення сигналу, але водночас - досить широким для забезпечення необхідної швидкості передачі. Крім того, для економного використання всієї смуги каналу, що розділяється на підканали, бажано розташувати частотні підканали якомога ближче один до одного, але при цьому уникнути міжканальної інтерференції, щоб забезпечити їхню повну незалежність. Частотні канали, що задовольняють перераховані вище вимоги, називаються ортогональними. Несучі сигнали всіх частотних підканалів ортогональні один одному. Важливо, що ортогональність несучих сигналів гарантує частотну незалежність каналів один від одного, а отже, і відсутність міжканальної інтерференції.

Розглянутий спосіб поділу широкосмугового каналу на ортогональні частотні підканали називається ортогональним частотним поділом з мультиплексуванням (*OFDM*). Для його реалізації в передавальних пристроях використовують зворотне швидке перетворення Фур'є (*IFFT*), яке переводить попередньо мультиплексований на *n-каналів* сигнал із *часового* представлення в частотне.

Однією з ключових переваг методу *OFDM* є поєднання високої швидкості передачі з ефективним протистоянням багатопроменевому поширенню. Звичайно, сама по собі технологія *OFDM* не виключає багатопроменевого поширення, але створює передумови для усунення ефекту міжсимвольної інтерференції. Річ у тім, що невід'ємною частиною технології *OFDM* є охоронний інтервал *(Guard Interval, GI*) - циклічне повторення закінчення символу, що прилаштовується на початку символу.

Охоронний інтервал створює паузи між окремими символами, і якщо його тривалість перевищує максимальний час затримки сигналу внаслідок багатопроменевого поширення, то міжсимвольної інтерференції не виникає.

При використанні технології *OFDM* тривалість охоронного інтервалу становить одну четверту тривалості самого символу. При цьому символ має тривалість 3,2 мкс, а охоронний інтервал - 0,8 мкс. Таким чином, тривалість символу разом з охоронним інтервалом становить 4 мкс.

У протоколі *IEEE* 802.11g на низьких швидкостях передавання застосовується двійкова і квадратурна фазові модуляції *BPSK* і *QPSK*. У разі використання *BPSK-модуляції* в одному символі кодується тільки один інформаційний біт, а в разі *QPSK-модуляції* - два інформаційні біти. Модуляція *BPSK* застосовується для передавання даних на швидкостях 6 і 9 Мбіт/с, а модуляція *QPSK* - на швидкостях 12 і 18 Мбіт/с.

Для передачі на більш високих швидкостях використовується квадратурна амплітудна модуляція *QAM* (*Quadrature Amplitude Modulation*), за якої інформація кодується за рахунок зміни фази та

амплітуди сигналу. У протоколі *IEEE* 802.11g застосовується модуляція *16-QAM* і *64-QAM*. Перша модуляція передбачає 16 різних станів сигналу, що дає змогу закодувати 4 біти в одному символі; друга - 64 можливі стани сигналу, що дає можливість закодувати послідовність 6 біт в одному символі. Модуляція *16-QAM* використовується на швидкостях 24 і 36 Мбіт/с, а модуляція *64-QAM* - на швидкостях 48 і 54 Мбіт/с.

Стандарт *IEEE* 802.11a передбачає швидкість передачі даних до 54 Мбіт/с. На відміну від базового стандарту специфікаціями *IEEE* 802.11a передбачено роботу в новому частотному діапазоні 5ГГц. Як метод модуляції сигналу обрано ортогонально частотне мультиплексування (*OFDM*), що забезпечує високу стійкість зв'язку в умовах багатопроменевого поширення сигналу.

Відповідно до правил *FCC* частотний діапазон *UNII* розбитий на три 100-мегагерцових піддіапазони, що розрізняються обмеженнями за максимальною потужністю випромінювання. Нижчий діапазон (від 5,15 до 5,25 ГГц) передбачає потужність лише 50 мВт, середній (від 5,25 до 5,35 ГГц) - 250 мВт, а верхній (від 5,725 до 5,825 ГГц) - 1 Вт. Використання трьох частотних піддіапазонів із загальною шириною 300 МГц робить стандарт *IEEE* 802.11a найширокосмуговішим із сімейства стандартів *IEEE* 802.11 і дає змогу розбити весь частотний діапазон на 12 каналів, кожен з яких має ширину 20 МГц, причому вісім із них лежать у 200-мегагерцовому діапазоні від 5,15 до 5,35 ГГц, а решта чотири канали - у 100-мегагерцовому діапазоні від 5,725 до 5,825 ГГц (рис. 2.3). При цьому чотири верхні частотні канали, що передбачають найбільшу потужність передавання, використовуються переважно для передавання сигналів поза приміщеннями.

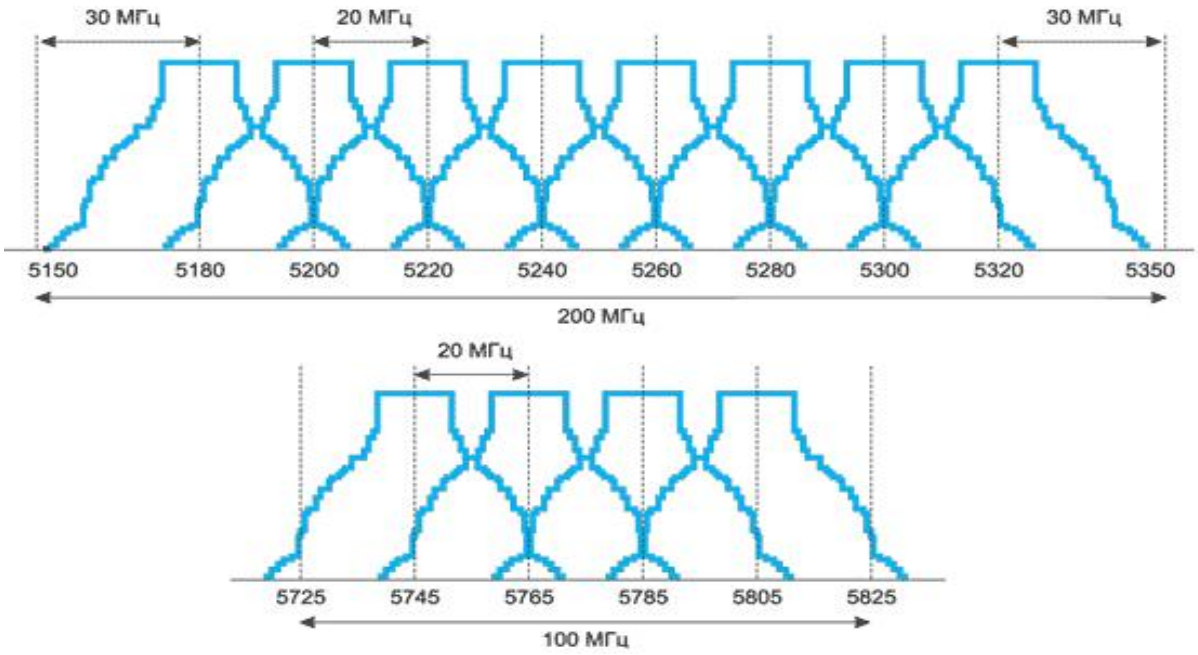

Рисунок 2.3 - Поділ діапазону *UNII* на 12 частотних піддіапазонів

Стандарт *IEEE* 802.11a ґрунтується на техніці частотного ортогонального розділення каналів із мультиплексуванням (*OFDM*). Для розділення каналів застосовується зворотне перетворення Фур'є з вікном у 64 частотних підканали. Оскільки ширина кожного з 12 каналів, визначених у стандарті *IEEE* 802.11a, має значення 20 МГц, виходить, що кожен ортогональний частотний підканал (піднесуча) має ширину 312,5 кГц. Однак із 64 ортогональних підканалів задіюється тільки 52, причому 48 із них застосовують для передавання даних (*Data Tones*), а решту - для передавання службової інформації (*Pilot Tones*).

За технікою модуляції протокол *IEEE* 802.11a мало чим відрізняється від *IEEE* 802.11g. На низьких швидкостях передавання для модуляції піднесучих частот використовується двійкова і квадратурна фазові модуляції *BPSK* і *QPSK*. При застосуванні *BPSK-модуляції* в одному символі кодується тільки один інформаційний біт. Відповідно у разі використання *QPSK-модуляції*, тобто коли фаза сигналу може набувати чотирьох різних значень, в одному символі кодуються два інформаційні біти. Модуляція *BPSK* використовується для передачі даних

на швидкостях 6 і 9 Мбіт/с, а модуляція *QPSK* - на швидкостях 12 і 18 Мбіт/с.

Для передачі на більш високих швидкостях у стандарті *IEEE* 802.11a використовується квадратурна амплітудна модуляція *16-QAM* і *64-QAM*. У першому випадку є 16 різних станів сигналу, що дає змогу закодувати 4 біти в одному символі, а в другому - вже 64 можливих стани сигналу, що дає змогу закодувати послідовність із 6 бітів в одному символі. Модуляція *16-QAM* застосовується на швидкостях 24 і 36 Мбіт/с, а модуляція *64-QAM* - на швидкостях 48 і 54 Мбіт/с.

Інформаційна ємність *OFDM-символу* визначається типом модуляції і числом піднесучих. Оскільки для передавання даних застосовуються 48 піднесучих, ємність *OFDM-символу* становить 48 х *Nb*, де *Nb* - двійковий логарифм від числа позицій модуляції, або, простіше кажучи, кількість біт, які кодуються в одному символі в одному підканалі. Відповідно ємність *OFDM-символу* становить від 48 до 288 біт.

Послідовність обробки вхідних даних (бітів) у стандарті *IEEE* 802.11a виглядає таким чином. Спочатку вхідний потік даних піддається стандартній операції скремблювання. Після цього потік даних надходить на згортковий кодер. Швидкість згорткового кодування (у поєднанні з пунктурним кодуванням) може становити 1/2, 2/3 або 3/4. Оскільки швидкість згорткового кодування може бути різною, то під час використання одного й того самого типу модуляції швидкість передавання даних виявляється різною. Розглянемо, наприклад, модуляцію *BPSK*, за якої швидкість передавання даних становить 6 або 9 Мбіт/с. Тривалість одного символу разом з охоронним інтервалом дорівнює 4 мкс, а отже, частота проходження імпульсів складе 250 кГц. З огляду на те, що в кожному підканалі кодується по одному біту, а всього таких підканалів 48, отримуємо, що загальна швидкість передачі даних складе 250 кГц х 48 каналів = 12 МГц. Якщо при цьому швидкість згорткового кодування дорівнює 1/2 (на кожен інформаційний біт

додається один службовий), інформаційна швидкість виявиться вдвічі меншою за повну швидкість, тобто 6 Мбіт/с. За швидкості згорткового кодування 3/4 на кожні три інформаційні біти додається один службовий, тому в цьому разі корисна (інформаційна) швидкість становить 3/4 від повної швидкості, тобто 9 Мбіт/с. Аналогічним чином кожному типу модуляції відповідають дві різні швидкості передачі (табл. 2.2).

Таблиця 2.2 - Співвідношення між швидкостями передавання і типом модуляції в стандарті *IEEE* 802.11a

Швидкість передавання Мбіт/с	Тип модуляції	Швидкість згорточного кодування	Кількість біт в одному символі в одному підканалі	Загальна кількість біт у символі (48 підканалів)	Кількість інформаційних біт у символі
6	*BPK*	1\2	1	48	24
9	*BPK*	3\4	1	48	36
12	*QPK*	1\2	2	96	48
18	*QPK*	3\4	2	96	72
24	*16- QAM*	1\2	4	192	96
36	*16- QAM*	3\4	4	192	144
48	*16- QAM*	2\3	6	288	192
54	*16- QAM*	3\4	6	288	216

Після згорткового кодування потік біт піддається операції переміщення, або інтерлівінгу. Суть її полягає у зміні порядку слідування біт у межах одного *OFDM-символу*. Для цього послідовність вхідних біт розбивається на блоки, довжина яких дорівнює числу біт в *OFDM-символі* (*NCBPS*). Далі за певним алгоритмом проводиться двоетапна перестановка біт у кожному блоці. На першому етапі біти переставляються таким чином, щоб суміжні біти під час передачі *OFDM-символу* передавалися на несуміжних піднесучих. Алгоритм перестановки

біт на цьому етапі еквівалентний такій процедурі. Спочатку блок біт довжиною *NCBPS* порядково (рядок за рядком) записується в матрицю, що містить 16 рядків і *NCBPS/16* рядів. Далі біти зчитуються з цієї матриці, але вже по рядах (або так само, як записувалися, але з транспонованої матриці). У результаті такої операції спочатку сусідні біти будуть передаватися на несуміжних піднесучих.

Потім слідує етап другої перестановки бітів, мета якого полягає в тому, щоб сусідні біти не опинилися одночасно в молодших розрядах груп, що визначають модуляційний символ у сигнальному сузір'ї. Тобто після другого етапу перестановки сусідні біти опиняються поперемінно в старших і молодших розрядах груп. Робиться це з метою поліпшення завадостійкості переданого сигналу.

Після переміщення послідовність біт розбивається на групи за числом позицій обраного типу модуляції і формуються *OFDM-символи*.

Сформовані *OFDM-символи* піддаються швидкому перетворенню Фур'є, внаслідок чого формуються вихідні синфазний і квадратурний сигнали, які потім піддаються стандартній обробці - модуляції.

Стандарт *IEEE* 802.11n було затверджено 11 вересня 2009 року. *IEEE* 802.11n за швидкістю передачі можна порівняти з дротовими стандартами. Максимальна швидкість передачі стандарту *IEEE* 802.11n приблизно в 5 разів перевищує продуктивність класичного *Wi-Fi*.

Можна відзначити такі основні переваги стандарту 802.11n:

- велика швидкість передачі даних (близько 300 Мбіт/с);

- рівномірне, стійке, надійне та якісне покриття зони дії станції, відсутність непокритих ділянок;

- сумісність із попередніми версіями стандарту *Wi-Fi.*

Недоліки:

- велика потужність споживання;

- два робочих діапазони (можлива заміна обладнання);

- ускладнена і більш габаритна апаратура.

Збільшення швидкості передачі в стандарті *IEEE* 802.11n досягається, по-перше, завдяки подвоєнню ширини каналу з 20 до 40 МГц, а по-друге, за рахунок реалізації технології *MIMO* [2].

2.3 Топології бездротових мереж Wi-Fi

Мережі стандарту *IEEE* 802.11 можуть будуватися за будь-якою з таких топологій:

1. Незалежні базові зони обслуговування (*Independent Basic Service Sets, IBSSs*);

2. Базові зони обслуговування (*Basic Service Sets, BSSs*);

3. Розширені зони обслуговування (*Extended Service Sets, ESSs*).

4. Незалежні базові зони обслуговування (*IBSS*)

IBSS (рис. 2.4) являє собою групу станцій, що працюють відповідно до стандарту *IEEE* 802.11 і зв'язуються безпосередньо одна з одною. На рис. 1.4 показано, як станції, обладнані бездротовими мережевими інтерфейсними картами (*network interface card, NIC*) стандарту *IEEE* 802.11, можуть формувати *IBSS* і безпосередньо зв'язуватися одна з одною.

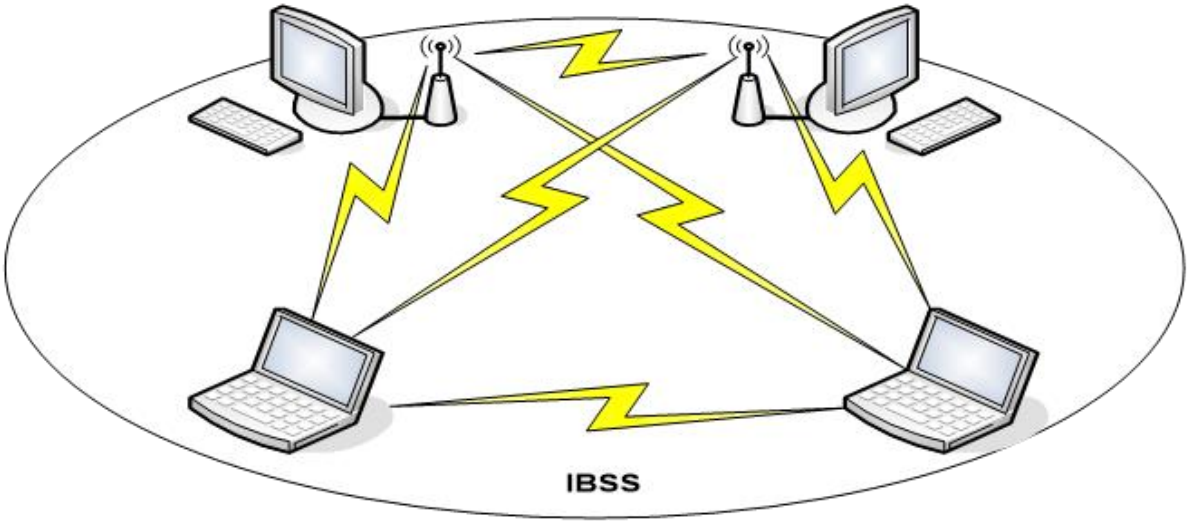

Рисунок 2.4 - Ad-Hoc мережа (IBSS)

Спеціальна мережа, або незалежна базова зона обслуговування (*IBSS*), виникає, коли окремі пристрої-клієнти формують

самопідтримувану мережу без використання окремої точки доступу (*AP - Access Point*). При створенні таких мереж не розробляють будь-які карти місця їхнього розгортання та попередні плани, тому вони зазвичай невеликі та мають обмежену протяжність, достатню для передавання даних, які спільно використовуються, у разі виникнення такої необхідності.

Оскільки в *IBSS* відсутня точка доступу, розподіл часу (*timing*) здійснюється нецентралізовано. Клієнт, який починає передачу в IBSS, задає сигнальний (маячковий) інтервал (*beacon interval*) для створення набору моментів часу передачі маячкового сигналу (*set of target beacon transmission time, TBTT*). Коли завершується *ТБТТ*, кожен клієнт *IBSS* виконує таке:

1. Призупиняє всі таймери затримки, що не спрацювали (*backoff timer*) з попереднього *TBTT*;

2. Визначає нову випадкову затримку;

Базові зони обслуговування (*BSS*) - це група станцій, що працюють за стандартом *IEEE* 802.11 і зв'язуються одна з одною. Технологія *BSS* передбачає наявність особливої станції, яка називається точка доступу AP (*Access Point*). Точка доступу - це центральний пункт зв'язку для всіх станцій BSS. Клієнтські станції не зв'язуються безпосередньо одна з одною. Замість цього вони зв'язуються з точкою доступу, а вже вона направляє кадри до станції-адресата. Точка доступу може мати порт висхідного каналу (*uplink port*), через який *BSS* підключається до дротової мережі (наприклад, висхідний канал *Ethernet*). Тому *BSS* іноді називають інфраструктурою *BSS*. На рис. 2.5 представлена типова інфраструктура *BSS*.

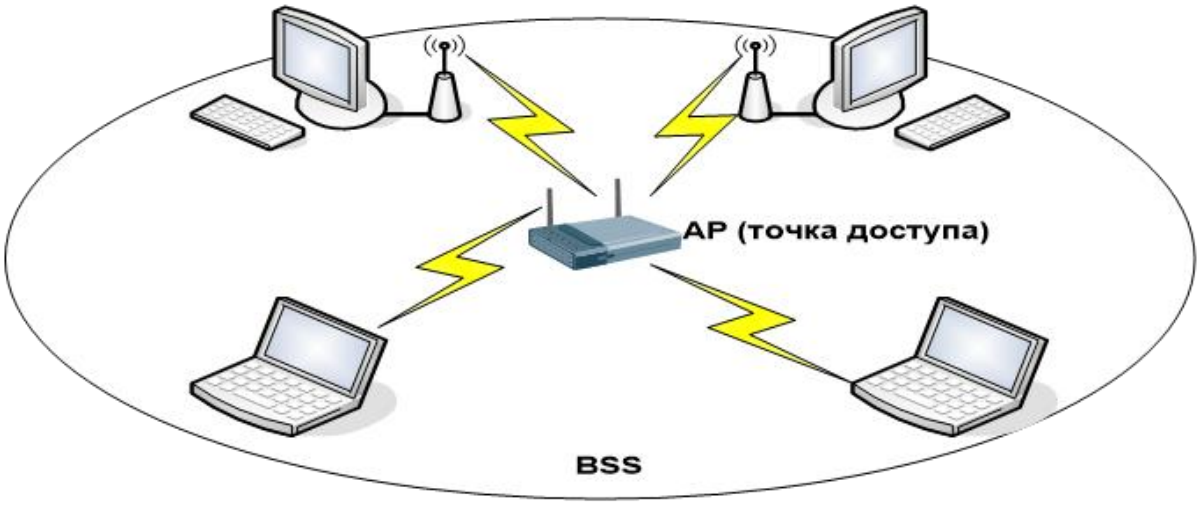

Рисунок 2.5 - Інфраструктура локальної бездротової мережі BSS

Кілька інфраструктур *BSS* можуть бути з'єднані через їхні інтерфейси висхідного каналу. Там, де діє стандарт *IEEE* 802.11, інтерфейс висхідного каналу з'єднує *BBS* із розподільчою системою (*Distribution System, DS*). Кілька *BBS*, з'єднаних між собою через розподільну систему, утворюють розширену зону обслуговування (*ESS*). Висхідний канал до розподільчої системи не обов'язково має використовувати дротове з'єднання. На рис. 1.6 наведено приклад практичного втілення *ESS*. Специфікація стандарту *IEEE* 802.11 залишає можливість реалізації цього каналу у вигляді бездротового. Але частіше висхідні канали до розподільчої системи являють собою канали дротової технології *Ethernet*.

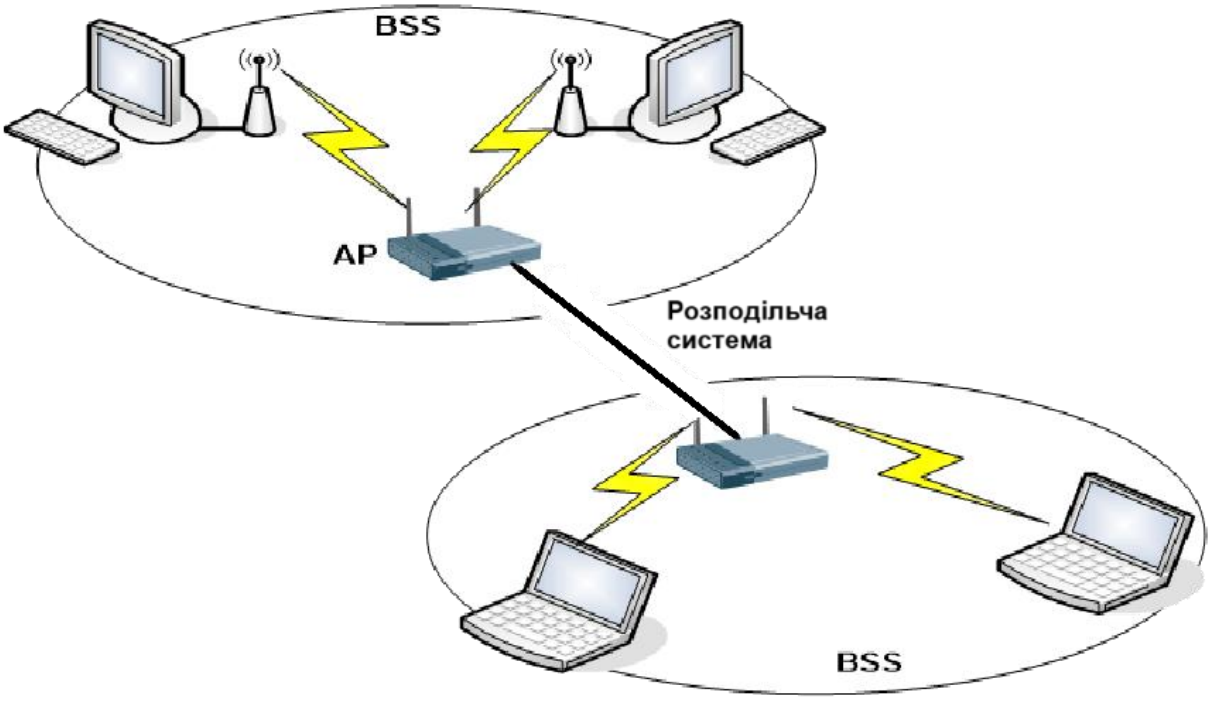

Рисунок 1.6 - Розширена зона обслуговування ESS бездротової мережі

2.4 Бездротове обладнання, що застосовується у Wi-Fi мережах

Сьогодні бездротові мережі дають змогу надати під'єднання користувачів там, де ускладнене кабельне підключення або необхідна повна мобільність. При цьому бездротові мережі без проблем взаємодіють із дротовими мережами.

Усі точки доступу можна розділити за способом підключення: через USB-порт і порт підключення *Ethernet* - *RJ45*. Останні мають найбільший успіх, оскільки найпростіші в налаштуванні та управлінні, а також володіють більшою швидкістю передачі в локальну мережу. Точки доступу можуть бути кімнатного (*in door*) і всепогодного (*out door*) виконання. Для створення бездротової мережі всередині приміщень використовують кімнатний варіант приладу. Він має меншу вартість і, як правило, більший естетичний вигляд. Працюють такі точки доступу в межах однієї або декількох кімнат. На відкритих ділянках місцевості (пряма видимість) можлива робота на відстані до 300 метрів з використанням стандартних всеспрямованих антен. Точки доступу всепогодного виконання призначені для створення радіомережі між

будівлями. Залежно від типів антен такі пристрої здатні організовувати канали зв'язку на відстані близько 3-5 км. Максимальна дальність бездротового каналу зв'язку помітно збільшується при використанні підсилювачів. У цьому разі довжина радіоканалу досягає 8-10 км. Пристрої типу точка доступу представлені на рис. 2.7.

Великий інтерес викликають бездротові точки доступу, що об'єднують у собі функції інших пристроїв, наприклад, високошвидкісного бездротового широкосмугового маршрутизатора з вбудованим комутатором *Fast Ethernet*. Маршрутизатор дає змогу швидко і легко налаштувати загальний доступ до Інтернету для дротової або бездротової мережі або організувати спільне використання широкосмугового каналу зв'язку та *кабельного/DSL* модему вдома або в офісі.

а) б) в) г)

Рисунок 2.7 - Види точок доступу: а), б) - внутрішні; в), г) - зовнішні

Для під'єднання до бездротової мережі *Wi-Fi* достатньо мати ноутбук або кишеньковий персональний комп'ютер (КПК) з під'єднаним *Wi-Fi* адаптером.

Будь-який бездротовий *Wi-Fi* адаптер має відповідати кільком вимогам:

1. необхідна сумісність зі стандартами;
2. робота в діапазоні частот 2,4 ГГц - 2,435 ГГц (або 5 ГГц);
3. підтримувати протоколи *WEP* і бажано *WPA*;
4. підтримувати два типи з'єднання "точка-точка", і "комп'ютер сервер";

5. підтримувати функцію роумінгу.

Існує три основні різновиди *Wi-Fi* адаптерів, що розрізняються за типом підключення:

1. Підключаються до *USB* порту комп'ютера. Такі адаптери компактні, їх легко налаштовувати, а *USB* інтерфейс забезпечує функцію "гарячого підключення";

2. Підключаються через *PCMCIA* слот (*CardBus*) комп'ютера. Такі пристрої розташовуються всередині комп'ютера (ноутбука) і підтримують будь-які стандарти, що дають змогу передавати інформацію зі швидкістю до 108 Мбіт/с;

3. Пристрої, інтегровані безпосередньо в материнську плату комп'ютера. Найперспективніший варіант. Такі адаптери встановлюються на ноутбуки серії *Intel Centrino*. І, в даний час використовуються на переважній більшості мобільних комп'ютерів. Усі види бездротових адаптерів представлені на рис. 2.8.

а) б) в)

Рисунок 2.8 - Бездротові адаптери: а) з *USB* портом, б) формату *PCMCIA*, в) вбудований у материнську плату

2.4 IEEE 802.11b

IEEE 802.11b — це розширення специфікації IEEE 802.11 DSSS, що допускає швидкості передачі даних 5,5 і 11 Мбіт/с. Швидкість передачі роздробленого сигналу дорівнює 11 МГц, тобто така ж, як у вихідній схемі

DSSS, отже, обидві схеми вимагають однакової смуги. Для одержання більш високої швидкості при незмінній смузі і швидкості передачі роздробленого сигналу використовується маніпуляція додатковим кодом (complementary code keying — ССК).

Модуляція ССК є досить складною. Приклад схеми ССК приводиться на рис. 2.9 для швидкості передачі 11 Мбіт/с. Вхідні дані розглядаються як восьмибітові блоки зі швидкістю 1,375 МГц (8 біт/символ х 1,375 МГц = 11 Мбіт/с). Шість бітів відображаються в одну з 64 кодових послідовностей, при цьому застосовується матриця Уолша 8х8. Результат плюс два біти, що залишилися подаються на вхід модулятора QPSK (quadrature phase-shift keying - квадратурна фазова маніпуляція).

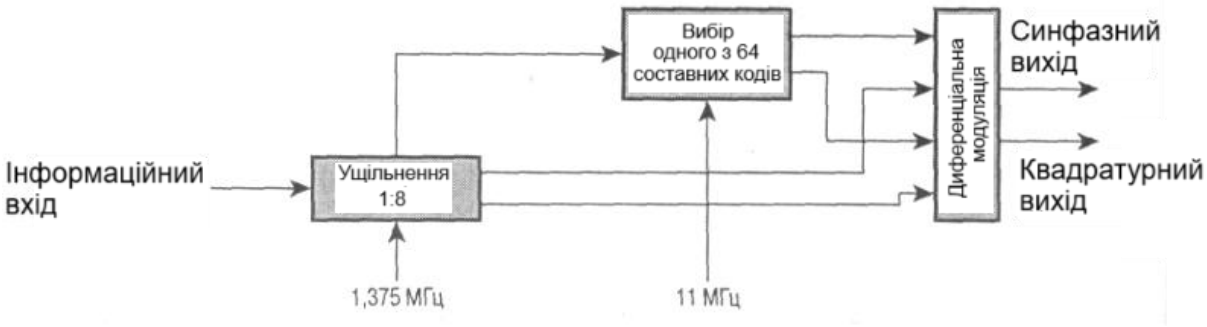

Рисунок 2.9 - Схема модуляції ССК для швидкості 11 Мбіт/с

Для підтримки дуже зашумлених середовищ, а також роботи на великих відстанях, мережі 802.11b використовують динамічне зрушення швидкості, що дозволяє автоматично змінювати швидкість передачі даних у залежності від властивостей радіоканалу. Наприклад, користувач може підключитися з максимальною швидкістю 11 Мбіт/с, але в тому випадку, якщо підвищиться рівень перешкод, або користувач видалиться на велику відстань, мобільний пристрій почне передавати на меншій швидкості – 5,5, 2 або 1 Мбіт/с. У тому випадку, якщо можливо усталену роботу на більш високій швидкості, мобільний пристрій автоматично почне передавати з більш високою швидкістю.

Зсув швидкості – механізм фізичного рівня, і є прозорим для вищестоящих рівнів і користувача.

2.5 IEEE 802.11a

Специфікація IEEE 802.11a використовує смугу 5 ГГц. На відміну від специфікації 2,4 ГГц, тут застосовується не розширений спектр, а ортогональне частотне ущільнення (OFDM). Мається до 52 що піднесуть, котрі модулюються з використанням схем BPSK, QPSK, 16-QAM або 64-QAM, у залежності від необхідної швидкості передачі. Відстань між що піднесуть складає 0,3125 МГц. У результаті підвищується пропускна здатність каналу і якість сигналу.

До недоліків 802.11a відносяться більш висока споживана потужність радіопередавачів для частот 5 ГГц, а так само менший радіус дії (устаткування для 2,4 ГГц може працювати на відстані до 300 м, а для 5 ГГц - близько 100 м).

2.6 IEEE 802.11g

Цей стандарт розроблений для більш високих значень пропускної здатності бездротових з'єднань у 54 Мбіт/с , працюючи на тій же частоті що і 802.11b (2,4 ГГц) він забезпечує в такий спосіб зворотну сумісність обох стандартів.

Використовується метод прямої послідовності з рознесенням сигналу по широкому діапазоні (DSSS) і метод мультиплексування з ортогональним розподілом частот (OFDM), на рис. 2.10 такий перехід представлений схематично.

Рисунок 2.10 - Радіус дії в офісному середовищі

Швидкість передачі в 54 Мбіт/с досягається у відкритому офісному середовищі на відстані до 14 м. При наявності якої-небудь перешкоди (приміром, перегородки), що повинне бути переборено, швидкість знижується. Чутливість при 11 Мбіт/с (у випадку модуляції CCK/802.11b) і чутливість при 12 Мбст/с (у випадку модуляції OFDM/802.11g), як правило, збігаються, тому така швидкість передачі може підтримуватися на відстані до 40 м від крапки доступу.

Особливості і переваги стандарту 802.11g:

• Швидкість передачі даних — до 54 Мбіт/с;

• Підвищений рівень безпеки;

• Сумісність з більш ранніми стандартами;

• Збільшена дальність передачі даних.

Результати порівняння стандартів 802.11 a,b і g зведені в табл. 2.3.

Таблиця 2.3 - Порівняння стандартів 802.11 a,b і g

	802.11b	**802.11a**	**802.11g**
Стандарт принят	Вересень 1999	Вересень 1999	Липень 2003
Смуга пропускания	83.5 МГц	300 МГц	83.5 МГц
Смуга частот (ГГц)	2.40 – 2.4835	5.15 – 5.35, 5.725 – 5.825	2.40 – 2.4835
Кількість непересекающихся каналов	3	8	3
Швидкість передачі (Мбіт/с)	1, 2, 5.5, 11, 22	6,9,12,18,24,36, 48,54	1, 2, 5.5, 11, 22, 6, 9, 12, 18, 24, 36, 48, 54
Тип модуляції	DSSS	OFDM	DSSS, OFDM

3 ПРОЕКТУВАННЯ ОФІСНОЇ БЕЗДРОТОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ТА ТЕСТ МЕРЕЖЕВОГО УСТАТКУВАННЯ

3.1 Проведення досліджень

Перед розгортанням бездротової мережі необхідно провести дослідження на місці. Для визначення зон покриття усередині будівель при створенні бездротових локальних мереж, на даний час використовуються два основні підходи : експериментальний і розрахунково-експериментальний. Розрахунковий вимагає спеціального програмного забезпечення і серйозного аналізу будівлі (з погляду геометрії приміщень, матеріалів стін і перекриттів і т.д.), але обов’язково необхідно проводити експериментальну перевірку і, при потребі, коректувати топологію системи (наприклад, при виявленні зон невпевненого прийому сигналу або недостатнього перекриття зон дії базових станцій).

На практиці багато що залежить від досвіду фахівців-установників. Можна або відразу намітити місця установки з хорошим перекриттям або потрібно спочатку "промацати" всю будівлю за допомогою спеціального приладу і клієнтського комп'ютера. Це робиться в цілях економії, оскільки дозволяє уникнути установки зайвого устаткування.

Процес дослідження включає:

- збір креслень будівлі і схем проводки, розташування електричних систем, розеток, структурних елементів (металевих перегородок, стін, дверних отворів);

- оцінку зони розповсюдження радіосигналу, включаючи вибір зон установки компонентів для забезпечення мінімальної втрати сигналу. Визначення оптимальної схеми розміщення точок доступу і антен;

- оцінку інтерференції каналів, включаючи тестування для забезпечення відсутності перекриття радіопередач;

- вибір положення антени, включаючи положення все направленої антени і направленої антени;

- визначення прийому, зокрема подолання інтерференції і загасання сигналу за допомогою розміщення в певних місцях декількох антен;

- оцінку електричних систем, зокрема оцінка альтернатив підключення точки доступу до електромережі для запобігання деградації продуктивності у зв'язку з випадковими або неминучими електричними проблемами.

Також слід закрити двері всіх офісів і приміщень перед початком дослідження, щоб оцінити рівень прийому на найнижчому рівні.

3.2 Обладнання необхідне для побудови мережі

Для того, щоб забезпечити зону покриття конференц-залу, розташуємо 2 бездротові пристрої SMC 2804WBR. До місця їх розміщення повинні бути підведені всі необхідні кабелі. Причому чим вище місце, в якому розташовується передавачі, тим більше радіус дії. Якщо ж все одно буде недостатньо зони покриття, що забезпечується даними пристроями, його можна модернізувати. Для збільшення площі покриття можна замінити стандартні антени або на антени з великим коефіцієнтом підсилення, або на направлені (секторні). Якихось серйозних обмежень щодо вентиляції і температури для місцеположення пристроїв немає. Природно не рекомендується встановлювати їх поблизу нагрівальних приладів і місць підвищеної вологості, а також в запорошених приміщеннях. В нашому випадку будь-яке місце в конференц-залі задовольняє цим вимогам (рис. 3.1).

Також для побудови бездротової локальної мережі конференц-залу нам необхідні:

- 5 Laptop (робочі місця);
- цифровий проектор;
- екран для перегляду презентацій;
- мережевий кабель 1000 Мбіт/с Ethernet LAN.

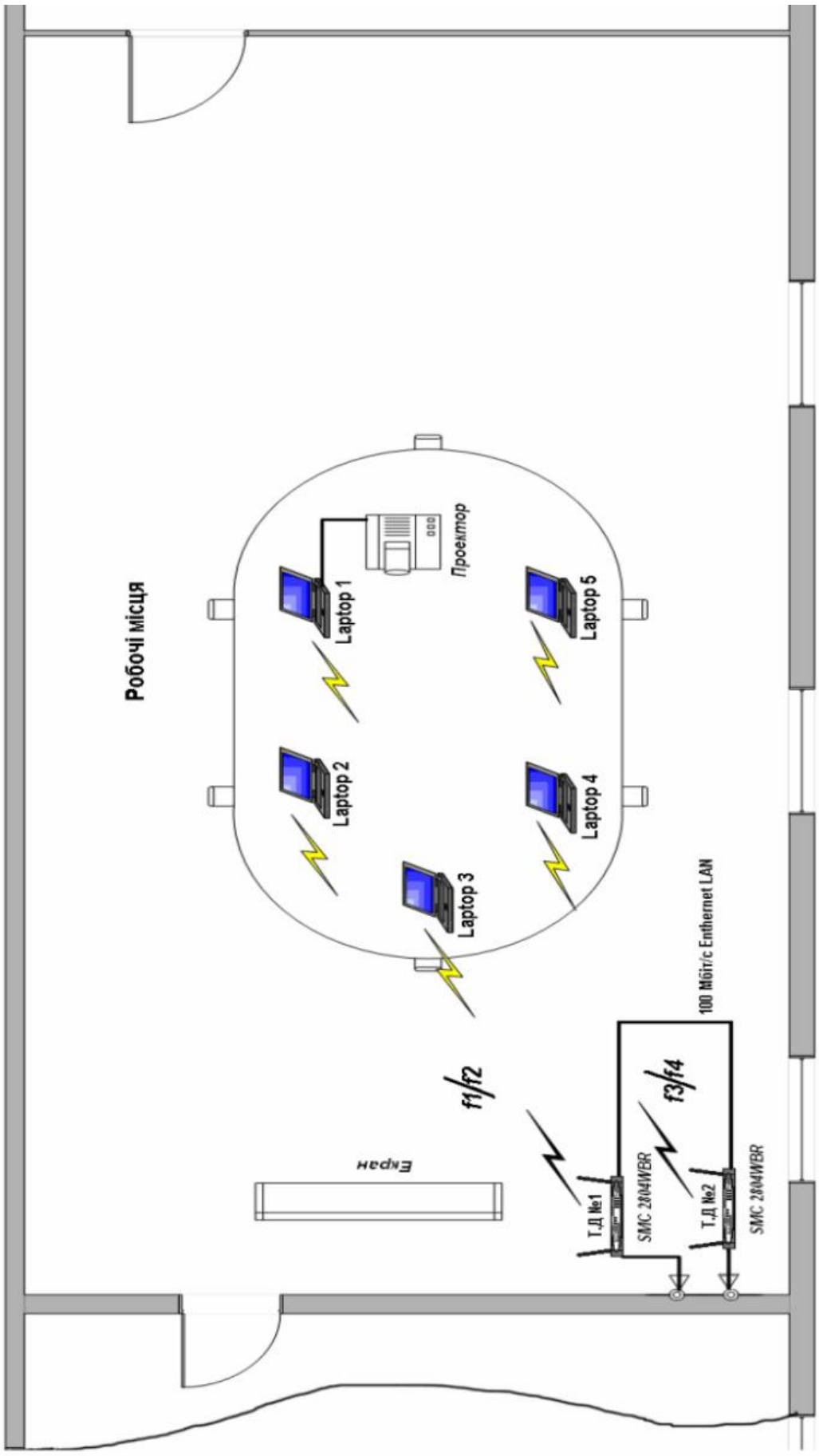

Рисунок 3.1 - План-схема конференц-залу

3.3 Підключення та налагодження Laptop та проектора

Для організації офісної локальної мережі ми використовуємо Laptop наступної конфігурації:

- процесор Intel Core I5;
- пам'ять 8 Гб DDR4;
- дротяний 1000 мегабітний мережевий адаптер;
- бездротовий мережевий адаптер стандарту 802.11g SMC2802W з підтримкою технології Nitro;
- операційна система Windows 11.

Зручно встановивши робочі місця й налагодивши їх підключаємо цифровий проектор.

3.4 Підключення маршрутизаторів SMC

Підключення маршрутизатора здійснюється за допомогою достатньо зручного і інтуїтивно зрозумілого web-інтерфейсу. До речі, інтерфейси у всіх таких пристроїв компанії SMC виконані в єдиному стилі, так що якщо у вас був досвід роботи з одним із пристроїв даної серії, то більше проблем виникнути не повинно. Після підключення маршрутизатора, для того, щоб перейти до його настройки, досить набрати в будь-якому браузері адресу маршрутизатора. Природно, ваша машина повинна знаходитися в тій же мережі, що і маршрутизатор. Він має перед встановлену IP-адресу 192.168.2.1, тому вам потрібно встановити на одному з клієнтів IP-адреса вигляду 192.168.2.X, маска 255.255.255.0. Пароль при першому вході указувати не потрібно. Відзначимо, що окремої Windows-утиліти для настройки маршрутизатора не існує, тому всі настройки необхідно виконувати через web-інтерфейс. Вікно запрошення, що вітає вас після введення пароля, показано на рисунку нижче (рис. 3.2). Варто відзначити, що SMC2804WBR, як і його попередник, не підтримує множинні адміністративні підключення. При спробі такого ви побачите

попередження про те, що адміністративний вхід в систему виконаний з машини з вказаною IP-адресою.

Рисунок 3.2 - Вхід в систему

В другій кімнаті розташований файловий сервер, 2 точки доступу, маршрутизатор та сегмент офісних клієнтських хостів, що показані на рис. 3.3.

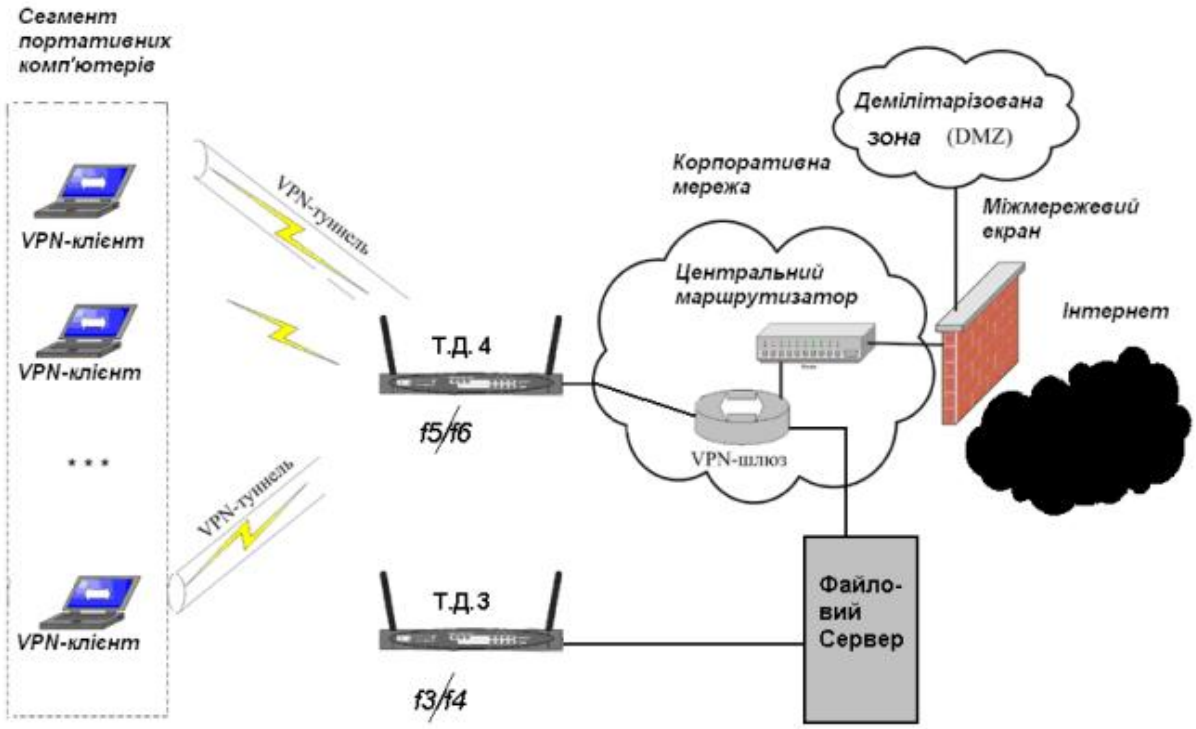

Рисунок 3.3 - Структурна схема спроектованої бездротової мережі в офісі

Меню системи (рис. 3.4).

Рисунок 3.4 - Меню системи

Закладки WAN и LAN.

Тут (рис. 3.5) можна вибрати один з декількох варіантів доступу в Інтернет:

- з динамічним отриманням IP-адреси у провайдера;
- PPoE;
- PPTP;
- BigPond;
- статична IP-адреса.

Такий набір дозволяє успішно використовувати цей маршрутизатор практично де завгодно: у Європі з її повсюдним розповсюдженням xDSL і в Австралії з її Telstra BigPond Cable Network

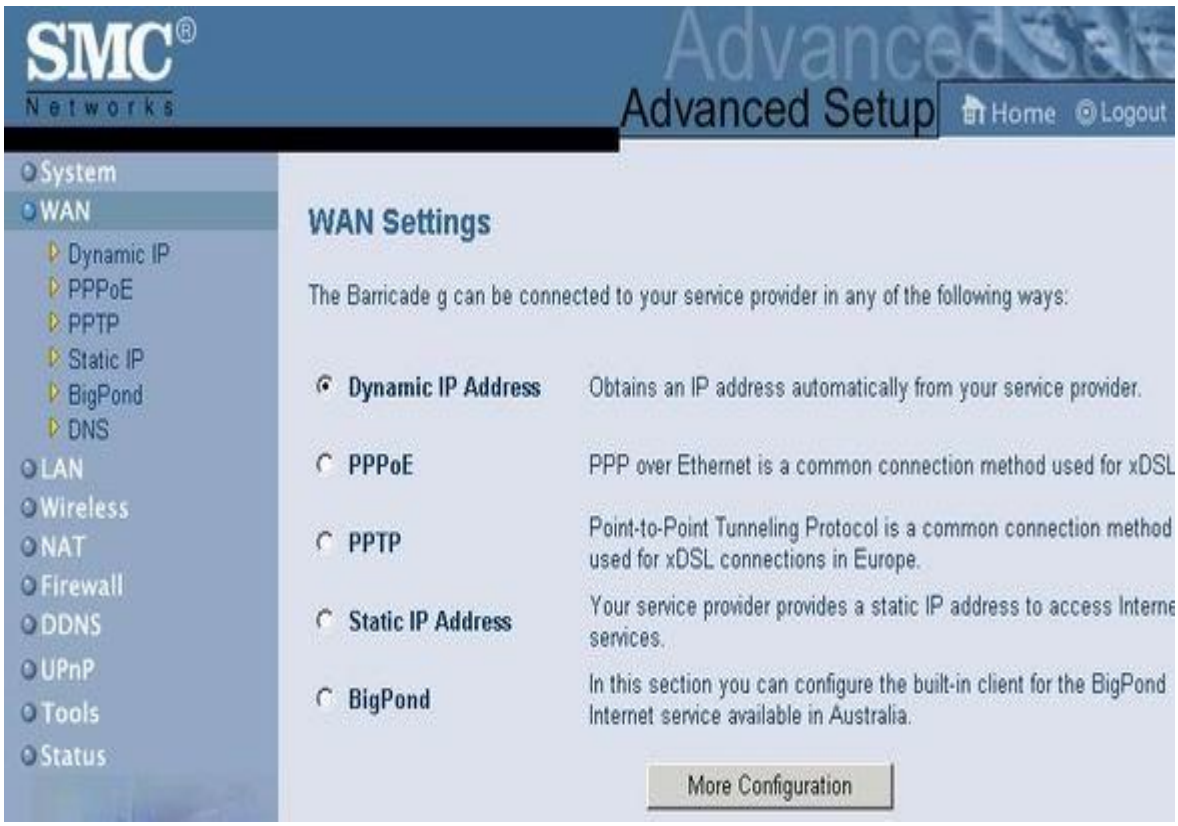

Рисунок 3.5 - Закладка WAN

У розділі LAN вказується внутрішній IP-адрес маршрутизатора, а також включається або виключається DHCP-сервер, якого теж можна налагодити в цьому пункті (рис. 3.6).

Рисунок 3.6 - Закладка LAN

Закладка Wireless (рис. 3.7).

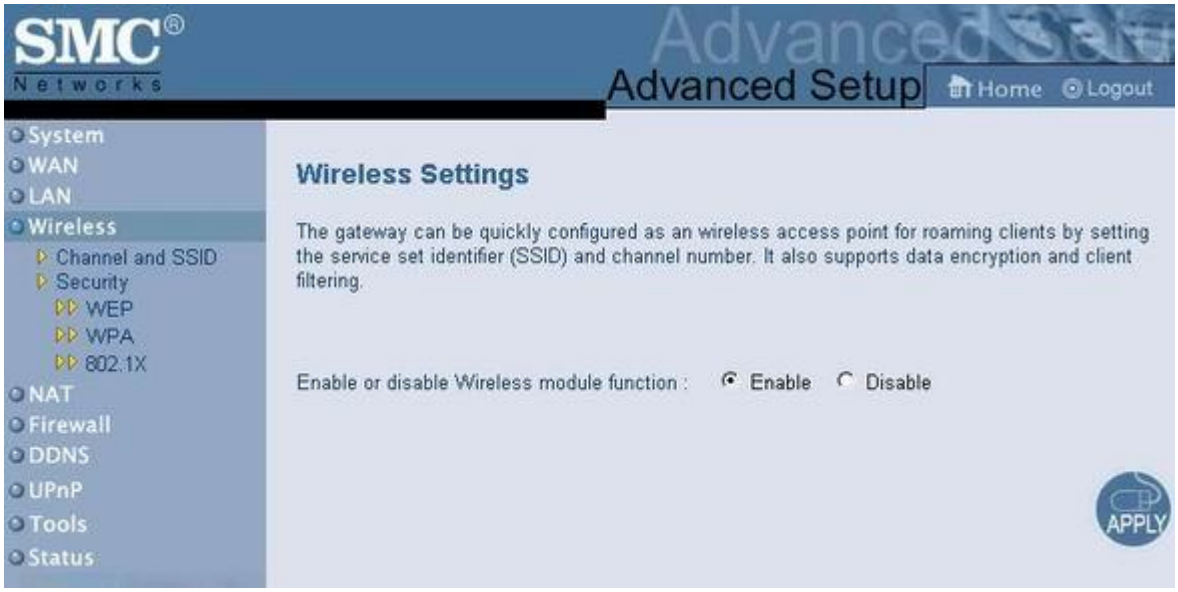

Рисунок 3.7 - Закладка Wireless

Тут можна налагодити такі його параметри: як SSID, швидкість роботи, канал, преамбула, включити/відключити широкомовлення SSID,

режим роботи, вибір швидкості передачі, канал і використання технології Nitro, яка дозволяє підвищити швидкість роботи бездротового мережевого устаткування. Причому компанія Intersil, що розробила цю технологію заявляє що все реалізується тільки програмним шляхом - грою з розміром пакету і затримками. Використання Nitro дозволяє збільшити швидкість роботи мережі в режимі тільки-11g на 30%, а в режимі 11b і 11g - в три рази. Виробник передбачив можливість відключення використання бездротового сегменту. Огляд характеристик пристрою приведений в табл. 3.1.

Таблиця 3.1 - Огляд налаштувань бездротового маршрутизатора SMC2804WBR

Інформація щодо підтримки WAN	
WAN інтерфейс	Один порт 100/1000 Ethernet
Підтримка комутаційного доступу в WAN	Ні
Особливості WAN	Порт WAN автоматично знаходить MDI/MDI-X
Аутентифікація	
PPPoE	Так
PPTP	Так
BigPond	Так
Установка імені хосту	Так
Установка MAC-адреси WAN	Так
LAN DHCP	
Установка пула адрес	Так
Відключення DCHP LAN сервера	Так
Зауваження щодо DHCP LAN сервера	Можна встановити діапазон орендованих DCHP адрес Неможливо зарезервувати IP-адреси
Адміністрування	
Спосіб адміністрування	HTTP
Зауваження по адмініструванню	- зручний інтерфейс адміністратора через вбудований HTTP-сервер; - тільки одне адміністративне підключення
Спосіб оновлення	HTTP

Безпека.

Варто приділяти особливу увагу безпеці інформації при бездротовій передачі. Тут виробники зробили великий крок вперед: окрім стандартної можливості використання WEP шифрування трафіку з використанням ключів завдовжки до 128 біт (64 або 128) маршрутизатор підтримує новий

стандарт безпеки бездротових мереж - WPA (Wi-Fi Protected Access) і засоби аутентифікації 802.1x (автоматичний розподіл сертифікатів сервером - звичайно використовується сервер RADIUS), що достатньо актуально сьогодні. Причому, WPA може використовувати не тільки 802.1x, але і PSK (Pre-Shared key). Є можливість сумісного використання обох засобів безпеки: WEP і WPA (рис. 3.8), але у такому разі WEP буде слабким місцем всієї мережі, тому такий варіант використовуватися не буде.

Рисунок 3.8 - Вікно налаштування WEP

Вікно налаштування WPA показане на рис. 3.9.

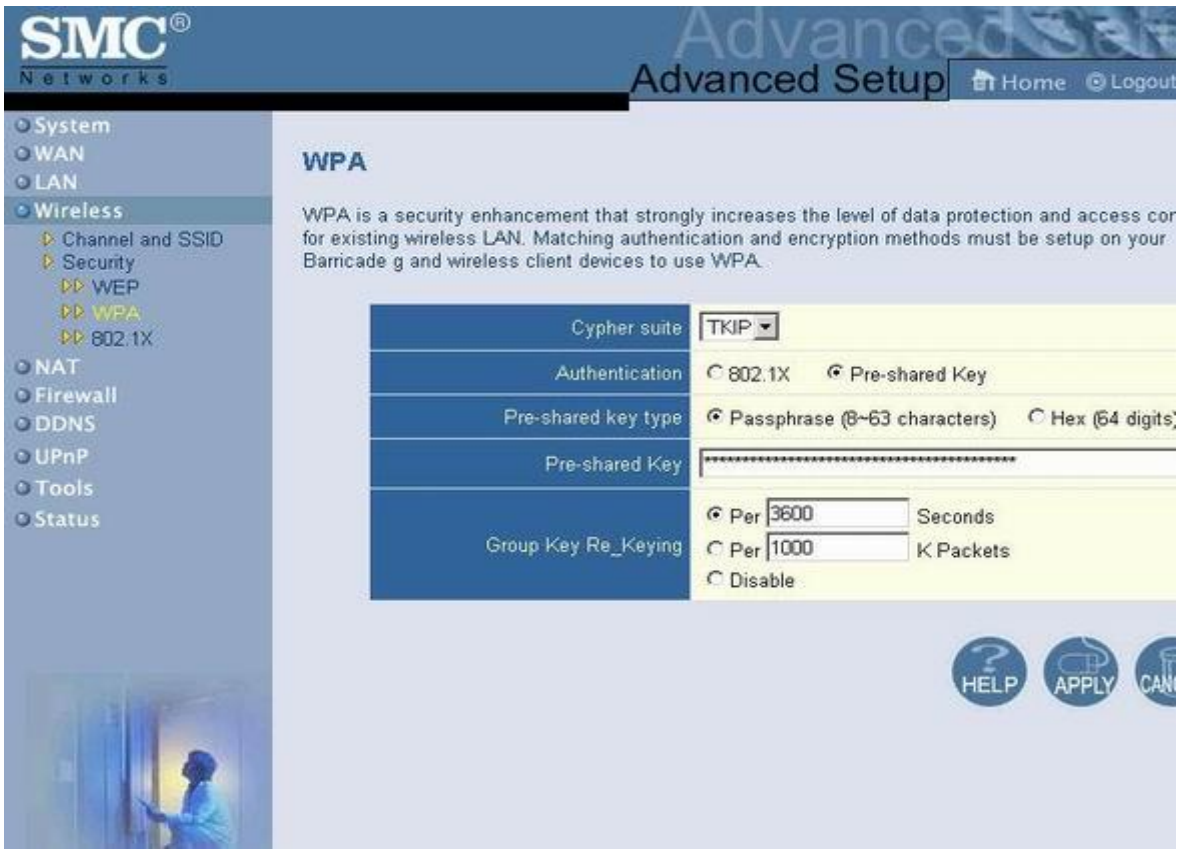

Рисунок 3.9 - Вікно налаштування WPA

Вікно налаштування 802.1X на рис. 3.10.

Рисунок 3.10 - Вікно налаштування 802.1X

Слід згадати про криптографічну діру в алгоритмі шифрування WEP, із-за якої різні зашифровані пакети даних мають схожість, що достатньо для того, щоб, захопивши декілька таких пакетів, шляхом їх аналізу одержати ключ шифрування.

Стандарт WPA позбавлений цієї проблеми і забезпечує вищий ступінь захисту даних. Цей стандарт припускає аутентифікацію, шифрування і перевірку цілісності переданих даних. Короткі характеристики стандартів безпеки 802.11 представлені табл. 3.2.

Таблиця 3.2 - Розвиток стандартів безпеки 802.11

Стандарт безпеки	**Коротка характеристика**	**Переваги**	**Недоліки**
WEP	Шифрування RC4; статичні ключі й необов'язкова ідентифікація користувача	Забезпечення мінімальної безпеки	Багато дірок безпеки; необхідні додаткові засоби
WPA	Шифрування TKIP, динамічні ключі й ідентифікація користувачів за допомогою EAP, RADIUS	Більш надійний стандарт, сумісний з WEP; легко інтегрується з існуючими WLAN-рішеннями	Проміжні рішення, котрі можливо використовувати до прийняття специфікації 802.11i
802.11i	Шифрування AES, WRAP, управління ключами в стандарті 802.11i, обов'язкова ідентифікація користувачів	Криптостійкий стандарт, надійний механізм управління ключами	Потреба в оновленні пристроїв

Закладка NAT.

В SMC2804WBR реалізована NAT - можливість трансляції мережевих адрес, що дозволяє діставати доступ до Інтернет сервісів декільком користувачам, використовуючи при цьому одне або декілька з'єднань і одні облікові дані, і, крім того, ще захищає внутрішню мережу від зовнішніх атак. Маршрутизатор 2804WBR дозволяє використовувати до десяти зовнішніх IP-адрес для перенаправлення їх на різні внутрішні IP-адреси або діапазони IP адрес (рис. 3.11).

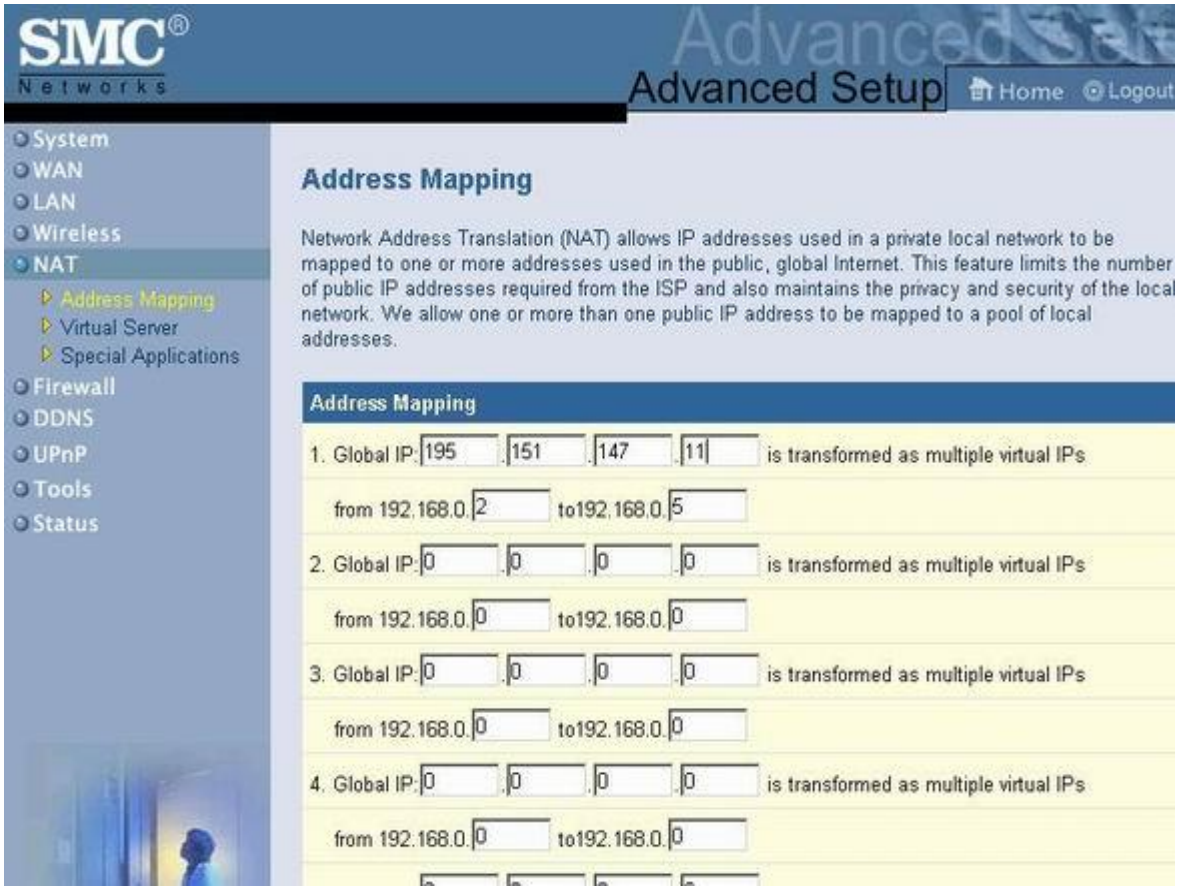

Рисунок 3.11 - Вікно налаштування трансляцій мережевих адрес

SMC2804WBR може надати також можливість організації віртуальних серверів. Він може перенаправляти запити, що поступають на зовнішній порт (або групу портів) на порт якої-небудь машини, розташованої усередині мережі (рис. 3.12).

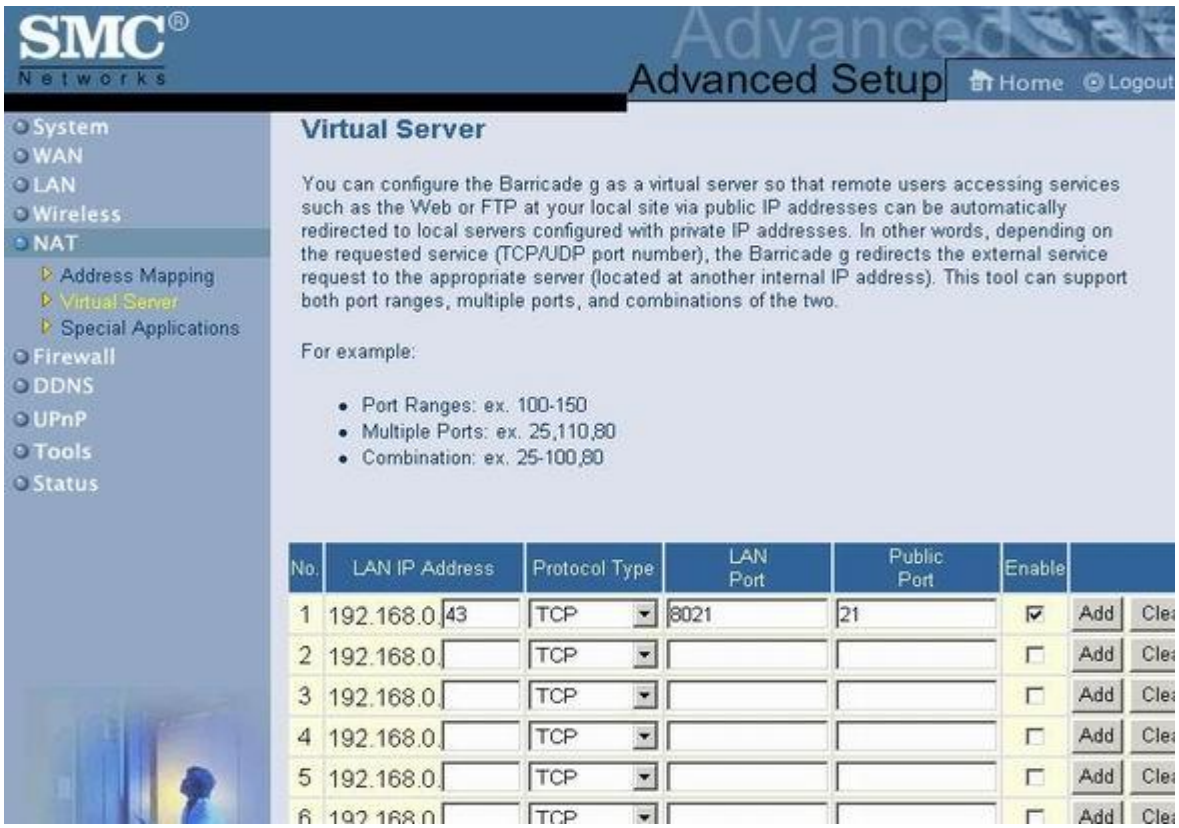

Рисунок 3.12 - Вікно налаштування віртуального серверу

Окрім постійних портів SMC2804WBR також можна налаштувати і для роботи з динамічно визначуваними портами. Для цього служить розділ Special Applications (рис. 3.13).

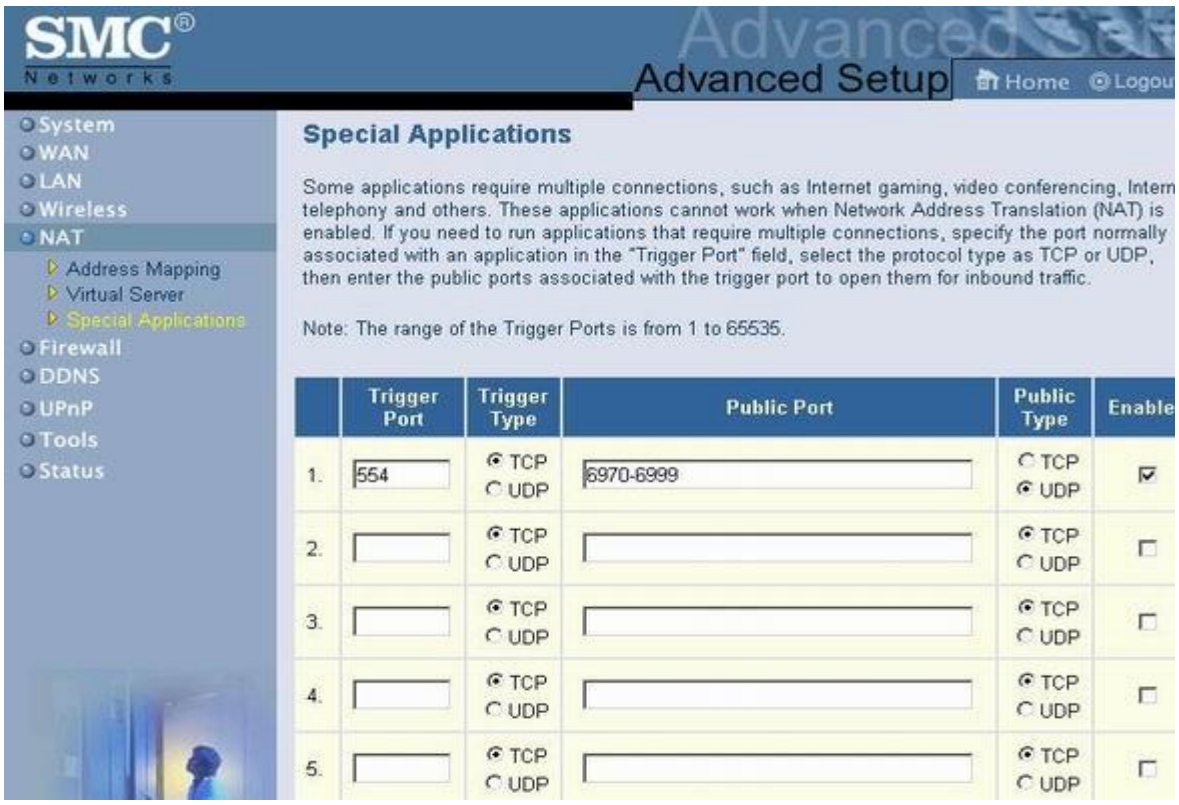

Рисунок 3.13 - Вікно налаштування Special Applications

Розділ Firewall дозволяє включити або відключити вбудований брандмауер, який захищає внутрішню мережу від різних видів мережевих атак і, в той же час, накладає різні обмеження. Як ви знаєте, активація брандмауера дозволять уберегти внутрішню мережу від різних видів мережевих атак і, в той же час, накладає різні обмеження. Так, за брандмауером буде вельми проблематично використовувати деякі види програмного забезпечення, тому, якщо вам необхідний необмежений доступ в мережу на одній або декількох машинах, ви можете помістити їх в демілітаризовану зону. SMC2804WBR пропонує демілітаризовані зони для восьми машин. Тобто зі всієї мережі ви можете вибрати від однієї до восьми машин, які знаходитимуться в DMZ.

Контроль доступу Access Control (рис. 3.14) традиційно задає правила, що вирішують або забороняють передачу певного типу трафіка. Традиційно можна зробити вибір серед установок, які пропонують такі сервіси як HTTP, SMTP, NNTP POP3, HTTPS, FTP та інші.

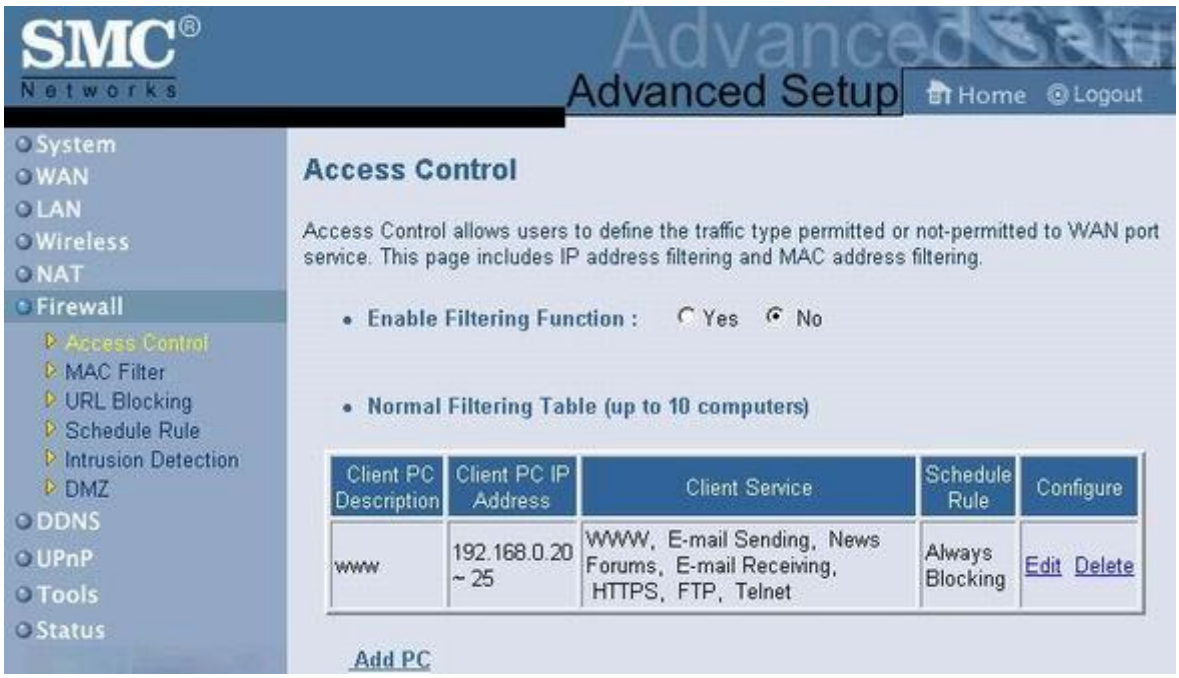

Рисунок 3.14 - Вікно налаштування Access Control

Нижче слідує вікно фільтрації по MAC-адресах (рис. 3.15), тут можна вказати MAC-адреси тих машин, з яких надалі ви зможете дістати доступ до маршрутизатора, для всіх інших, відповідно, доступ буде заборонений. Максимальне число дозволених MAC-адрес – 32.

Рисунок 3.15 - Вікно налаштування MAC-адрес

Наступним пунктом настройки брандмауера є блокування доступу до web-сайтів (рис. 3.16). Є можливість блокування сайту за допомогою вказівки його повної адреси або ключового слова. До речі, блокування застосовуватиметься для користувачів тих машин, для яких вказана опція "*WWW with URL Blocking*".

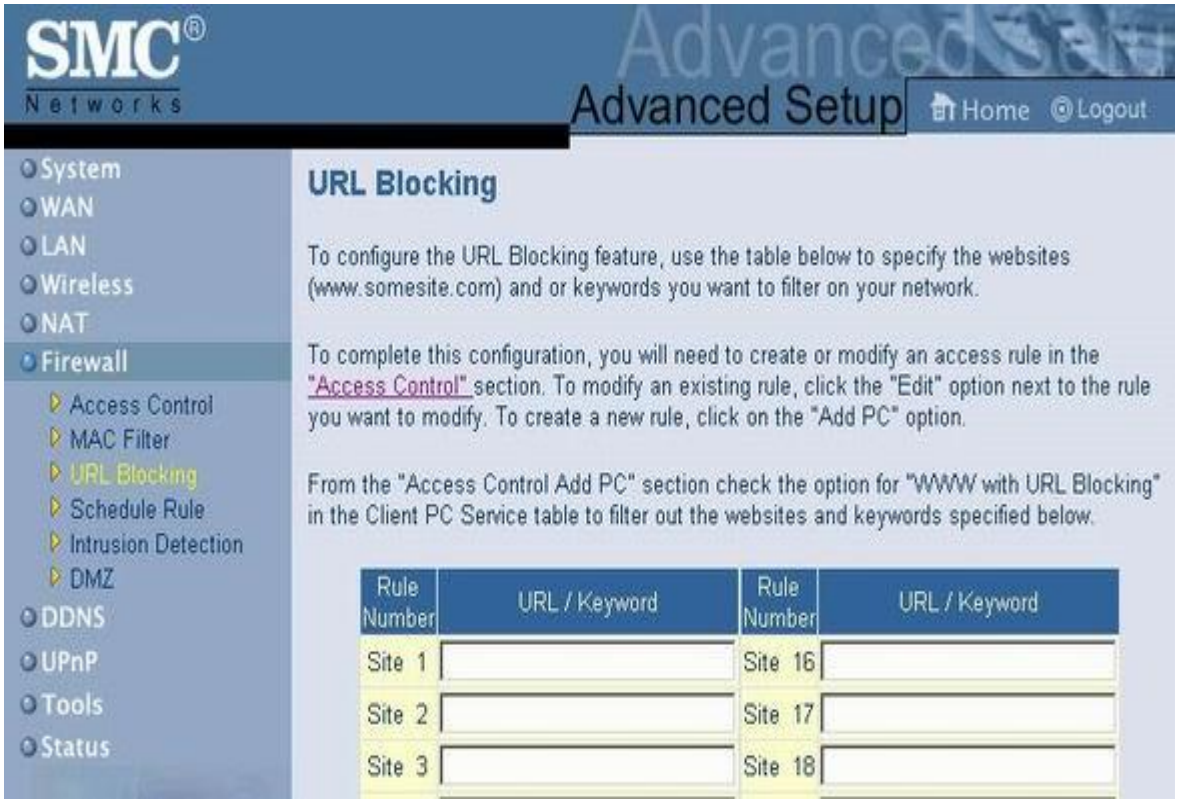

Рисунок 3.16 - Вікно налаштування блокування доступу

Робота з готовими розкладами здійснюється в пункті Schedule Rule (рис. 3.17).

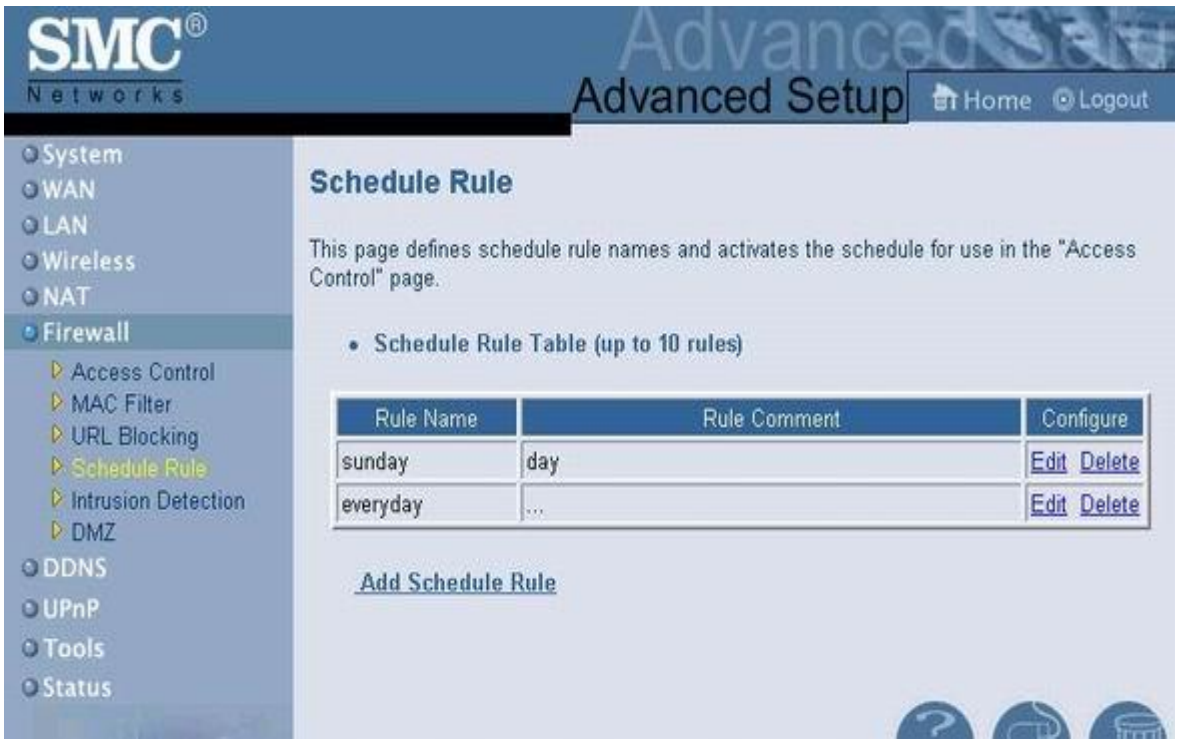

Рисунок 3.17 - Вікно Schedule Rule

На SMC2804WBR реалізована функція виявлення атак (Intrusion Detection), яка дозволяє виявити наступні атаки:

- IP Spoofing;
- Land Attack;
- Ping of Death;
- IP with zero length;
- Smurf Attack;
- UDP port loopback;
- Snork Attack;
- TCP null scan;
- TCP SYN flooding.

Крім того, можна заборонити відсилання відповідей на луна-запити PING, що прийшли на WAN порт. Природно, що при виявленні якої-небудь атаки є можливість повідомлення про неї системного адміністратора, для цього потрібно вказати параметри електронної пошти (рис. 3.18).

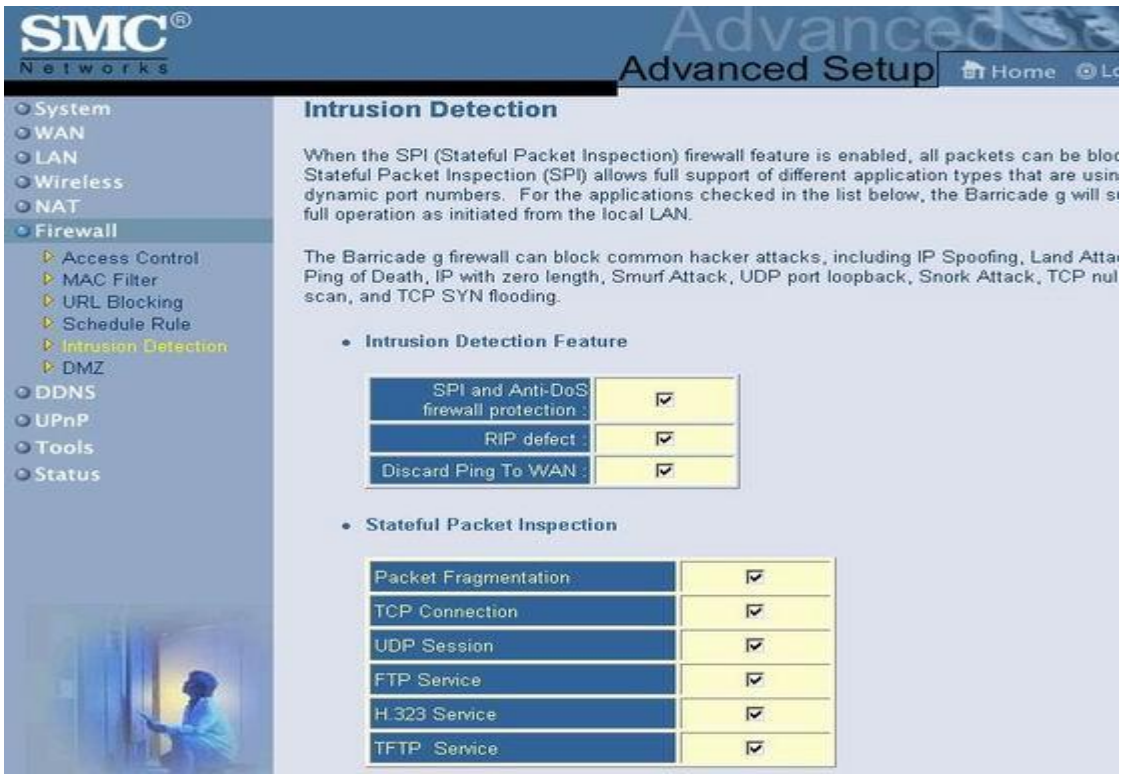

Рисунок 3.18 - Вікно Intrusion Detection

Як ми вже говорили, маршрутизатор підтримує демілітаризовані зони (DMZ) (рис. 3.19). Така можливість може виявитися вкрай необхідною, якщо якесь програмне забезпечення вимагає повного доступу в Інтернет. У DMZ ви можете помістити до восьми комп'ютерів з вашої локальної мережі.

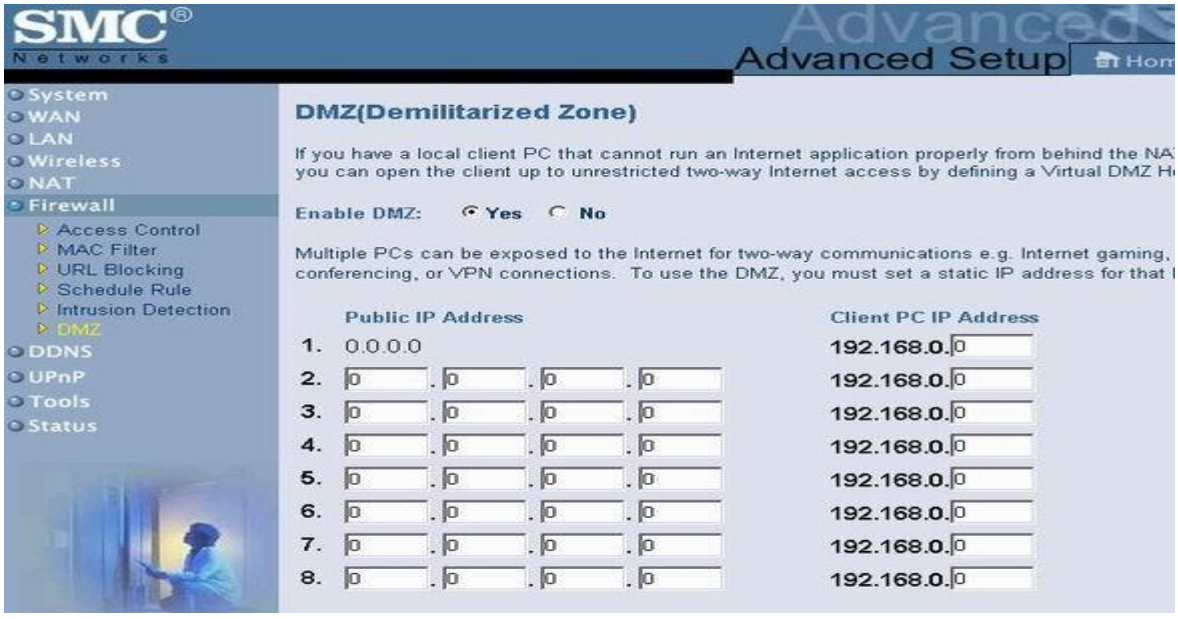

Рисунок 3.19 - Вікно DMZ

В табл. 3.3 приведені брандмауери.

Таблиця 3.3 - Короткий огляд брандмауера

Опції брандмауера	
NAT	Так
SPI	Так
Зовнішній сервер/"DMZ"	Так, до 8
Фільтрація портів	Так
Перенаправлення діапазону портів	Так
Прив’язка портів по події (Trigger)	Так
Управління змістом	
Управління змістом	Так
За адресою	Так
По ключовому слову	Так
Фіксація атак	IP Spoofing, Land Attack, Ping of Death, Ip with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan и TCP SYN flooding, реагування на атаки
Повідомлення атаки	Так, E-mail

У маршрутизаторі також реалізована підтримка DDNS. Дана функція дозволяє організувати web-сайт, поштовий або FTP сервер на одному з комп'ютерів навіть в тому випадку, якщо IP-адреса видається динамічно.

3.5 Тестування продуктивності устаткування

Встановивши без провідні маршрутизатори й налагодивши робочі місця, проведемо тестування продуктивності мережевого устаткування.

Для тестування використовувалася утиліта NetIQ Chariot.

У місці проведення тестування іншого бездротового устаткування стандартів 802.11 a,b або g не було, рівно як і інших пристроїв, що працюють в діапазоні 2,4 ГГц.

Значення "якість сигналу" набуте за допомогою клієнтської утиліти SMC. Конфігурації працювали з тестованим пристроєм безпосередньо, без якихось проміжних пристроїв.

3.5.1 Бездротова частина

Умови тестування продуктивності:

- шифрування WEP: вимкнено;
- швидкість передачі: автоматична;
- енергозбереження вимкнено.

Результати бездротової продуктивності 802.11g при передачі 1 Мбайт даних представлені в табл. 3.4.

Таблиця 3.4 - Продуктивність бездротової частини SMC2804WBR

	Якість сигналу, %	**Швидкість передачі, Мбіт/с**	**Час реакції, мс 10 ітерацій пакетів по 100 байт**	**Пропускна здатність UDP, кбіт/с**	**Втрата даних потоку UDP, %**
Умова 1	100	23,59 без WEP 23,47 з WEP	1 (сер.) 3 (макс.)	499	0
Умова 2	75	22,551	1 (сер.) 4 (макс.)	499	0
Умова 3	55	19,062	2 (сер.) 6 (макс.)	497	1
Умова 4	25	5,957	4 (сер.) 76 (макс.)	443	6

Нижче представлені діаграми, видані утилітою NetIQ Chariot для всіх 4 умов (рис. 3.20 - 3.24).

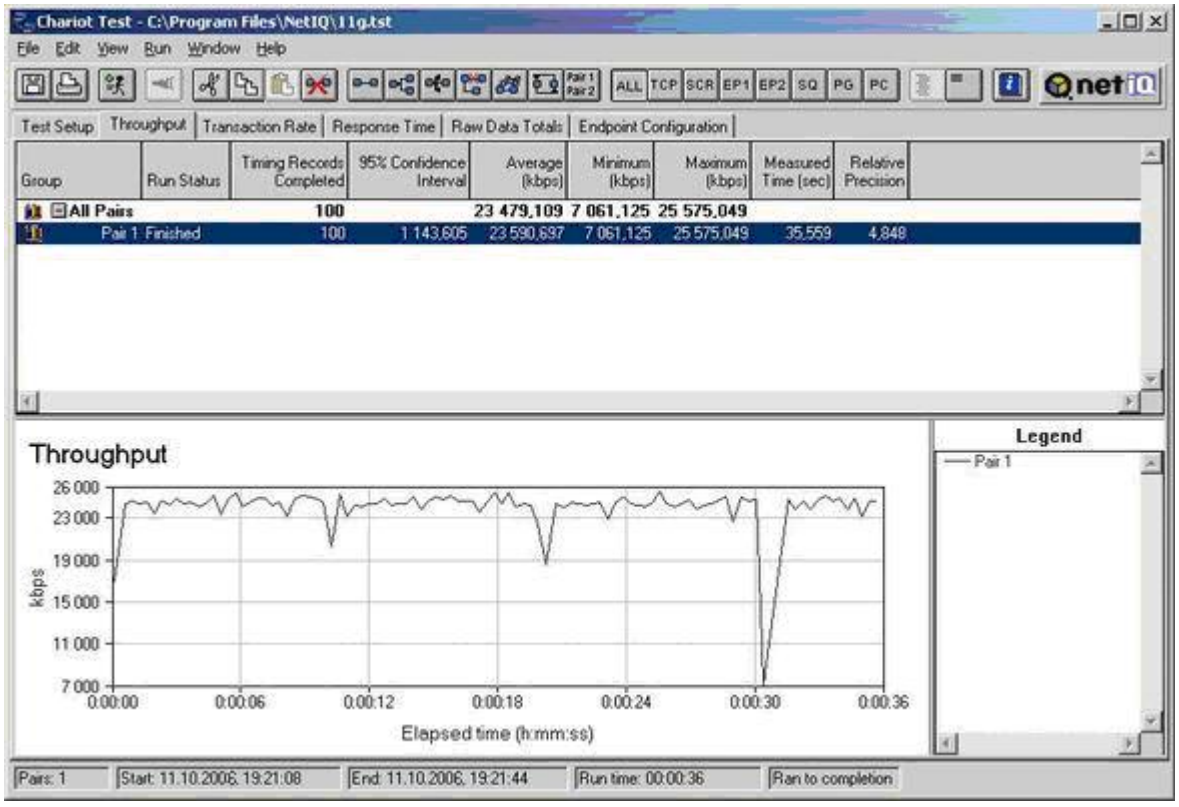

Рисунок 3.20 - Тестування бездротової частини. Умова 1 (без WEP)

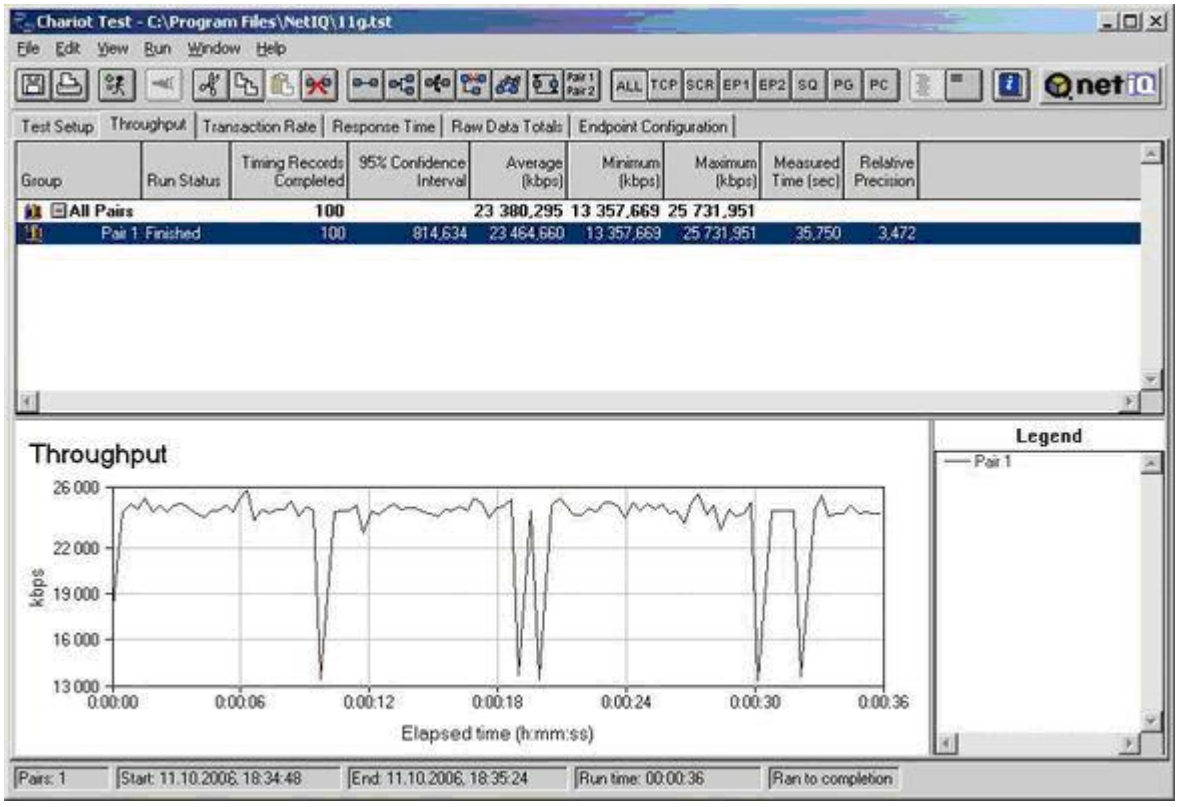

Рисунок 3.21 - Тестування бездротової частини. Умова 1 (з WEP)

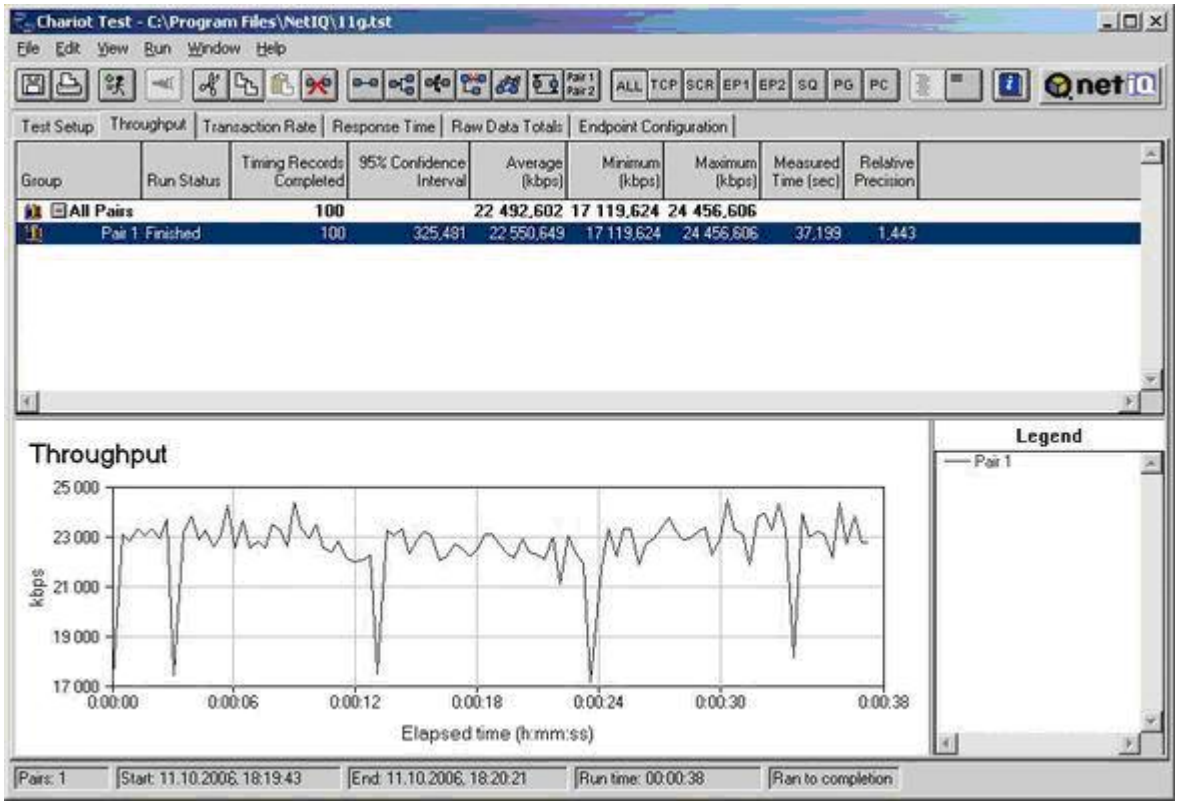

Рисунок 3.22 - Тестування бездротової частини. Умова 2

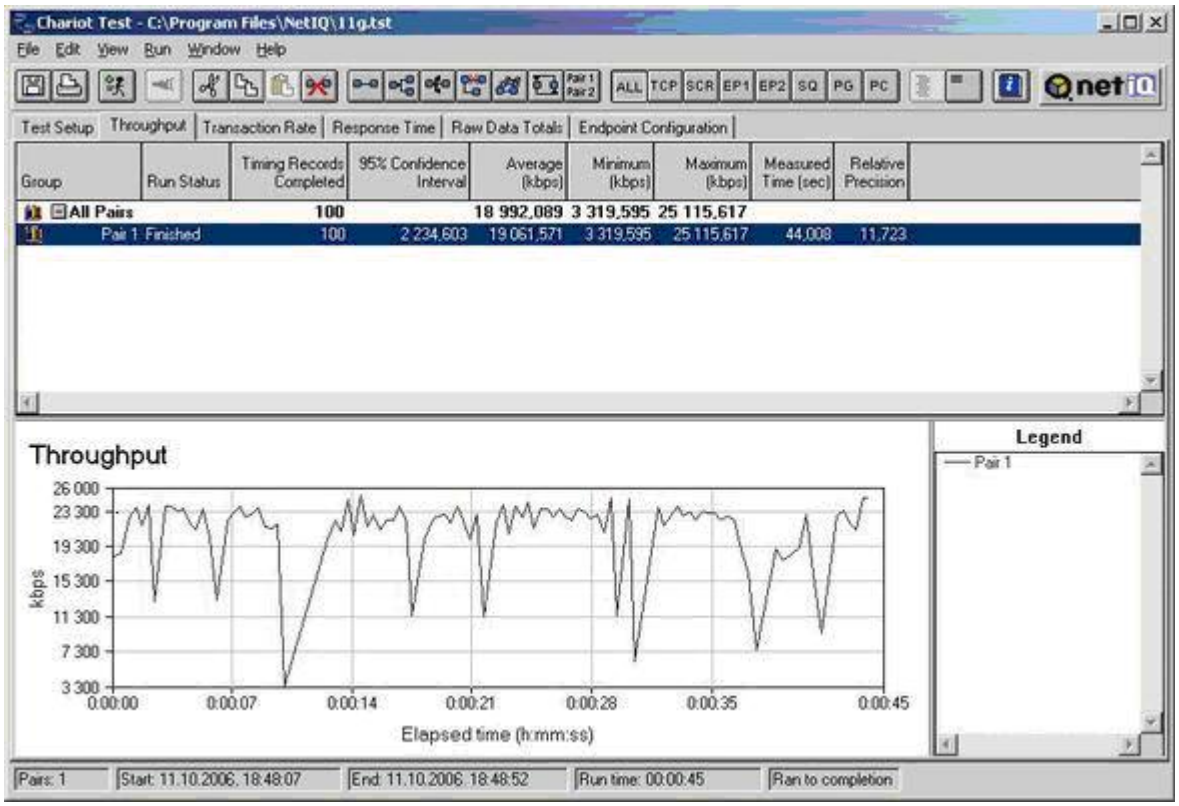

Рисунок 3.23 - Тестування бездротової частини. Умова 3

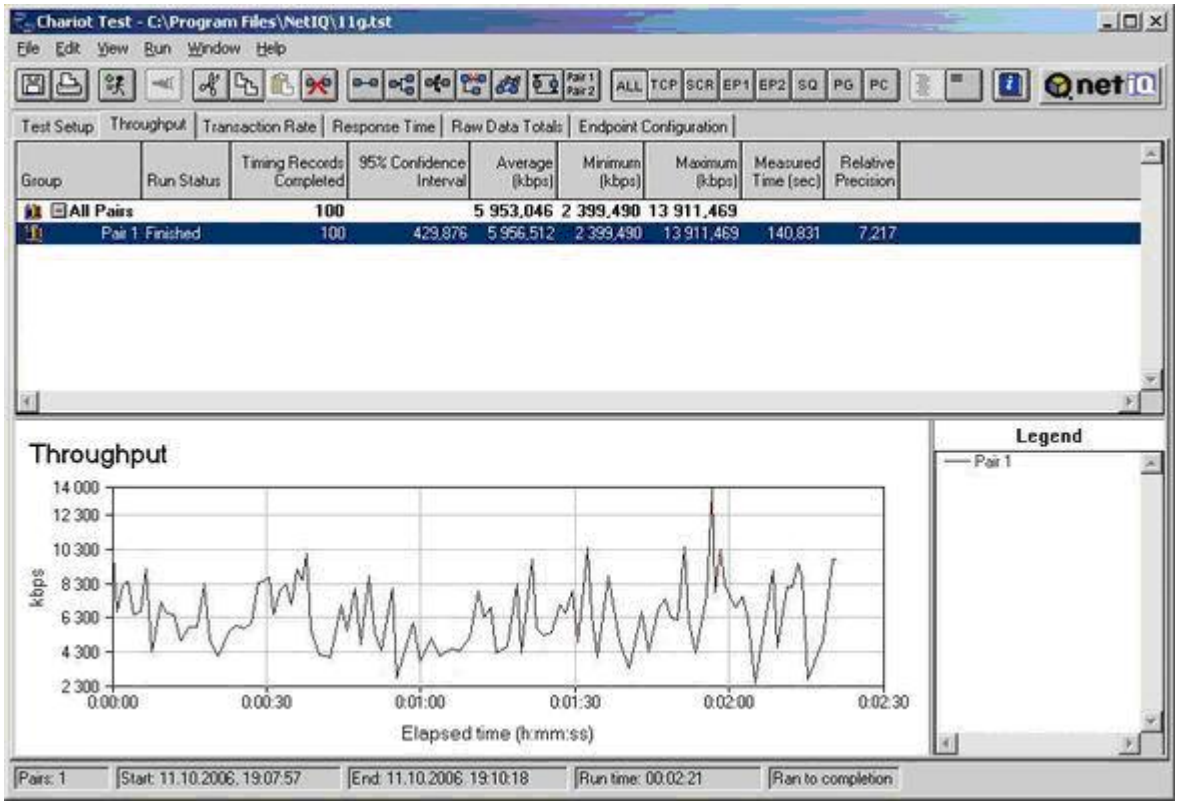

Рисунок 3.24 - Тестування бездротової частини. Умова 4

Швидкість передачі великих об'ємів даних опинилася на рівні інших пристроїв даного стандарту - вище 20 Мбіт/с, але нижче 25 Мбіт/с. За наслідками тестування швидкості при включеному шифруванні WEP і при вимкненому, варто відзначити, що істотної різниці не відмічено. Відмінність, що вийшла, можна віднести до погрішності вимірювань. Таким чином, шифрування WEP практично не позначається на продуктивності мережі і його рекомендується використовувати для забезпечення хоч би мінімального захисту мережі в цілому.

3.5.2 Вбудований комутатор

Для даного тестування використовувалися дві клієнтські машини, обладнані 100-мегабітнимі мережевими адаптерами Ethernet. Клієнти розташовувалися в сегменті LAN і були підключені безпосередньо до портів пристрою, тому швидкість маршрутизації, а також зовнішні параметри ніяк не вплинули на результат цього тестування (рис. 3.25).

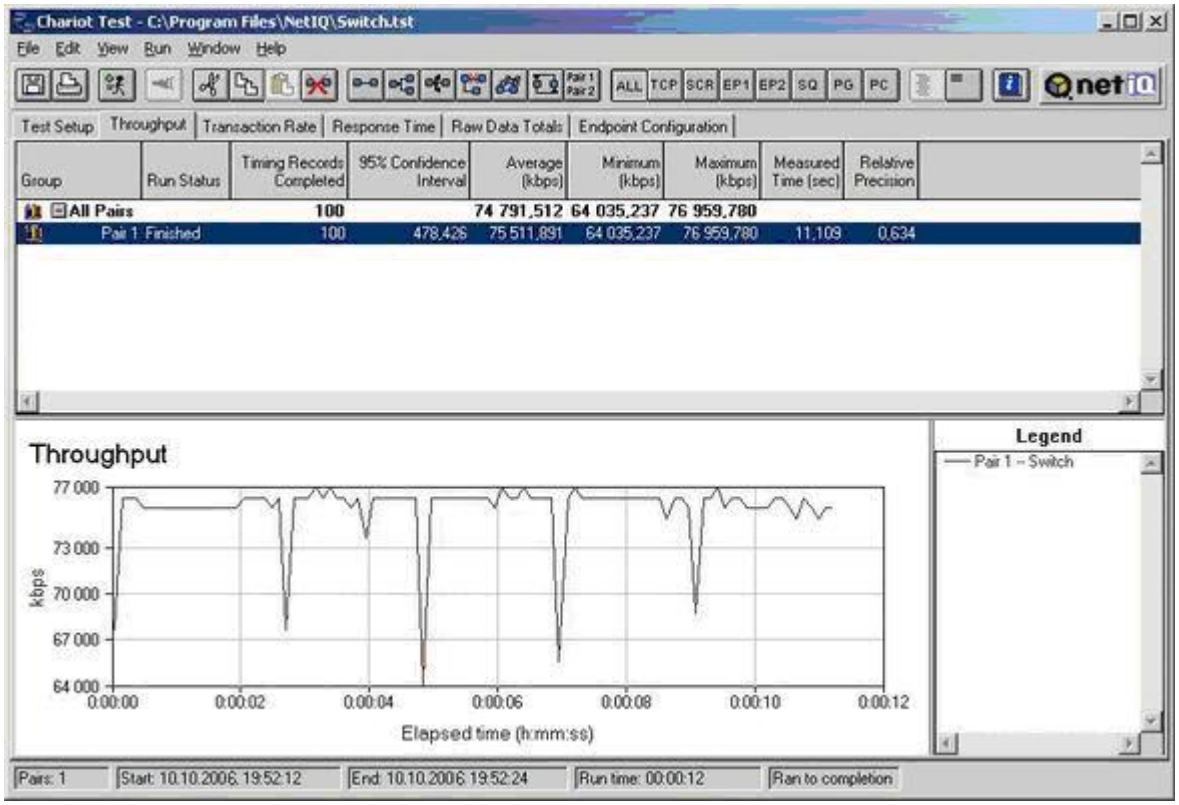

Рисунок 3.25 - Тестування продуктивності комутації

Середня швидкість склала 75,512 Мбіт/с. Такий показник швидкості характерний для 100-мегабітного мережевого устаткування, тому вбудований комутатор даного устаткування відповідає нормам мережевого комутаційного устаткування.

3.5.3 Маршрутизація

При тестуванні до маршрутизатора SMC2804WBR були підключені тільки машини, за допомогою яких проводилося тестування. Бездротова частина також була відключена. Розмір передаючих даних склав 1 Мбайт. Результати тесту продуктивності представлені в табл. 3.5.

Таблиця 3.5 - Продуктивність маршрутизації SMC 2804WBR

Тест	**Швидкість передачі, Мбіт/с**	**Час відповіді, мс 10 ітерацій по 100 байт**	**Потік UDP Актуальна пропускна здатність, кбіт/с**	**Потік UDP, % (втрачених даних)**
WAN-LAN	34,3	1 (серед.) 5 (макс.)	498	0 %
LAN-WAN	37,5	1 (серед.) 4 (макс.)	499	0 %

Як видно по значеннях, представлених в таблиці, швидкість маршрутизації SMC2804WBR є більш ніж гідною для пристроїв такого класу. Вона виявилася трохи вищою для напряму LAN-WAN (рис. 3.26 - 3.27), але, як видно, різниця мінімальна.

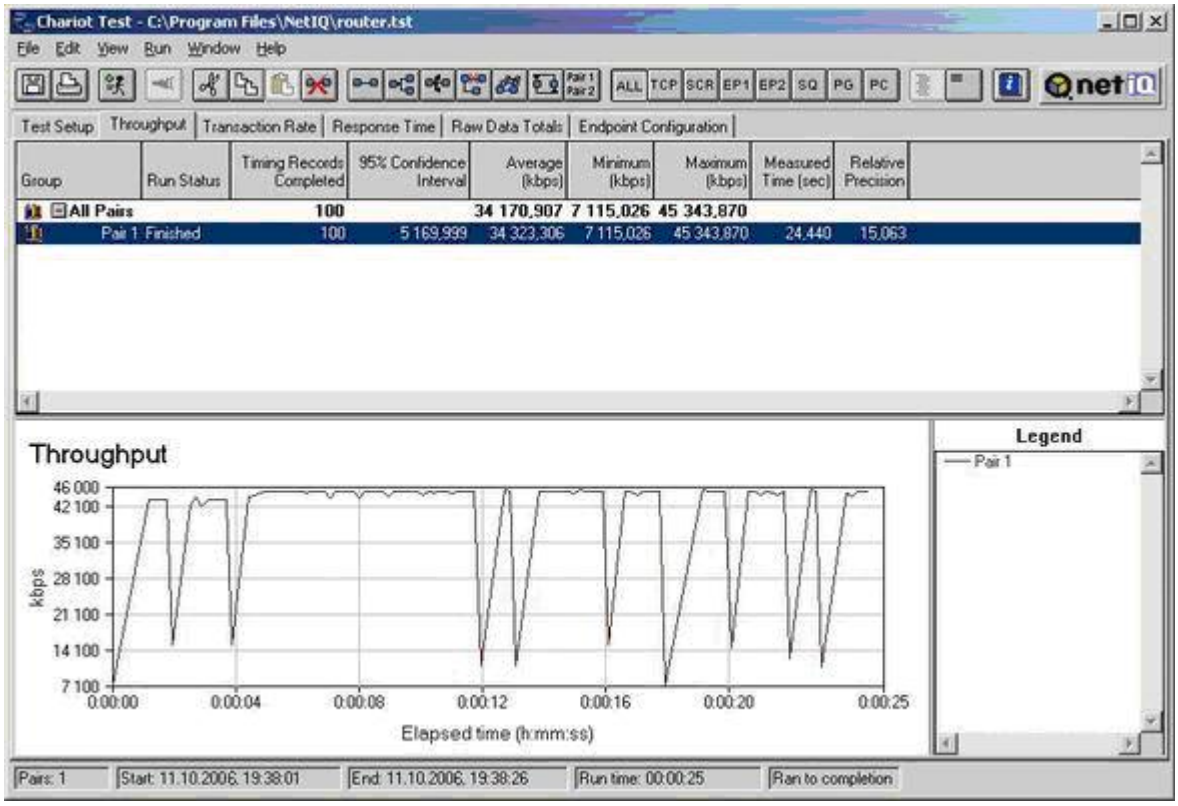

Рисунок 3.26 - Тестування маршрутизатора в напрямку WAN-LAN

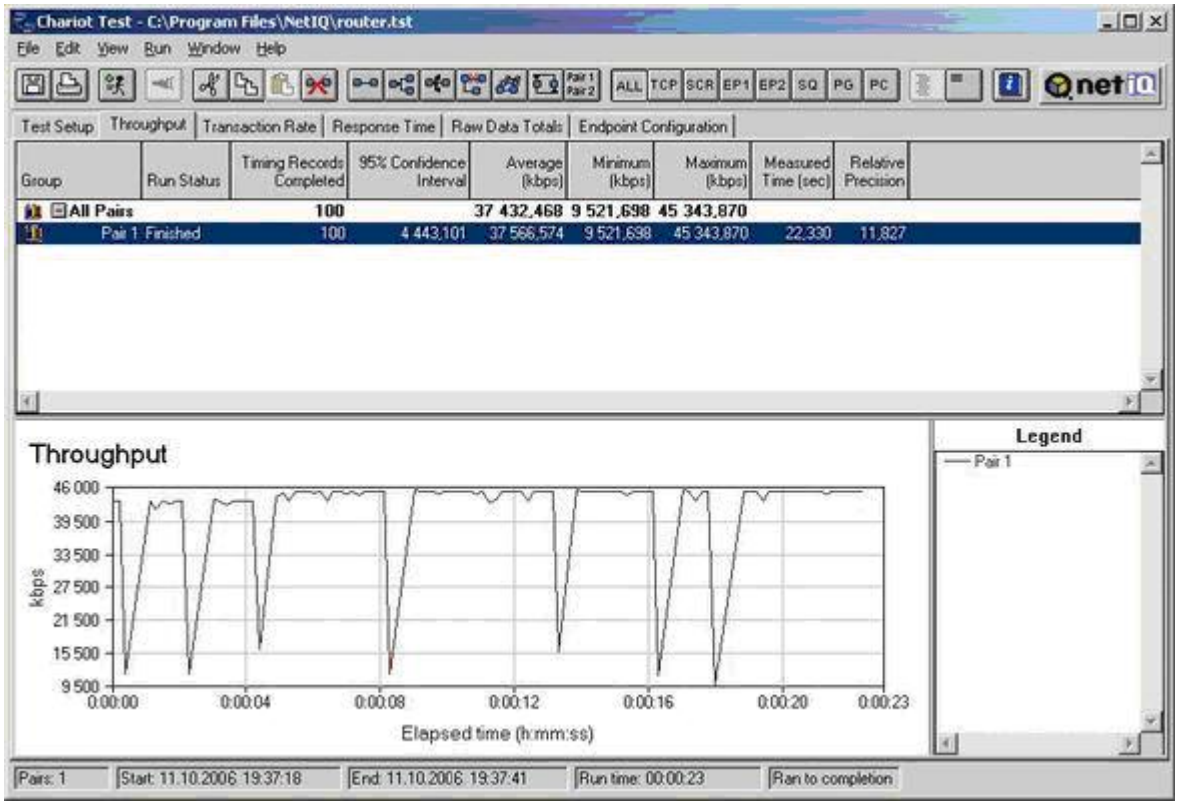

Рисунок 3.27 - Тестування маршрутизатора в напрямку LAN-WAN

3.5.4 Шифрування

При проведенні тестування з’ясувалось, що пропускна здатність зменшилась при використанні WPA шифрування (рис. 3.28) і майже не змінилась при WEP шифруванні (табл. 3.6).

Таблиця 3.6 - Залежність швидкості роботи від режиму роботи мережі

Режим	**Швидкість, Мбіт/с**
Без шифрування	23,590
Шифрування WEP	23,465
Шифрування WPA	18,138

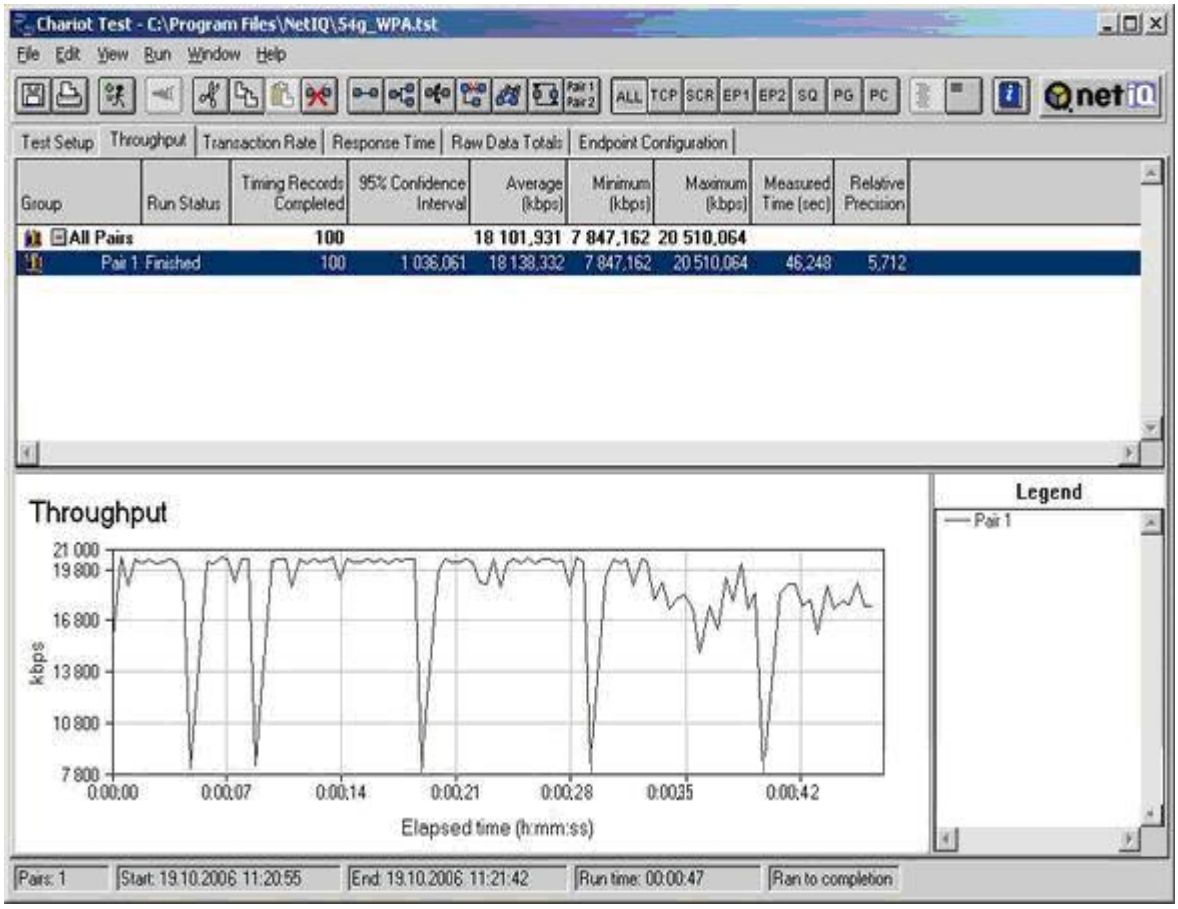

Рисунок 3.28 - Тестування бездротової частини (Шифрування WPA)

Таким чином, якщо швидкість незахищеного з'єднання прийняти за 100%, швидкість з'єднання при використанні шифрування WEP буде близько 99,5%, а швидкість при використанні WPA - 76,9%. Ціна більш надійного захисту складає 23,1% пропускної спроможності мережі. Проте варто відзначити, що при проникненні в мережу зловмисника можна понести не тільки небажаний витік інформації, але і те ж саме, а може навіть більше зниження пропускної спроможності.

3.5.5 Результати

Продуктивність вбудованого комутатора виявилася дуже хорошою. В цілому пропускна спроможність була стабільна, за винятком двох короткочасних падінь, які, відбулися не з вини комутатора.

Швидкість маршрутизації виявилася більш ніж достатня, вимірювалася швидкість маршрутизації при передачі даних із зовнішнього

інтерфейсу на внутрішній. Тим самим була змодельована типова картина офісного використання маршрутизатора, коли користувачі внутрішньої мережі приймають більше даних, ніж передають.

Оскільки передбачається використання захищеної бездротової мережі, з використання шифрування WPA, середня пропускна спроможність SMC2804WBR складе 18 Мбіт/с (за умови використання радіокарт стандарту 802.11g). Така швидкість дозволить працювати до 20 дуже активним користувачам, що постійно використовують мережу і працюють з великими файлами.

ВИСНОВКИ

У даній роботі приводиться опис технології побудови бездротової локальної мережі на основі технології WLAN та протоколу передачі інформації IEEE 802.11g та аналіз роботи устаткування на цій технології. На основі цього вибирається оптимальна схема впровадження цієї технології при побудові бездротового сегменту в конференц-залі офісу та VPN комп'ютерної мережі всього офісу. Найбільш підходяще устаткування – це 4 точки доступу – 4 маршрутизатори SMC2804WBR. З метою підвищення захисту бездротової мережі буде використана технологія VPN та спеціалізоване програмне забезпечення з контролем доступу та шифруванням передаваємої інформації, організацією захисту від комп'ютерних вірусів (комплекс програм) та несанкціонованим підключенням до сегменту мережі (FireWall).

Впроваджувана технологія сприяє прояву соціального ефекту, що досягається за рахунок того, що при впровадженні проекту представляться наступні можливості:

- одержання співробітниками постійного доступу до Інтернет, вони можуть переглядати електронну пошту, перевіряти свою базу даних на конференції або нараді, надавати дані, що знаходяться в мережі, колегам при зустрічі;
- не потрібно бути прив'язаним до мережного кабелю, можна спільно працювати в будь-якому конференц-залі, атріумі, приймальні або навіть у кафетерії.

Так само варто відзначити, що дана технологія бурхливо розвивається і є перспективним ринком для інвестування засобів у розвиток точок публічного доступу ("хот-спотів"), що обіцяє високі доходи компаніям-учасникам. У силу специфіки технології, схожістю із системами мобільного зв'язку, вона особливо приваблива для стільникових компаній, що мають великий досвід у вирішенні проблем, пов'язаних з

роумінгом і тарифікацією клієнтів бездротових мереж. Тому організація бездротового сегменту існуючої локальної мережі в офісній компанії дозволить також на практиці оцінити переваги і комерційну привабливість даної технології.

Розроблено топологію офісної бездротової комп'ютерної мережі за технологією WLAN з протоколом обміну даними IEEE 802.11g з використанням 4-х точок доступу та запропоновано систему захисту інформації та контролю доступу до Laptop, ступінь захищеності яких, перевірена за допомогою спеціального програмного забезпечення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Столлингс В. Беспроводные линии связи и сети. М.: Издательский дом «Вильямс», 2003, – 640 с.

2. Ladrom O., Feurstein M.J., Rappaport T.S. A comparison of theoretical and empirical reflection coefficients for typical exterior wall surfaces in a mobile radio environment. IEEE Trans. Antennas Propagat., 1996, v. 44, pp. 341-351.

3. Lawton M.C., MacGeehan J.P. The application of a deterministic ray launching algorithm for the prediction of radio channel characteristics in small-cell environments, IEEE Trans. Vehic. Tech., 1994, vol. 14, pp. 955-969.

4. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. Пер. с англ./ Под ред. В.И.Журавлева – М.: Радио и связь, 2000. – 520 с.

5. Вишневский В.М Теоретические основы проектирования компьютерных сетей, 2003, 512 с.

6. Лихограй В.Г., Стрельницкий А.А., Стрельницкий А.Е., Цопа А.И., Шокало В.М. Методы прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала [Текст] , / Под. ред. А.И. Цопы, В.М. Шокало. – Харьков: КП «Городская типография», 2011. – 501 с.

7. Стрельницкий А.А. Сравнительный анализ помехозащищенности *Wi-Fi* радиоканалов с антеннами различных типов [Текст] / А.А. Стрельницкий, А.И. Цопа, В.М. Шокало // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ, 2008. – Спеціальний випуск. – С. 103-107.

8. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей [Текст]. – М.: Горячая линия-Телеком, 2008. – 288 с.

9. Lau B. K., Ow S. M. S., Kristensson G., Molisch A. F. Capacity Analysis for Compact MIMO Systems [Текст] // IEEE Vehicular Technology

Conference (VTC) (ISSN; 1550-2251). – IEEE Xplore, 2005. – Vol. 1. – P. 165–170.

10. Schneider K., Sandstrom L. *MIMO* vs. *SISO* capacity on twisted pair loops [Текст] //*T1E1.4 committee*, contribution 2002-259, November 2002.

11. Цопа А.И. Обобщенная модель оценки защищенности цифровых систем передачи информации с отводными каналами [Текст] / А.Г. Лукьянчук, А.И. Цопа, В.М. Шокало // Труды 12-й Международной научно-практической конференции «Современные информационные и электронные технологии» /*СИЭТ'2011*/. – Одесса, 2011. – С. 166.

12. Цопа А.И. Идеология создания отечественных специальных цифровых систем передачи информации [Текст] / И.Е. Алексеев, В.В. Воронин, А.Е. Стрельницкий, А.А. Стрельницкий, В.М. Шокало, А.И. Цопа // Сборник тезисов докладов 16-ой Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии» /*CriMiCo'2006*/ – Севастополь: СНТУ, 2006. – Том. 1. – С. 346–447.

13. Шинкаренко И.В. Исследование влияния отводного канала с электрической связью на параметры защищенности цифровых систем передачи информации на основе *xDSL* технологий [Текст]. /В.В. Шинкаренко, А.И. Цопа // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2011. – Выпуск № 165. – С. 88-95.

14. A. A. M. Saleh and R. A. Valenzuela, A statistical model for indoor multipath propagation, IEEE J. Select. Areas Comm [Текст]., vol.5, 1987, pp. 128-137.

15. Medbo J., Schramm P. Channel models for HIPERLAN-2 [Текст] // ETSI/BRAN document no. 3ERI085B. – 1998.

16. Кузнецов А.А. Приближенный анализ защищенности системы MIMO на основе кластерной модели отводного канала [Текст]. Часть 1: Модель. /А.А. Кузнецов, А.И. Цопа // Радиотехника. Всеукраинский

межведомственный научно-технический сборник. – 2011. – Выпуск № 164. – С.72-76.

17. Кузнецов А.А. Приближенный анализ защищенности системы MIMO на основе кластерной модели отводного канала [Текст]. Часть 2: Модель. /А.А. Кузнецов, А.И. Цопа // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2011. – Выпуск № 164. – С.72-76.

18. Цопа А.И. Выбор линейных сигналов и анализ их спектральных характеристик в системах передачи информации с использованием *xDSL* технологий [Текст] // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2006. – Выпуск № 146. – С. 66–74.

19. Цопа А.И. Способы повышения и качественной оценки качества передачи видеоинформации по беспроводным каналам связи [Текст] / Стрельницкий А.А., Цопа А.А., Цопа А.И., Шокало В.М. // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації. – Львів, 2008. – Випуск № 618. – С. 168–173.

20. Цопа А.И. Экспериментальная оценка помехозащищенности мультимедийных цифровых систем передачи информации на основе *SHDSL* технологий [Текст]. / И.В. Шинкаренко, А.И. Цопа // Журнал «Известия Вузов: Радиоэлектроника». – Київ: НТУ «КПИ», 2011. – Вип. 54. – №5. – С. 30-36.

21. Цопа А.И. Оценка безопасности работы *Wi-Fi* радиоканала с различными условиями распространения [Текст] /А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало, Е.В. Ягудина // Науково-технічний журнал «Сучасний захист інформації». – Київ: ДУІКТ, 2011. – Вип. № 2. – 56 С.

22. Цопа А.И. Подход к оценке защищенности цифровых систем передачи информации с отводным каналом [Текст] / В.А. Хорошко,

А.И. Цопа, В.М. Шокало // Науково-технічний журнал «Захист інформації». – Київ: НАУ, 2011. – Вип. № 2. – 76 С.

23. Цопа А.И. Теория и практика построения радиоканалов локальных беспроводных сетей с заданным качеством передачи информации [Текст] / А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало // Сборник тезисов докладов 18-й Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии»/*CriMiCo'2008*/. – Севастополь: СНТУ, 2008. – Том. 1. – С. 3–9.

24. Цопа А.И. Развитие теории и моделей отводного канала [Текст] / А.И.Цопа, В.М.Шокало // Збірка тез науково-практичної конференції «Захист інформації в інформаційно-комунікаційних системах». – Київ: НАУ, 2010. – С. 52–53.

25. Цопа А.И. Разработка и исследование модели отводного канала для проводных цифровых систем передачи информации [Текст] /А.И.Цопа, В.М. Шокало // Материалы XIII международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». – Київ, 2010. – С. 64.

26. Цопа А.И. Пути повышения защищенности каналов связи цифровых систем передачи информации на физическом уровне [Текст] / А.А. Дудка, А.В. Стрельницкий, А.А. Стрельницкий, А.И. Цопа, В.М. Шокало// Сборник тезисов докладов 20 Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии» /*CriMiCo'2010*/. Пленарный доклад. – Севастополь: СевНТУ, 2010. – Том. 1. – С. 28–31.