МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КГ-05

Дипломний проект

здобувача освіти денної форми навчання
КГ.05.12.000.ДП

Капралов Денис Олександрович

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Обслуговування комп'ютерних систем і мереж»**

Група: **4КГ-05**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Проектування ЛОМ для підприємства з територіально рознесеними об'єктами

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на _____ аркушах (слайдах).

Дипломник _____ (Капралов Д.О.)

Керівник _____ (Гаджиев М.М.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Скорнякова О.В.)

До захисту допущений

Голова циклової комісії _____ (Скорнякова О.В.)

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 2022 р. Протокол ДКК №_____

Оцінка ДКК _____

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Обслуговування комп'ютерних систем і мереж»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____2022 р.

З А В Д А Н Н Я

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти **Капралов Денис Олександрович**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) **Проектування ЛОМ для підприємства з територіально рознесеними об'єктами**

затверджена наказом по коледжу від "____"_____202___р. №___

2. Термін здачі закінченого проекту (роботи) _____

3. Вихідні данні до проекту (роботи); дослідження ринку, аналіз проблеми, постановка задачі, технічне завдання, вимоги до функціональності та практичності, вимоги до протоколів мережі, структура підприємства.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити); Вступ. Дослідження задач безпеки, загрози, атаки та структури захисту мережевих структур. Обгрунтування вибору мережевих технологій, дані. Вихідні вибір і налаштування контролера безпровідної мережі підприємства. Архітектура та проектування безпровідних направляючих систем. Економічні розрахунки. Охорона праці. Висновок. Використана література. Додатки.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Слайд 1–5 - Структура будівлі; план терміналу; функціональної взаємодії відділів; методи захисту інформації у мережі Fi-Wi.

Слайд 6-10 – Організація каналів зв'язку з використанням бездротових мережевих технологій; елементи мережі; сетеви адаптери.

Слайд 11-15 - Адмін відділ; транспортний відділ; вантажній відділ, загальна топологія мережі, топологія ЛОМ.

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1 - 3	Гаджиєв М.М.		
Економік	Копайгородська Т. Г.		
Охорона праці	Чорновол Н.І.		
ЕСКД	Петрашова В. І.		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
	Визначення задач та цілей ДП. Обговорення тематики та розділів ДП.	16.05.2022.	
	Актуальність теми. Аналітичний розділ. Огляд існуючих рішень та аналогів їх недоліки. Пошук технічного рішення. Постановка задачи.	22.05.2022.	
	Конструкторський розділ. Вибір елементної бази. Структура розробки. Критерії вибору компонентів для розробки. Розробка алгоритмів роботи пристрою та програмного забезпечення.	05.06.2022.	
	«Економічний розрахунок».	10.06.2022.	
	«Охорона праці».	12.06.2022.	
	Графічна частина. Розробка слайдів. Оформлення пояснювальної записки. Оформлення додатків, переліку літератури, специфікації та переліку елементів	16.06.2022.	
	Попередній «малий» захист.	17.06.2022.	
	Захист дипломних проектів.	21.06.2022.	

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Позн.	Позначення	Назва	Кільк.	Примітка
				Документація		
			КГ 05.12 000.00 ДП	Дипломний проект	1	
А4			КГ 05.12 000.00 ДП ПЗ	Пояснювальна записка	1	
				СЛАЙДИ	14	

Зм	Арк	№ документа	Підпис	Дата	КГ 05.12.000.00 ДП		
Розробив		Капралов Д.О.			**Проектування ЛОМ для підприємства з територіально рознесеними об'єктами**	Література	Аркуш / Аркушів
Перевір		Гаджиев М.М.					
Н.контр.		Петрашова В.І.				ОТФК ОНТУ гр. 4КГ-05	
Затв.		Скорнякова О.В.					

ЗМІСТ

ВСТУП

У зв’язку із зростанням кількості користувачів Інтернет і прогресом у розвитку комп’ютерних технологій, які дозволяють на сьогоднішній момент вирішувати найрізноманітніші завдання, пов’язані з прийомом і передачею різних видів даних, будь то відео, аудіо чи текстова інформація, зросла необхідність у правильній організації локальних мереж.

Локальні комп’ютерні, або як їх ще називають, обчислювальні мережі – це система, що включає в себе інтеграцію різних комп’ютерів, розташованих не тільки в одному приміщенні і будівлі, а й часто віддалених на достатню відстань. Всі вони можуть зв’язуватися як з допомогою кабелів, так і бездротовим способом. Локальна обчислювальна мережа (ЛОМ) призначена для об’єднання обчислювальної техніки в єдину мережу передачі даних, мови і зображення.

Технології Wi-Fi - це складна система, що включає тисячі найрізноманітніших компонентів: комп'ютери різних типів, починаючи з настільних і закінчуючи смартфонами та планшетими, системного та прикладного програмного забезпечення, мережевих адаптерів, концентраторів та роутерів. А оскільки життя не стоїть на місці, то і зміст інформації, інтенсивність потоків та способи її обробки постійно змінюються так само, як і небезпеки пов’язані з незаконним вторгненням в безпровідну мережу та зловмисним маніпулюванням інформації в ній.

Використання технологій Wi-Fi - недороге та доступне практично всім підприємствам (а через голобальну мережу Internet і одиночним користувачам) - істотно полегшило завдання побудови територіально розподіленої мережі, одночасно висунувши на перший план завдання захисту корпоративних даних при передачі їх через загальнодоступну публічну мережу з багатомільйонним "населенням".

Актуальність роботи пов'язана з усе зростаючою роллю, яку відіграють бездротові корпоративні Wi-Fi мережі для забезпечення ефективності управління і успішного функціонування самих різних організацій. При цьому

практично в кожній такій мережі спостерігається загальна тенденція збільшення числа користувачів, обсягів циркулюючої інформації, інтенсивності трафіку і пов'язаних з цими обставинами погіршення якості мережевих послуг.

Мета роботи – спроектувати функціональну мережу передачі даних на основі Wi-Fi. Для досягнення поставленої мети необхідно вирішити ряд завдань:

– дати розширене визначення поняттю мережа;

– розглянути процес створення мережі;

– розглянути структуру мережі;

– дослідити роль Internet в мережі;

– виявити особливості використання методів захисту інформації в бездротовій мережі Wi-Fi;

– охарактеризувати особливості атак на мережі.

Теоретичне значення даної роботи визначається тим, що її основні положення можуть бути використані у дослідницьких роботах, присвячених подальшій розробці систем захисту інформації в бездротовій мережі.

Робота складається зі вступу, трех розділів, висновку та списку літератури. У дипломної роботи були розглянуті особливості структури мереж, принципи, за якими будується така мережа, та безпека Wi-Fi мереж, обговорюються сценарій проектування та перші кроки впровадження технології Wi-Fi мереж до підприємств. Розроблен проект створення безпровідної локальної мережі на основі Wi-Fi та її захист.

1 ТЕХНОЛОГІЧНА ЧАСТИНА

1.1 Загальні відомості

Побудова сучасних локальних мереж і аналіз їх основних якісних показників є актуальним завданням. В бакалаврської роботи для проведення відповідних досліджень аналізується функціонування локальної мережі в чинній типовою підприємстві з заздалегідь відомими інфраструктурою і завданнями.

Підприємство спеціалізується на будівництві і виробництві дерев'яних виробів. Розташовується підприємство в побудованому двох поверховому будинку, має накопичувальний майданчик для контейнеровозів і тягачів площею 1500 м2, склади тимчасового зберігання (СТЗ) і віддалений виробничий цех знаходиться в приміській частині міста.

Для функціонування даного підприємства, є необхідним постійне інформаційне взаємодія віддаленого цеху і складів тимчасового зберігання з головним офісом, в якому, в свою чергу, розташовуються 12 різних відділів, взаємодія яких так само необхідна.

Виходячи з отриманих відомостей , про діяльність підприємства можна зробити висновок про те, що для будівлі головного офісу, складів тимчасового зберігання та термінальних майданчиків потрібне створення єдиного інформаційного простору. Тому, необхідно провести розгляд планів будівель іспоруд , а так само особливості їх територіального розташування.

План розміщення приміщень. Детально аналізуючи план першого і другого поверху головного офісу підприємства з нанесеними позначеннями телекомунікаційного устаткування можна зробити наступні висновки:

– товщина несучих стін не менше 500 мм;

– товщина між поверхових перекриттів не менше 250 мм;

– товщина внутрішніх стін будинку не менше 250 мм;

– у будівлі вже є локальна обчислювальна мережа , організована з можливістю використовувати технології Ethernet на швидкостях 100Мб / с і 1000Мб / с;

– всі стаціонарні комп'ютерні пристрої і мережеві принтери мають підключення до існуючої ЛОМ;

– максимальна довжина будівлі дорівнює 5200 мм;

– максимальна ширина будівлі дорівнює 1800 мм;

Відділи підприємства розділені по поверхах наступним чином, перший поверх розміщує в себе:

– адміністрація;

– комерційний відділ;

– бухгалтерія;

– відділ адміністрування , обробки інформації та зв'язку;

– відділ телекомунікацій і зв'язку;

– автотранспортний відділ;

– загальна кількість робочих місць дорівнює 25 шт.

Другий поверх розмістив в собі такі відділи:

– відділ логістики та експедирування;

– юридичний відділ;

– відділ обробки інформації;

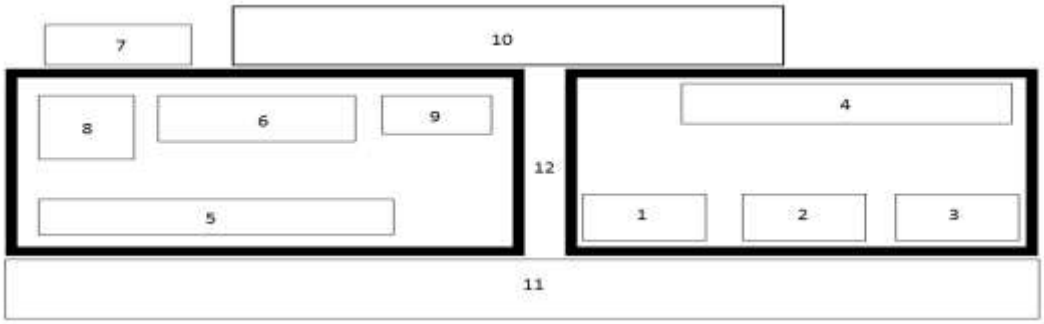
– відділ вантажно -розвантажувальних робіт на терміналі;

– господарський відділ;

– відділ режиму безпеки;

– загальна кількість робочих місць 18 шт.

Розглянемо план складу тимчасового зберігання на рисунку 1.1.



1, 2, 3, 4, 5, 6 - Зона складських приміщень.

7 - Приміщення для зберігання товару.

8 - Зона для зберігання товарів.

9 - Рентгено-оглядова установка.

10 - Рампа для вивантаження автотранспортних засобів і перевірки товарів.

11 - Дебаркадер для навантаження товарів у вагон.

12 - Тамбур

Рисунок 1.1 - План розміщення приміщень

При розгляді плану складу тимчасового зберігання можна виявити лише одну важливу деталь з точки зору побудови обчислювальної мережі: на складі вже є одне автоматизоване робоче місце , яке виконує певні функції і позначено піктограмою.

Розглянемо план віддаленого виробничого цеху, представлений на рисунку 1.2.

З плану видно, що територія віддаленого цеху має протяжність в 320 метрів і ширину близько 90 м, на якій розташовуються:

– місце для тимчасового розміщення контейнерів;

– місце перевантаження вантажу;

– стоянка вантажного автотранспорту;

– стоянка легкових автомобілів;

– два вагончики оброблених під офіс , для розміщення контрольно управлінського персоналу складається з 4 осіб.

– цифрою 2 позначено підсобне приміщення, в якому розташовуються дизель генератор та інше електрообладнання.

Рисунок 1.2 - План транспортного терміналу

Територіальне розміщення підрозділів підприємства. Головною особливістю територіального розміщення будівель підприємств можна вважати велику відстань між ними. Віддалений цех знаходиться на відстані 15 кілометрів від головного офісу , а склади тимчасового зберыання - 1,5 кілометра. Так само важливою особливістю є той факт , що місто знаходиться в гористій місцевості, головний офіс знаходиться на пагорбі, а склад тимчасового зберігання і контейнерний термінал в низині, що робить істотний впливу на вибір мережевої технології , яка використовуватиметься для організації каналів зв'язку.

Організаційна структура підприємства. Підприємство в цілому складається з 12 відділів і має штат в 147 співробітників. Узагальнено організаційну структуру підприємства можна представити таким чином: на підприємстві існує директор, у якого є заступники. Кожен відділ має

начальника, у якого в свою чергу є заступник . Остання ланка в цій структурі займають менеджери відділів та рядові співробітники.

Основні потоки інформації циркулюють між співробітниками відділів, начальники ж отримують лише зведені таблиці і звіти. Для того щоб зрозуміти як на функціональному рівні взаємодіють відділи між собою побудуємо функціональну модель підприємства за допомогою CASE -засоби BPWin.

Рисунок 1.3 - Діаграма організаційної структури підприємства

На рисунку 1.4 показано діяльність підприємства в загальному вигляді. Вхідними для підприємства є інформація із зовнішнього середовища - це замовлення, дані по об'єктах, розклад залізно дорожніх і автотранспортних перевезень, зведення Гідрометцентру , пропозиції постачальників і т.д.; вихідні дані - інформація в зовнішнє середовище : дані про відвантажений товар покупцеві, укладені договори, час і дата прибуття вантажу. З декомпозиції , наведеної на рисунку 1.4 видно, що кожен відділ виконує свої функції.

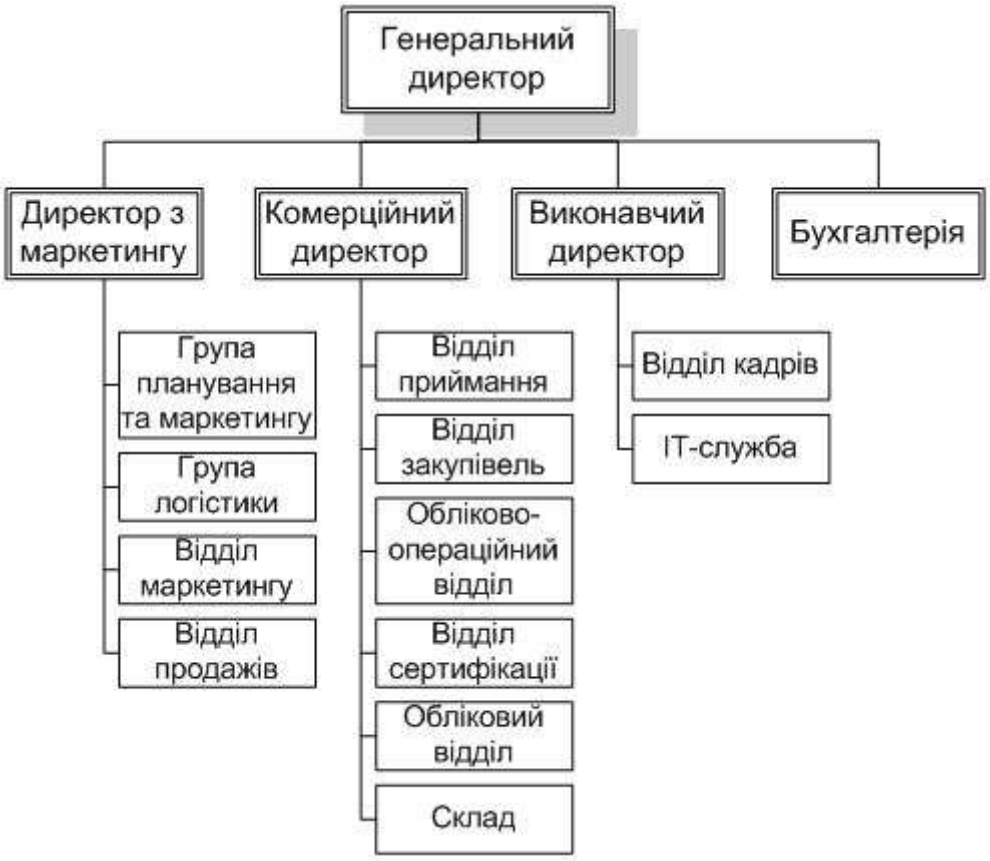


Рисунок 1.4 - Діаграма функціональної взаємодії відділів

Очевидно, що найбільш завантаженими відділами на підприємстві є: комерційний відділ, відділ логістики та експедирування , автотранспортний відділ і відділ вантажно-розвантажувальних робіт на терміналі.

1.2 Технології функціонування бездротових мереж

У ході передпроектного обстеження було виявлено, що центром розміщення комунікаційного обладнання є серверна кімната , розташована на 1 поверсі головного офісу. Всі телекомунікації виходять в центральній жилі з серверної, що знаходиться у відділі обробки інформації та зв'язку, потім в коридорах будівлі проходять в кабель каналах під фальш стелею, в кабінет спускаються зі стелі по стіні, розділяючись на телефон і локальну мережу.

Завдяки тому, що вся історія побудови безпечної інформаційної системи пов'язана, або з зміцненням захисту по периметру, або з організаційними та фізичними заходами захисту, сьогодні рідко можна побачити мережу, яка стійка до злому і атакам зсередини.

Сьогодні вже ніхто не може уявити, як завгодно серйозну організацію без робочих місць, оснащених комп'ютерами, підключеними до загальної мережі. Як правило, комп'ютерна мережа підключається до загальнодоступних мереж, зазвичай до Інтернету. Оскільки більша частина життєво важливої інформації компанії, включаючи і конфіденційну, знаходиться в мережі, то виникає серйозне питання, хто може отримати доступ до цієї інформації.

Якщо розглянути рішення проблеми захисту доступу до ресурсів мережі в розвитку, то можна відзначити суттєві зміни за останнє десятиліття.

Вирішуючи проблему безпеки мережі, фахівець, що відповідає за вибір того чи іншого рішення, як правило, повинен відшукати «золоту середину», як мінімум у трьох показниках інформаційної системи в цілому. Цими показниками, або характеристиками інформаційної системи є вартість володіння, продуктивність, безпека. Причому всі ці параметри взаємопов'язані. При підвищенні безпеки системи та зниження ризиків вартість системи в цілому зростає, а продуктивність, як правило, знижується.

Іншими конфліктуючими параметрами інформаційної системи є відкритість і зручність, з одного боку, і захищеність і надійність - з іншого. Безумовно, задовольнити всі вимоги неможливо - при побудові, або модернізації інформаційної системи важливо знайти прийнятний компроміс. Таким чином, побудова безпечної сучасної інформаційної системи - це управління виникаюче внаслідок певних компромісів ризиками.

Ще на етапі планування системи потрібно розробити політики безпеки, визначити порядок робіт (які продукти, як, ким і в якому порядку будуть впроваджуватися), описати планований аналіз інцидентів. На етапі впровадження системи засобами управління і адміністрування вибудувати спланована систему політик безпеки, встановити доступні на поточний момент пакети оновлення і доповнення до всіх застосовуваним рішенням і продуктам в системі, налаштувати мережевий аудит. У ході експлуатації системи необхідний постійний моніторинг і розслідування інцидентів, аналіз

зібраного аудиту. На основі цих даних можна буде коригувати політики безпеки, конфігурувати вже впроваджені і додавати нові мережеві рішення. На цьому кроці ми знову переходимо до етапу планування, але вже не системи в цілому, а її доробок і вдосконалення.

Важливо відзначити, що під атаками і зломом системи зсередини розуміються не стільки дії зловмисників, які підключилися безпосередньо до корпоративної мережі і при цьому є професіоналами в комп'ютерних атаках. Швидше за все, їх якраз небагато. Набагато частіше зустрічаються випадки, коли звичайні співробітники компанії бажають отримати більший доступ до мережевих ресурсів, скористатися заблокованими, або недозволеними програмами, або просто через незнання, або всупереч інструкціям встановити додаткове програмне забезпечення, «попрацювати» з даними свого колеги. Саме таких атак і боїться, як вогню будь-який співробітник IT-безпеки. Причина криється в складності і багатофункціональності (одну і ту ж дію можна виконати різними способами) сучасних операційних систем, а також в труднощі надати тільки ті можливості користувачам, які їм дійсно потрібні.

1.3 Інформаціїна безпека сучасних ЛОМ та дослідження загроз

Популярність бездротових технологій і розширення мобільного робочого простору сприяють становленню нового типу рівня доступу. Все частіше так називають архітектуру, яка безпечно і надійно надає користувачеві інфраструктуру скрізь - в офісі компанії, на віддалених сайтах, вдома, в будь-якому місці, де є доступ до інтернету. Однак мобільність, включаючи бездротові технології, має потенціал створювати умови, за яких можливий несанкціонований доступ в мережу, можливі втрати закритої інформації, а також можливі умови для проникнення в мережу вірусів і черв'яків. Якісне та повноцінне планування дозволяє уникати ці проблеми без надмірних капітальних і операційних витрат.

Використання шифрування трафіку і аутентифікації усуває багато проблем, але важливо не забувати про більш просунуті технології нашого

часу. Це, наприклад, системи запобігання вторгнень (IPS / Intrusion Prevention System), необхідні для виявлення і запобігання атак. Системи IPS давно існують і чудово себе показали не тільки в дротовому, але і в бездротовому світі. IPS дозволяє не витрачати значуще час на спроби вирішення проблем із з'єднанням у WLAN, в той час як фактична проблема, наприклад, у вже розпочатій атаці.

Сучасні методи захисту беспроводних мереж. Парольний захист заснована на тому, що для використання будь-якого ресурсу необхідно задати деяку комбінацію символів (пароль), що відкриває доступ до цього ресурсу. За допомогою паролів захищаються файли, особисті чи корпоративні архіви, програми та окремі комп'ютери. Недоліки такого захисту: слабка захищеність коротких паролів, які за допомогою спеціальних програм на високопродуктивних комп'ютерах досить швидко розкриваються простим перебором. У мережах паролі використовуються, як самостійно, так і в якості основи для різних методів аутентифікації.

Ідентифікація являє собою процедуру розпізнавання користувача (процесу) за його іменем. Для користувачів мережі вона може бути реалізована програмно, або апаратно. Апаратна реалізація заснована на застосуванні для ідентифікації користувачів спеціальних електронних карт, що містять ідентифікаційну конкретного користувача інформацію (подібно банківськими кредитними картками). Системи ідентифікації користувачів, реалізовані апаратно, є більш надійними, ніж парольний захист.

Рисунок 1.5 - Основні методи захисту інформації у мережі Fi-Wi

Використання закладених з ОС можливостей захисту - це обов'язкове правило. Однак більшість ОС або мають мінімальний захист, або надають можливості її реалізації додатковими засобами.

При підключенні комп'ютерної мережі до відкритих мереж, наприклад до мережі Internet, з'являються загрози несанкціонованого вторгнення в закриту (внутрішню) мережу з відкритої (зовнішньої), а також загрози несанкціонованого доступу із закритої мережі до ресурсів відкритої. Подібний вид загроз характерний також для випадку, коли об'єднуються окремі мережі, орієнтовані на обробку конфіденційної інформації різного рівня секретності.

Міжмережевий екран - це програмна, або програмноапаратна система міжмережевого захисту, що дозволяє розділити дві (або більше) взаємодіючі мережі і реалізувати набір правил, що визначають умови проходження пакетів з однієї мережі в іншу.

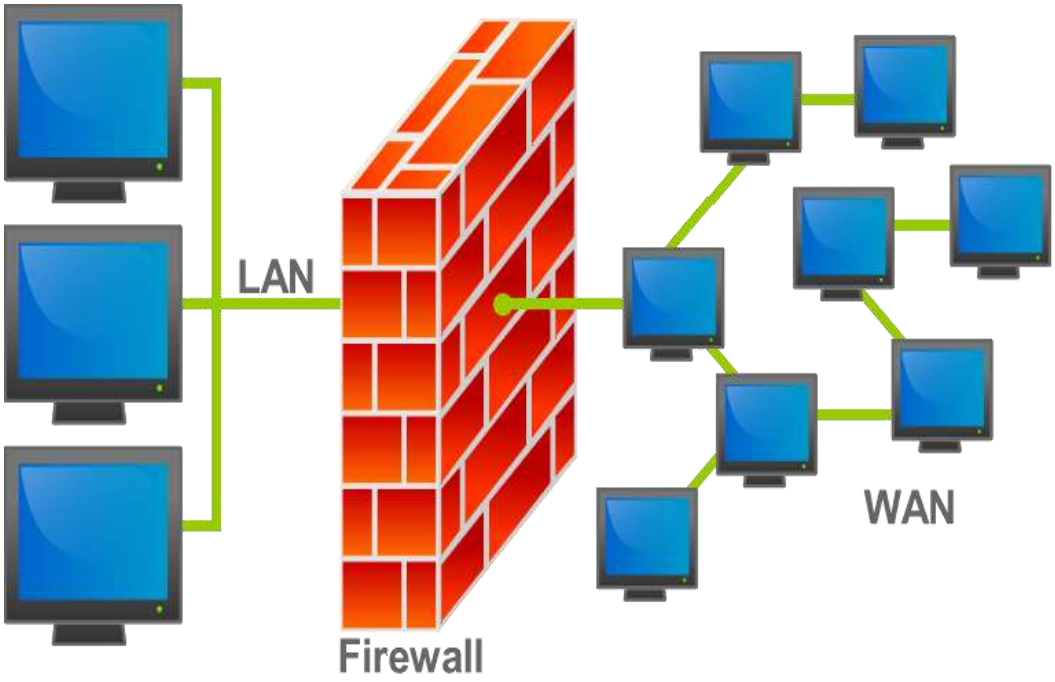


Рисунок 1.6 - Схема розташування брандмауера

Для протидії несанкціонованого міжмережевого доступу він повинен розташовуватися між захищаючою мережею організації, що є внутрішньою, і потенційно ворожою зовнішньою мережею (рис. 1.6) хоча подібними екранами можна розділити один від одного внутрішні локальні мережі. Якщо мережа складається з ряду віддалених локальних мереж (ЛОМ1, ЛОМ2,...), з'єднаних між собою засобами глобальних мереж, то міжмережеві екрани ставляться в кожній локальної мережі на кордоні з глобальною (рисунок 1.7).

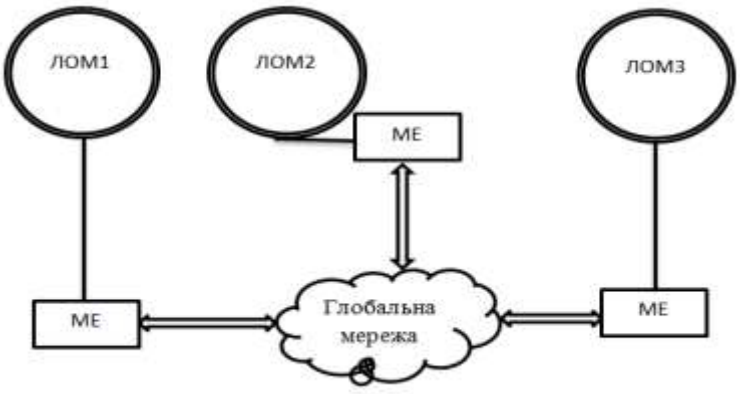


Рисунок 1.7 - Схема захисту мережі

Головний аргумент на користь застосування міжмережевих екранів полягає в тому, що без них внутрішня мережа піддається небезпеці з боку

мало захищених служб мережі Internet. Міжмережевий екран пропускає через себе весь трафік, приймаючи щодо кожного пакету, рішення - пропускати його, або відкинути. Для того щоб МЕ міг здійснити це, йому необхідно визначити набір правил фільтрації відповідно до прийнятої політикою мережевої безпеки.

Міжмережеві екрани експертного рівня поєднують в собі елементи маршрутизаторів, що екранують та прикладних шлюзів. Наявність екрану є необхідним, але не достатнім засобом забезпечення безпеки мережі.

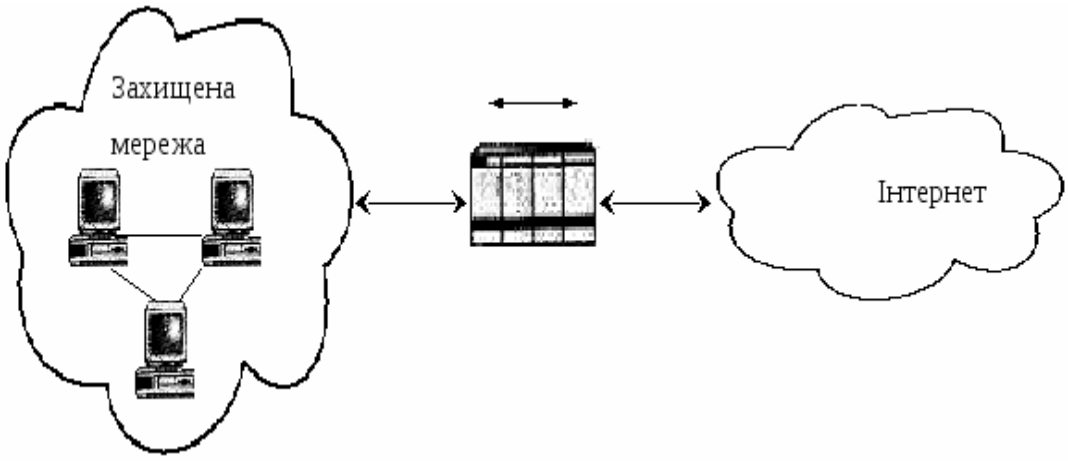


Рис.1.8- Двосторонній хост з заблокованим перенаправленням

Ще одним полезнім методом ЗІ є двосторонній бар'єрний хост. Бар'єрними, або бастіонними, хостами (bastion hosts) є укріплені системи, сконфігуровані для роботи з Інтернетом. Двосторонній шлюз складається з хост-системи із двома мережевими інтерфейсами: один інтерфейс для внутрішньої захищеної мережі й один для зовнішньої мережі.

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання глобальних відкритих мереж на початку 90-х років народилася і активно розвивається концепція побудови захищених віртуальних приватних мереж VPN (Virtual Private Networks). Тунель VPN представляє собою з'єднання, проведене через відкриту мережу, по якому передаються криптографічно захищені пакети повідомлень

віртуальної мережі.

За допомогою цієї методики пакети даних передаються через загальнодоступну мережу як в звичайному двоточковому з'єднанні. Між кожною парою «відправник-одержувач» встановлюється своєрідний тунель - безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

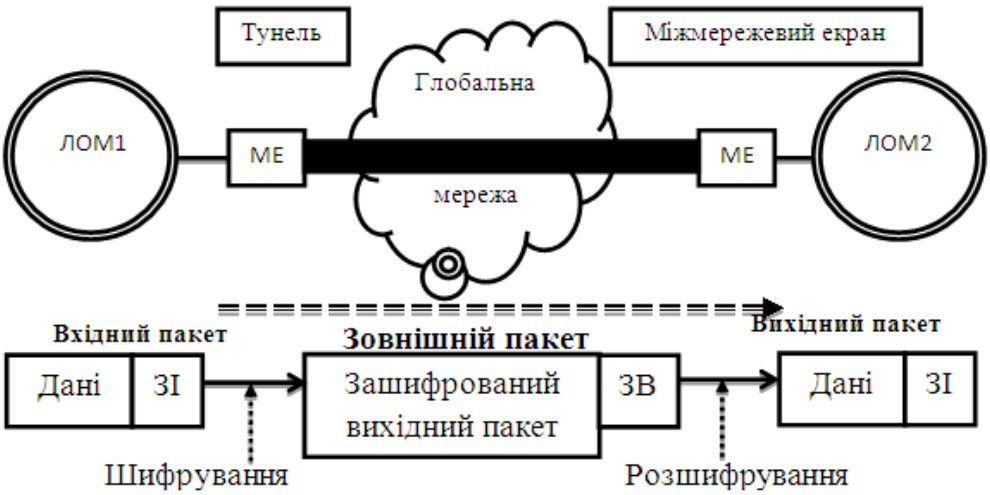


Рисунок 1.9- Схема віртуального тунелю

Суть тунелювання полягає в тому, щоб «упакувати» передану порцію даних (разом зі службовими полями) в новий «конверт». Щоб забезпечити конфіденційність переданих даних, відправник шифрує вихідний пакет разом із заголовком, упаковує його в поле даних зовнішнього пакета з новим відкритим IP-заголовком і відправляє по транзитній мережі. Схема віртуального тунелю представлена на малюнку 1.9 (де ЗІ - заголовок вихідного пакета, ЗВ - заголовок зовнішнього пакета). Для транспортування даних по відкритій мережі використовуються відкриті поля заголовка зовнішнього пакета. Для зовнішніх пакетів використовуються адреси прикордонних маршрутизаторів, встановлених на початку і кінці тунелю, а внутрішні адреси кінцевих вузлів містяться у внутрішніх вихідних пакетах в захищеному вигляді. Після прибуття в кінцеву точку захищеного каналу із зовнішнього пакета витягують і розшифровують внутрішній вихідний пакет і

використовують його відновлений заголовок для подальшої передачі по внутрішній мережі.

Побудова та забезпечення безпеки мережі Wi-Fi. Все ще нерідко доводиться чути, що мережа бездротового доступу WLAN небезпечна в порівнянні з дротяними рішеннями. На теперішньому етапі розвитку технології Wi-Fi це твердження невірно. Просто безпекою треба займатися (проектувати і підтримувати), як і у випадку провідної мережі. Можна констатувати, що практично найгірша політика зараз - це просто забороняти використання Wi-Fi в компанії. Найчастіше співробітники починають приносити власні дешеві маршрутизатори з Wi-Fi (рівня рішень «для дому) просто тому, що використовувати Wi-Fi - це зручно.

Побудова системи безпеки мережі Wi-Fi має враховувати всі ці фактори, щоб максимально наблизитися до подібного рівня безпеки бездротових сегментів мережі.

Заснована на стандарті бездротового зв'язку IEEE 802.16-2004 технологія WiMAX (Worldwide Interoperability for Microwave Access) на сьогоднішній день розвивається стрімкими темпами і, ймовірно , буде грати ключову роль у створенні регіональних (міських) мереж (Metropolitan Area Networks - MAN) в найближчому майбутньому. WiMAX стандартизований інститутом IEEE технологія, як широкосмуговий бездротовий зв'язок, який доповнює лінії DSL і кабельні технології в якості альтернативного вирішення проблеми "останньої милі" на великих відстанях. Стимулом для розвитку мереж WiMAX нового покоління також прийняття індустріальним.

Рисунок 1.10 - Організація каналів зв'язку з використанням бездротових мережевих технологій

Базові характеристики стандарту 802.16 передбачають дальність дії радіозв'язку до 50 кілометрів , покриття з можливістю роботи поза прямою зони видимості і пікову швидкість обміну даними до 100 Мбіт / с на сектор однієї базової станції. Інтерфейс мобільного бездротового зв'язку WiMAX грунтується на використанні модуляції OFDMA (Orthogonal Frequency Division Multiple Access), або масштабованої модуляції SOFDMA (стандарт 802.16e) для підтримки динамічно змінюваної ширини каналу - від 1.25 до 20 МГц. Фактично обладнання мереж WiMAX функціонує в декількох частотних каналах шириною по 10 МГц в межах ліцензованого діапазону 2 ГГц - 11 ГГц. Широкий розкид діапазонів обраний для обліку специфіки різних країн світу.

У ході виконання передпроектного обстеження було зібрано достатню кількість даних, для того щоб перейти до наступних етапів побудови обчислювальної мережі. Враховуючи зроблені висновки в кожному з розділів, ми підійшли до того, що для вирішення поставленого завдання буде використовуватися два стандарти бездротових мереж:

– IEEE 802.11g (Wi -Fi) - в якості стандарту на основі якого буде побудована локальна мережа всередині головного офісу і мережа зв'язує воєдино головний офіс і склад тимчасового зберігання;

– IEEE 802.16 (WiMAX) - в якості стандарту , для організації каналів зв'язку між розрізненими підрозділами, а саме між головним офісом і контейнерним терміналом. Наступним етапом проектування обчислювальної мережі буде етап моделювання інформаційних потоків підприємства з метою визначення обсягу трафіку на кожне робоче місце.

1.4 Інформаційні потокі у сучасних ЛОМ

Зазвичай бездротові мережеві технології групуються в три типи, що розрізняються за масштабом дії їх радіосистем, але всі успішно застосовуються в бізнесі.

PAN (персональні мережі) - короткодіючі, радіусом до 10 м мережі, які об’єднуть ПК і інші пристрої - КПК, мобільні телефони, принтери. За допомогою таких мереж реалізується проста синхронізація даних, усуваються проблеми з достачею кабелів в офісах, реалізується простий обмін інформацією в невеликих робочих групах. Найбільш перспективний стандарт для PAN - це Bluetooth.

WLAN (бездротові локальні мережі) - радіус дії до 100 м. За їх допомогою реалізується бездротовий доступ до групових ресурсів у будівлі, університетському кампусі і т. д. Зазвичай такі мережі використовуються для продовження дротяних корпоративних локальних мереж. У невеликих компаніях WLAN можуть повністю замінити дротяні з'єднання. Основний стандарт для WLAN - 802.11.

WWAN (бездротові мережі широкої дії) - бездротовий зв'язок, який забезпечує мобільним користувачам доступ до їх корпоративних мереж і Інтернету. Поки тут немає домінуючого стандарту, найбільш активно впроваджується технологія GPRS - найшвидше в Європі і з деяким відставанням у США.

На сучасному етапі розвитку мережевих технологій, технологія бездротових мереж Wi-Fi є найбільш зручною в умовах, які вимагають мобільності, простості установки і використання. Wi-Fi (від англ. Wireless fidelity - бездротовий зв'язок) - стандарт широкосмугового бездротового

зв'язку сімейства 802.11 розроблений у 1997 р. Як правило, технологія Wi-Fi використовується для організації бездротових локальних комп'ютерних мереж, а також для створення так званих гарячих точок високошвидкісного доступу до Інтернету.

1.5 Вібир мережевих технологій.

Спочатку необхідно сказати, що існує два великих напрямки розробки і використання архітектур Wi-Fi-рішень:

– автономна архітектура;

– централізована / керована архітектура.

Саме базуючись на дані архітектур, створюється основна кількість проектів мереж Wi-Fi.

У разі автономної архітектури рішення являє собою набір незв'язаних точок доступу, кожна з яких конфігурується і обслуговується незалежно. Тому складність обслуговування мережі, побудованої подібним чином, зростає лінійно, а часом і експоненціально, із зростанням кількості пристроїв. Звідси мережі з автономною архітектурою, як правило, давно не проектують великими, зазвичай не більше 3-5 пристроїв. Тут існують деякі винятки, які полегшують створення трохи більше масштабних мереж, наприклад, технологія кластеризації точок доступу. Але це не повноцінно керована архітектура у будь-якому випадку. Також у разі автономної архітектури виникають величезні проблеми з реалізацією системи безпеки бездротової мережі, тому що майже неможливо виконувати корелляцію атаки з урахуванням всіх точок доступу в зоні покриття за відсутності єдиного центру. Точки доступу незалежні і бачать ефір кожна по своєму, а для повноцінної інтерпретації події як атаки, важливий масштаб сприйняття, розуміння динаміки атаки. Це ж явище спостерігається і при виникненні проблем з інтерференцією, коли неможливо організувати спільне динамічне управління радіоресурсами (RRM-Radio Resource Management) з причини відсутності єдиного центру збору інформації з усіх точок доступу та

відповідного прийняття рішень. Варто відзначити, що відомі випадки автономних мереж, що складаються з десятків точок доступу. Але гарантією ефективної роботи такої інфраструктури в нашій практиці була наявність кваліфікованих інженерів з WLAN в IT-службі, які самі писали спеціальні скрипти для масового управління всіма точками доступу, контролю по SNMP та збору статистики і т.д. У будь-якому випадку, це досить нетривіальний підхід, який ще й дуже небезпечний через проблеми з обслуговуванням подібного рішення у разі звільнення інженера-розробника даного ПЗ.

У разі централізованої архітектури повне управління інфраструктурою мережі радіодоступу виконується контролером WLAN. Наприклад, у Cisco подібна архітектура називається CUWN (Cisco Unified Wireless Network). Контролер у централізованому рішенні управляє завантаженням/зміною ПЗ, змінами конфігурації, RRM (динамічне управління радіоресурсами), управляє зв'язком мережі WLAN із зовнішніми серверами (AAA, DHCP, LDAP і т.п.), управляє аутентифікацією користувачів, управляє профілями якості обслуговування QoS та спеціальними функціями. Більше того, контролери можуть об'єднуватися в групи для забезпечення безшовного роумінгу клієнтів між різними точками доступу в зоні покриття. Наприклад, у рішеннях Cisco Systems можна об'єднати десятки контролерів в один мобільний домен і, відповідно, до декількох десятків тисяч точок доступу. Створення подібних мобільних доменів дозволяє забезпечити безшовні хендоверів (у термінах Wi-Fi - це роумінг) між точками доступу керованих як одним контролером, так і різними. Існують ефективно працюючі мережі, кількість точок доступу в яких наближається до 100.000. Подібних масштабів можна домогтися тільки в керованій архітектурі рішення. Слід зазначити, що централізовану архітектуру в своїх рішеннях вже пропонують різні виробники.

Для точок доступу, або маршрутизаторів з Wi-Fi необхідно орієнтуватися на підтримку 802.11n.

У даному випадку ключовою проблемою є те, що в силу звичайної

практики мінімізації витрат у бізнесі, комунікаційні канали для зв'язку з малими офісами із штаб-квартири рідко бувають виділеними, широкими і надійними. Найчастіше підключення малих віддалених офісів виконується шляхом "підключення до інтернету" через найближчого і дешевого провайдера, а про підписання контракту з SLA (ServiceLevelAgreement) з цим провайдером ніхто й не замислюється (а провайдер, ймовірно, навіть не забезпечує такими послугами). Доступ до корпоративної мережі організовується через VPN. При такому підході дуже часто виникає ситуація, коли канал у віддаленому офісі падає або виникають перевантаження на мережі провайдера або на стику його мережі з мережею провайдера, до якого підключена штаб-квартира, і зв'язок зі штаб-квартирою тимчасово пропадає або стає дуже нестабільним. У будь-якому випадку подібні проблеми не скасовують бажання мати бездротову мережу в віддаленому офісі, але якщо таких офісів багато (як майже в кожному банку), то обслуговування їх стає великою проблемою, оскільки тримати IT-персонал в кожному офісі просто не рентабельно, а посилати інженера з центру при найменших проблемах з мережею довго і дорого. Необхідно відзначити, що для реалізації Wi-Fi-рішень у різних умовах оточеннях розроблені і використовуються точки доступу трьох основних типів конструкцій:

1. ТД для використання всередині приміщень/"офісний" варіант. (Часто такі ТД характеризуються привабливим зовнішнім виглядом, інтегрованими антенами і відносно вузьким температурним діапазоном, наприклад, від 0 до +40 C^o);

2. ТД для використання всередині приміщень/"ангарно-складський" варіант. (Часто такі точки доступу мають металевий корпус, можливість використання зовнішніх антен і більш широкий температурний діапазон, наприклад, від -20 до +55 C^o);

3. Токи доступу для використання поза приміщеннями, на вулиці/"вуличний" варіант (Часто характеризуються посиленим зовнішнім корпусом, зовнішніми, іноді інтегрованими антенами, вологозахищеним

корпусом і з'єднаннями, широким температурним діапазоном, наприклад, від -40 до +55 C^o).

1.6 Маршрутизація, комутація і розподіл інформаційних пакетів.

Проект бездротової мережі Wi-Fi завжди повинен включати в себе радіообстеження об'єкта на стадії проектних робіт і до початку інсталяції обладнання. Це єдина дійсно реальна можливість, при правильному проведенні, отримати достатньо підстав для створення працездатного рішення бездротової мережі з передбачуваними характеристиками.

Великі приміщення, такі великі офіси, житлові будинки, лікарні, ангари, цехи зазвичай вимагають детального радіообстеження. Без обстеження користувачі зіткнуться з недостатнім покриттям і будуть відчувати проблеми з продуктивністю мережі (пропускною здатністю) у деяких зонах. Навряд чи захочеться заново міняти місця встановлення кількох десятків точок доступу, а також всі їх підключення, якщо проблема вимагає редизайну радіопідсистеми вже після розгортання.

При проведенні радіообстеження об'єкта для Wi-Fi необхідно зробити наступні кроки:

1. Отримати план приміщення. До початку радіообстеження отримайте план всієї території майбутньої мережі, включаючи поверхові плани всіх приміщень, де передбачається покриття. Якщо немає нічого доступного, то намалюйте свій план з розмірами і вкажіть положення всіх стін, переходів, вікон, ліфтів тощо.

2. Візуально оглянути весь об'єкт. До початку будь-яких тестів пройдіть по всьому об'єкту і перевірте точність планів приміщень. Це також хороший момент для виявлення потенційних перешкод, які можуть впливати на поширення радіосигналів. Наприклад, візуальне обстеження допоможе виявити такі перешкоди для радіосигналу, як металеві шафи та перегородки, яких зазвичай немає на плані приміщення.

3. Визначити місця знаходження майбутніх користувачів WLAN. На плані приміщення відзначте зони знаходження користувачів з провідним і

бездротовим з'єднанням. Додатково проілюструйте де може знадобитися роумінг для бездротових / мобільних користувачів, а також куди вони не ходять. Можливо вдасться обійтися меншою кількістю точок доступу, якщо вдасться обмежити зони роумінгу або взагалі перейти до моделі організації «гарячих зон» Wi-Fi, а не суцільного покриття.

4. Визначити тип і модель точок доступу в майбутньої мережі. Виходячи з первинного повного обстеження об'єкту і зібраної інформації необхідно визначитися з типами точок доступу, антен для майбутньої мережі. Це може залежати від великої кількості факторів, наприклад: необхідність використання інтегрованих антен, коли є вимоги з естетики; високі стелі, відповідно до рішення із зовнішніми антенами; зони високої щільності користувачів, необхідне збільшення ємності шляхом формування вузьких осередків, відповідно точки із зовнішніми антенами з вузькою діаграмою спрямованості.

5. Визначити попередні місця встановлення точок доступу. Попередньо можна оцінити місце розташування і кількість точок доступу для забезпечення адекватного покриття необхідної зони шляхом аналізу місць положення користувачів WLAN, очікуваної зони покриття і величини осередків, сервісів на мережі і самих елементів радіопідсистеми. Для забезпечення суцільного покриття необхідно планувати деяке перекриття осередків суміжних точок доступу, але треба пам'ятати, що при призначенні каналів для точок доступу (при ручному конфігуруванні або при попередньому плануванні) Крапка з ідентичним частотним каналом повинна бути досить далеко від даної, або була мінімальною інтерференція від випромінювання через сусідню крапку доступу. Пам'ятайте, що в спектрі 2.4GHz у нас доступні лише три частотних каналу 1, 6 і 11, які не перекриваються.

6. Перевірка місць положення точок доступу і реального рівня параметрів мережі.

Це відбувається на початку реальних тестів. Зазвичай розміщується

кілька точок доступу в попередньо сплановані позиції на об'єкті і проводяться натурні тести з використанням спеціалізованих інструментів для проведення радіообстеження, наприклад Ekahau, Fluk / AirMagnet і т.п. Дуже важливо використовувати при обстеженні саме ті моделі точок доступу та антен, які згодом будуть на реальній мережі, а також виконувати тести з урахуванням найгірших за радіохарактерістіками користувача пристроїв, які Ви очікуєте побачити на своїй мережі. Також дуже важливо проводити не просто пасивні тести знімаючи характеристики саме радіомережі, а треба робити Активні тести з формуванням реального навантаження від трафіку, тому що тільки це покаже реальну картину майбутньої поведінки мережі.

Дуже корисно також мати в арсеналі аналізатор спектру для частотних діапазонів 2.4GHz і 5GHz. Це дозволить виявити і точно уявляти собі інтерференційну картину в зоні покриття.

Найбільш часто така діаграма зустрічається у точок доступу з інтегрованими антенами, у точок доступу із зовнішніми антенами типу диполь, монополь, із зовнішніми багатоелементними Омні антенами з рознесенням випромінюючих елементів для підтримки MIMO. Специфіка випромінювання антени такого типу завжди накладає свої умови на розміщення в зоні покриття. Спрямована антена діаграма спрямованості виглядає, як груша з точок доступу у вузькій частині цієї "груші".

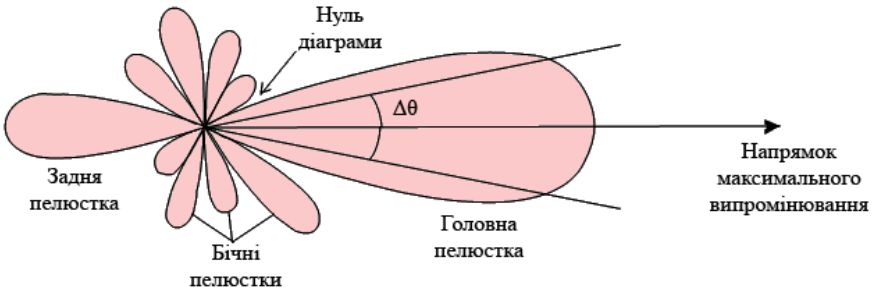


Рисунок 1.11 - Діаграма спрямованості антени

Найчастіше, як "спрямована", використовується панельна (Patch), хоча є маса інших типів, наприклад Яги. Якщо точка доступу підтримує 802.11n, то вона повинна підтримувати MIMO. Сучасні точки доступу підтримують

MIMO аж до 4x4, що означає наявність чотирьох передавачів і чотирьох приймачів. Для максимальної ефективності системи та використання можливостей рознесення (diversity) краще використовувати рекомендовані виробником антени (це стосується і випадку з Omni).

Антени спрямованого типу широко застосовуються для забезпечення покриття в приміщеннях з високими стеля (при монтажі точок доступу на стелі або в Пленумі), в дизайнах WLAN з високою щільністю користувачів, де необхідно створювати вузькі комірки і підвищувати загальну ємність мережі.

Головним критерієм, за яким можна визначити необхідну пропускну здатність мережі, є обсяг трафіку який припадає на кожного абонента мережі. Приблизний трафік можна підрахувати, знаючи з якими документами доводитися працювати тому чи іншому абоненту. Для цього проведемо декомпозицію цікавлять нас відділів.

На основі отриманої інформації побудовані діаграми потоків даних для кожного з відділів та складена зведена таблиця , в якій відображається:

- посаду співробітника;
- найменування відділу ;
- типи документів , з якими йому доводиться працювати ;
- фізичне місце його роботи (територіальне розташування) ;
- програмні засоби , які він використовує в своїй роботі ;
- приблизний обсяг споживаного трафіку;

Розглянемо комерційний відділ , декомпозиція якого представлена на рисунку 1.12. З діаграми видно, що у відділі використовуються такі типи документів:

- текстові файли;
- електронні таблиці;
- файли електронної пошти;
- інтернет файли;

– відео файли;

– фото файли.

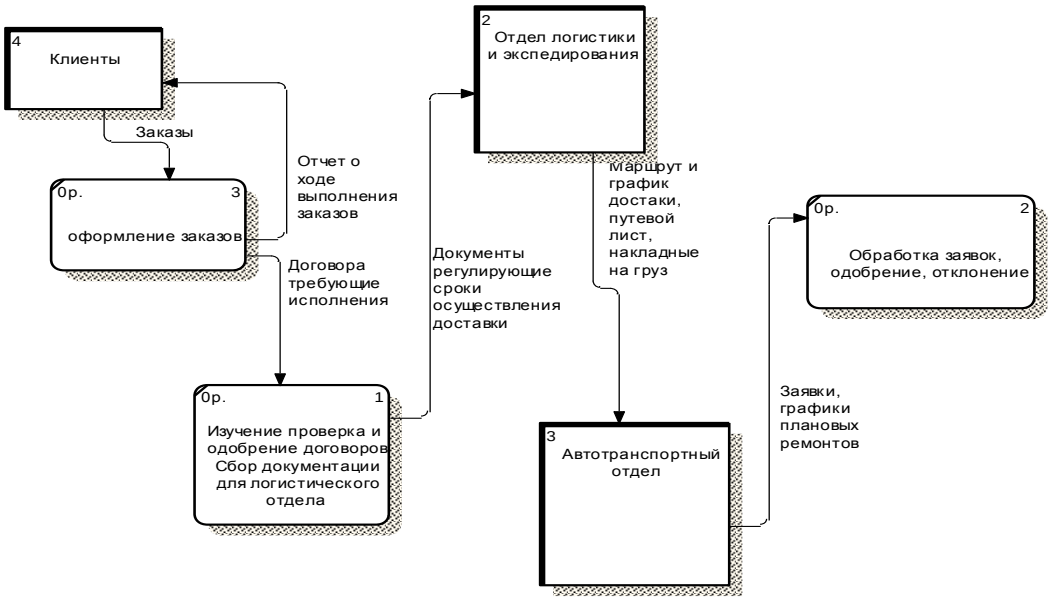


Рисунок 1.12- Комерційний відділ

Для контролю трафіку на комп'ютер кожного співробітника відділів було поставлено спеціалізоване ПЗ «Net Limiter» і проводилося спостереження протягом двох тижнів.

Розглянемо автотранспортний відділ на рисунку 1.13

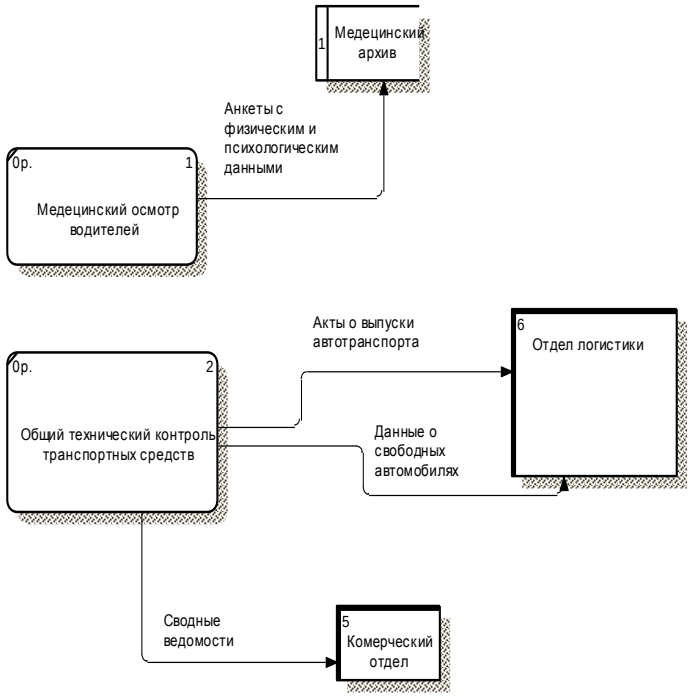


Рисунок 1.13- Автотранспортний відділ

З діаграми видно , що автотранспортний відділ працює з наступними типами документів:

– електронні таблиці;

– файли електронної пошти;

– інтернет файли;

– фото файли;

– SQL – запити;

– електронні книги формату PDF.

Процедура оцінки середнього споживаного трафіку аналогічна з процедурою проведеної в комерційному відділі.

Останній цікавий для нас відділ вантажно-розвантажувальних робіт представлений на рисунку 1.14

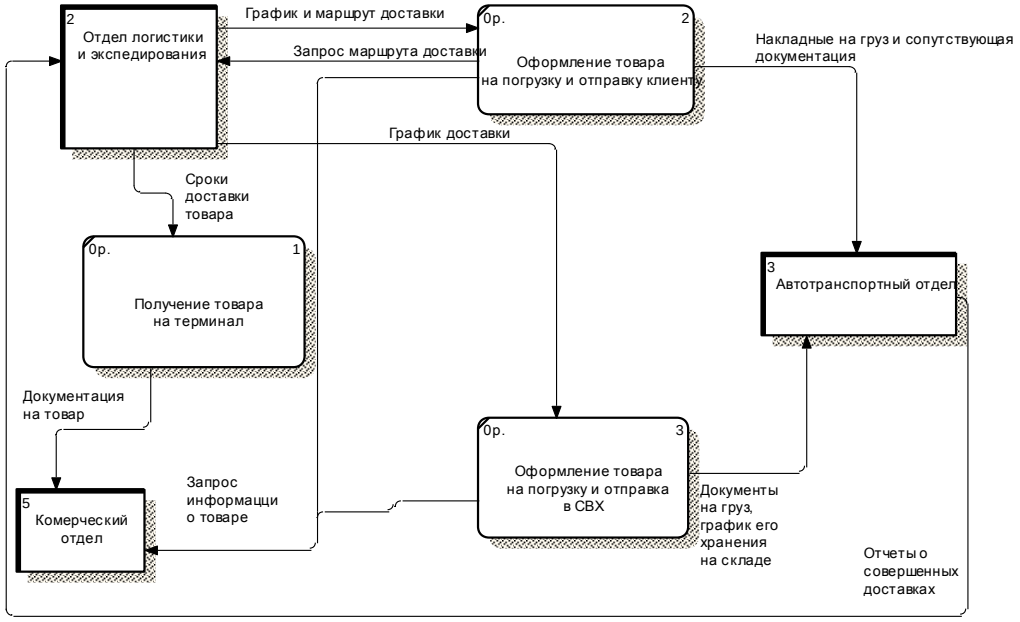


Рисунок 1.14- Відділ вантажно-розвантажувальних робіт

З діаграми видно , що відділ вантажно -розвантажувальних робіт на терміналі працює з документами наступних типів:

– електронні таблиці;

– файли електронної пошти;

– SQL – запити;

– електронні книги формату PDF.

Розрахунок середнього споживання трафіку був проведений аналогічно розрахунку трафіку в попередніх відділах.

Трафік розподіляється наступним чином:

– будівля головного офісу 4000 Мб / день;

– віддалений офіс 1890 Мб / день;

– склади тимчасового зберігання 1400 Мб / день.

Використовуючи схему, яка наочно відображає, в яких місцях підприємства буде реалізовуватися бездротова локальна обчислювальна мережа, і аналізую дані отримані в ході моделювання інформаційних потоків підприємства можна зробити висновок про необхідну мінімальної пропускної здатності для кожного з виділених місць.

Мережа всередині головного офісу: P = V / t = 4000/28800 = 0,13 Мб/с. Мережа між головним офісом і територією віддаленого цеху: P=V/t=1890 28000=0,06Мб/с. Мережа між головним офісом і складами тимчасового зберігання : P= V/t=1400/28800=0,04 Мб/с.

1.7 Розміщення і налаштування мережного обладнання

Проектування - мабуть, найбільш важливий етап у процесі побудови обчислювальних мереж. Від того на скільки кваліфіковано буде виконаний даний етап безпосередньо залежать такі чинники як: продуктивність мережі, надійність, безпека і звичайно ж вартість. Саме тому до виконання даного етапу слід підходити з особливою ретельністю і відповідальністю, оскільки помилки, допущені на даному етапі, в 90 відсотках випадках виявляються тільки на етапі пуско-наладки. А їх виправлення тягне за собою високі економічні витрати. Бездротова локальна мережа (wireless LAN або WLAN) надає змогу комп’ютерам та іншим пристроям обмінюватися даними за допомогою радіочастотної технології. За допомогою цієї технології користувачам забезпечено можливість пересування без втрати зв’язку з

мережею і без потреби у використанні кабелів з’єднання, характерних для традиційних мережевих систем Ethernet.

Як правило, створення подібних систем зв'язку викликано необхідністю колективного використання даних користувачами, які працюють на віддалених обчислювальних машинах. Беспровідна мережа не тільки дає можливість майже миттєвого обміну інформацією та одночасної роботи з файлами, але і дозволяє використовувати віддалено мережеві принтери та інші пристрої.

Даний розділ слугує реалізацією теоретичного матеріалу на практиці, а саме створення безпровідної мережі на базі технології Wi-Fi. Дане ТОВ «ГРАНТ-ПРОДУКТ» раніше вже використовувало у своїй діяльності бездротову мережу Wi-Fi для підключення користувачів переносних комп'ютерів до локальної обчислювальної мережі, доступом до корпоративних ресурсів, та Інтернет. У силу особливостей діяльності замовника, а також конфігурації приміщень, було скрутно забезпечити всіх потенційних користувачів проводовим підключенням.

Принципова схема побудованого рішення наведена на рис. 1.15

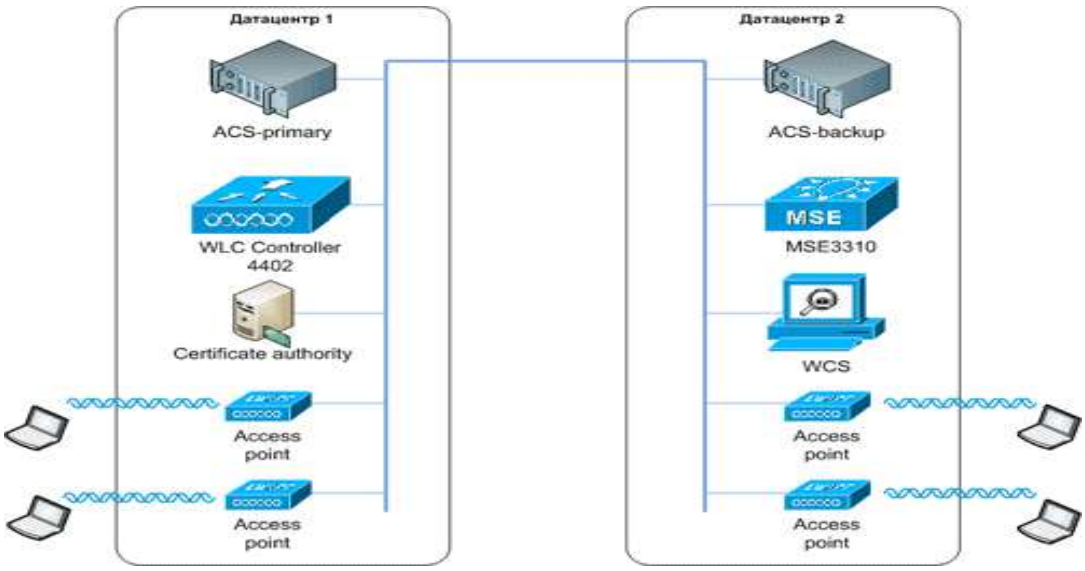


Рисунок 1.15 - Інфраструктура на основі нового обладнання

Мережа розподілена на два офіси, кожен з яких має невеликий дата-центр. Об’єднавши офіси захищеним каналом пропускною здатністю 10

Гігабіт/с використовуючи обладнання Cisco Catalyst в локальній мережі. В одному з офісів встановив контролер бездротових точок доступу Cisco WLC4402, що підтримує до 12 «легких» точок доступу. Ці пристрої, моделей LAP-1131 і LAP-1121, розподілив по приміщеннях замовника які здійснюють безпосереднє обслуговування бездротових клієнтів (ноутбуків), яких у мережі одночасно може нараховуватися до ста. Для авторизації і контролю доступу користувачів бездротової мережі точок доступу, разом з контролером, використав протокол 802.1x. При цьому в якості механізму авторизації застосовував EAP-TLS, з авторизацією по доменних сертифікатах служб каталогів Windows. Кожен користувач бездротової мережі має обліковий запис у службі каталогів наявного домену Windows. На базі облікового запису в службі сертифікатів домену створюється сертифікат, який встановлюється на ноутбук користувача і використовується при його авторизації. В якості серверів авторизації (RADIUS) виступають пристрої Cisco ACS 5.2 (2 штуки в різних дата-центрах, для відмовостійкості) робоче вікно пристрою на рис. 1.16

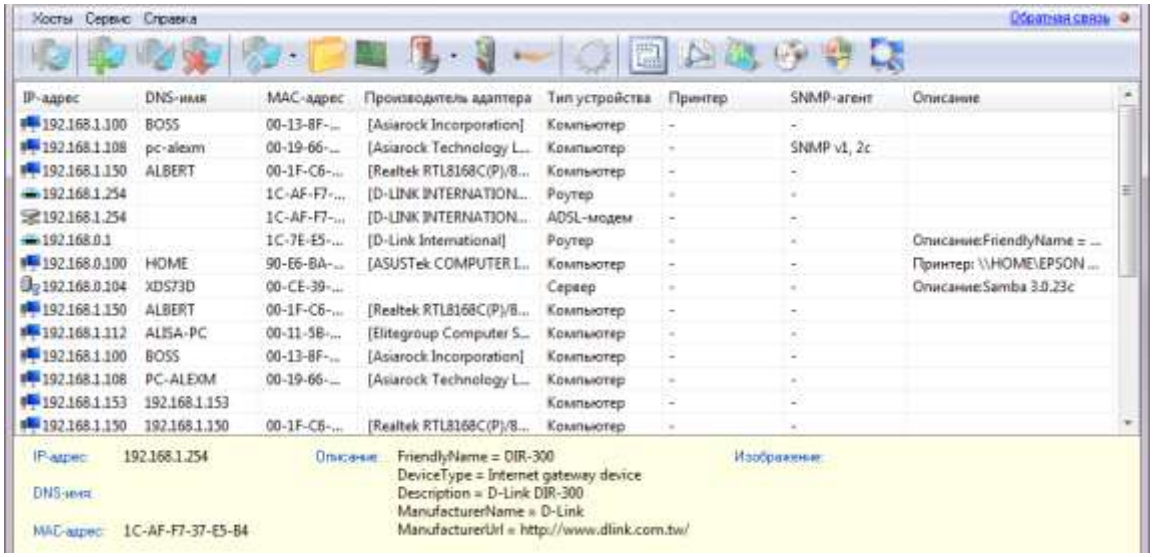


Рисунок 1.16 - Моніторинг користувачів

Для більш точного позиціонування працюючих бездротових клієнтів на карті-плані приміщення в мережі встановив додатковий контролер, Mobility Services Engine, безперервно обробляючий інформацію від бездротових точок доступу, та контролера.

Для централізованого управління мережею, перегляду статистики, налаштування, візуалізації застосовував програмне забезпечення Cisco Wireless Control System.

Для скорочення витрат з обслуговування апаратної інфраструктури «пристрою» MSE, ACS, WCS, служби каталогу та сертифікати домену виконуються в віртуальних машинах VMware.

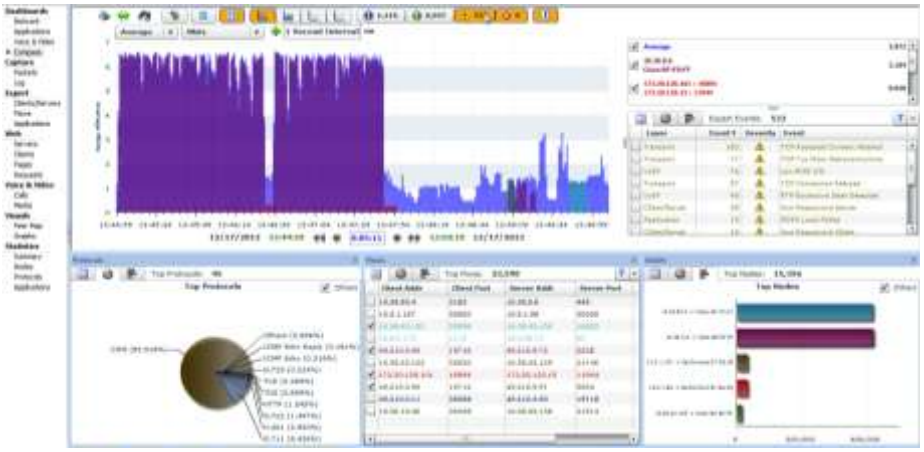


Рисунок 1.17 - Результати аналізу мережі

Таким чином, шляхом побудови сучасної бездротової мережі були успішно вирішені наступні завдання замовника:

– безпечне та надійне підключення користувачів до бездротової мережі, що використовує існуючий механізм домену Windows.

– централізоване управління, моніторинг, обслуговування безпровідних пристроїв та супутніх систем.

– автоматичний мереж на базі єдиної фізичної інфраструктури з різними політиками безпеки (департаменти, гостьовий доступ).

– додаванням контролерів і точок доступу, бездротова мережа може бути масштабирована в десятки разів, у тому числі і на віддалені майданчики, без будь-яких змін в її конфігурації.

– **Налаштування Wi-Fi контролера Cisco**контроль над радіо-обстановкою, роумінгом, визначенням положення легітимних і несанкціонованих клієнтів.

– підтримка декількох бездротових

. Наданий мені контролер wi-fi виробництва Cisco, та ще декілька нових точок доступу, для налаштування, отже, навіщо потрібен контролер? Не сильно вдаючись у подробиці, точки доступу і контролер спільно надають доступ бездротовим клієнтам до решти (дротових) частини мережі. Половину завдань, пов'язаних з доступом до радіо-середовища, генерацією beacon-фреймів, шифрування, виконує сама точка доступу. Іншу половину, в основному асоціацію та авторизацію, обслуговує контролер. Це називається Split-MAC архітектурою рис.1.18

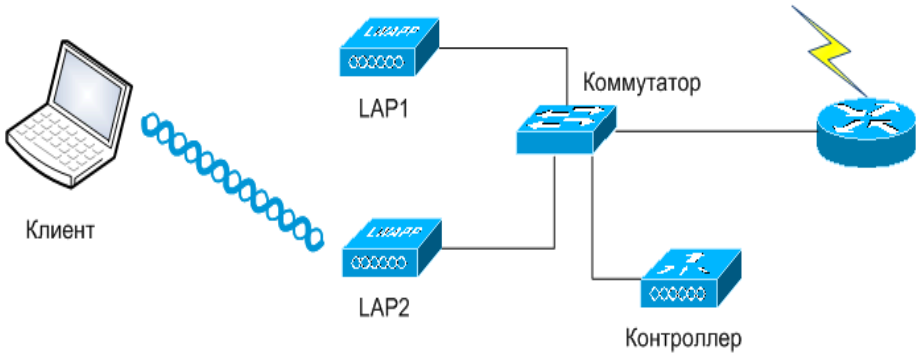


Рисунок 1.18 - Split-MAC архітектура

До контролера через локальну комутовану мережу підключені точки доступу (звичайно виробництва Cisco, навіть коли протокол взаємодії CAPWAP відкритий). Їх може бути до сотень на контролер, залежно від його продуктивності. Кілька контролерів можна об'єднати в групи, при цьому забезпечується скоординована робота контролерів, і самих точок, згідно загальних налаштувань. Переваги такого підходу очевидні: централізоване управління, гнучкість налаштувань, відмовостійкість, балансування навантаження, інтелектуальні функції безшовного роумінгу, управління частотним ресурсом, потужністю, якістю обслуговування, авторизацією.

На точках доступу, підключених до контролера, так званих «Легковагих» працює практично такий же образ IOS (AIR-LAP-xxx), що і на звичайних (standalone, AIR-AP-xxx). Різниця у відсутності режиму «conf t», так як точки налаштовуються контролером централізовано. Прошивки між standalone lightweighted можливо змінювати в ручну. «туди і назад».

При старті точка доступу виробляє пошук кращого з доступних контролерів за досить складною схемою, авторизується, викачує прошивку (якщо потрібно), налаштування, і починає обслуговувати клієнтів. Між точкою і контролером організував канал управління (UDP порт 5246), і канал даних (UDP порт 5247). Користувальницькі дані інкапсулюються в UDP пакети незалежно від номера клієнтського WLAN/VLAN, що дозволяє розміщувати точки доступу де завгодно в мережі (на access портах комутаторів), та централізовано керувати безпекою на рівні VLAN на стороні контролера. Для випадку «віддаленого офісу», де немає контролера, передбачений режим з локальним свічингом трафіку клієнтів рисунок 1.19

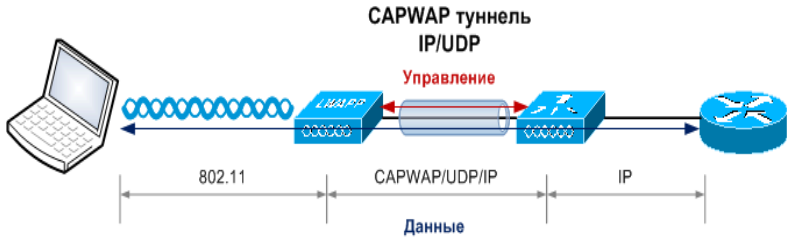


Рисунок 1.19 - Керування безпекою VLAN на стороні контролера

Контролер архітектурно являє собою спеціалізований комп'ютер (різної апаратної архітектури та розрядністю, залежно від моделі) з досить старою версією MontaVista Linux всередині. До ядра додано декілька модулів, іноді драйвери для «заліза», що займається апаратним прискоренням шифрування або пересилання пакетів. Всі дії, пов'язані з життєдіяльністю контролера, виконує великий монолітний процес, оформлений як user-додаток.

1.8 Направляючи системи та функціонування ЛОМ.

Для початку необхідно вибрати тип мережевого обладнання, яке буде використовуватися для побудови мережі, а вже потім визначатися з виробником.

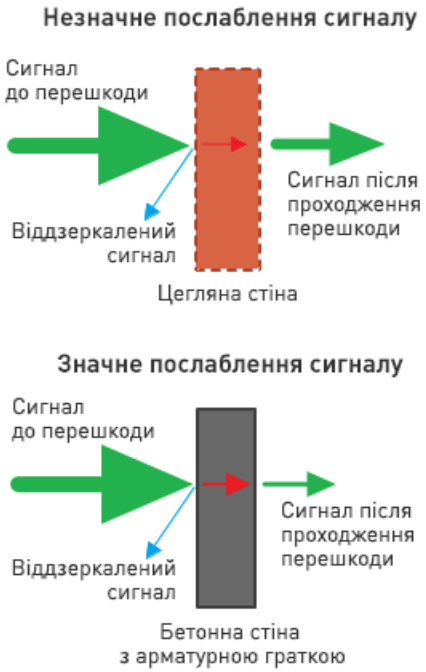


Рисунок 1.20 - Вплив стін на якість зв’язку

Тому антена з самою точкою доступу розташована асиметрично відносно горизонтальної осі будинку (back спрямований на 1 / 5 довжини , front на 4/ 5). Що дозволяє збільшити ймовірність проходження сигналу через вертикальні перешкоди.

Для економії витрат на організацію мережевого живлення для точок доступу було прийнято рішення про використання технології Power of Ethernet - PoE (живлення по витій парі), для організації такого харчування потрібні спеціальні адаптери.

Вибір типу обладнання та його кількості проведений, тепер необхідно вибрати виробника і конкретні моделі пристроїв. Так як завдання стоїть у виборі обладнання, призначеного для роботи з конкретним стандартом (IEEE 802.11g) то такі показники як продуктивність, безпеку та інші технічні характеристики розглядати не має сенсу.

У ході дослідження ринку телекомунікація було виявлено три найбільші виробники активного мережного обладнання : Cisco Systems , 3Com і D- Link. Повертаючись до аналізу інформаційних потоків проведених у другому розділі можна побачити, що абоненти працюють

усередині будівлі використовують програми критичні до часу реакції мережі, тому для побудови мережі всередині будівлі буде використовуватися бездротове обладнання фірми Cisco System, висока вартість якого компенсується максимально можливим показником безвідмовності, що в даному випадку дуже важливо. Був проведений пошук необхідного обладнання у виробника Cisco Systems і обрані моделі , що задовольняють всім пропонованим умовам.

Підключення та налагодження мережного оснащення. Мережеве обладнання є найважливішою складовою безпровідної мережі. Вихід з ладу навіть одного маршрутизатора, або комутатора може серйозно порушити функціонування бізнес-процесів підприємства. Обрані точки доступу слід підключити до комутатора, монтаж самих точок доступу здійснити згідно плану. Налаштування точок доступу слід провести так, щоб користувачам бездротової мережі присвоювалися Ip - адреси з наступного діапазону: 192.168.133.1 - 192.168.133.255. Реалізована мережу відповідає всім критеріям, вона сучасна, легко маштабується і має сучасний рівень інформаційної безпеки.

На попередніх етапах проектування були створені окремі, бездротові ділянки локально обчислювальної мережі масштабу підприємства, так само на підприємстві вже була локальна обчислювальна мережа. Бездротові мережі підключаються до корпоративного маршрутизатора, який інтегрують їх з провідною мережею утворюючи єдиний інформаційний простір, який в свою чергу вимагає управління. На даному підприємстві вже є сервер, який під управлінням ОС Microsoft Windows Server 2003 SP3, який здійснює управління провідний мережею. По суті, сервер не розрізняє, які типи мереж в ньому використовуються, бездротові сегменти представляються для нього точно так само як і дротяні. Така архітектура управління обчислювальними ресурсами називається розподіленою. Вона дозволяє гнучко управляти політикою безпеки, загальними ресурсами, а так само надійністю і продуктивністю мережі в цілому. Однак, при її використанні виникає ряд

складнощів, наприклад наявність в штаті співробітників кваліфікованого системного і мережевого адміністратора. Узагальнено топологію всієї ЛВС підприємства можна представити так, як показано на малюнку 1.21

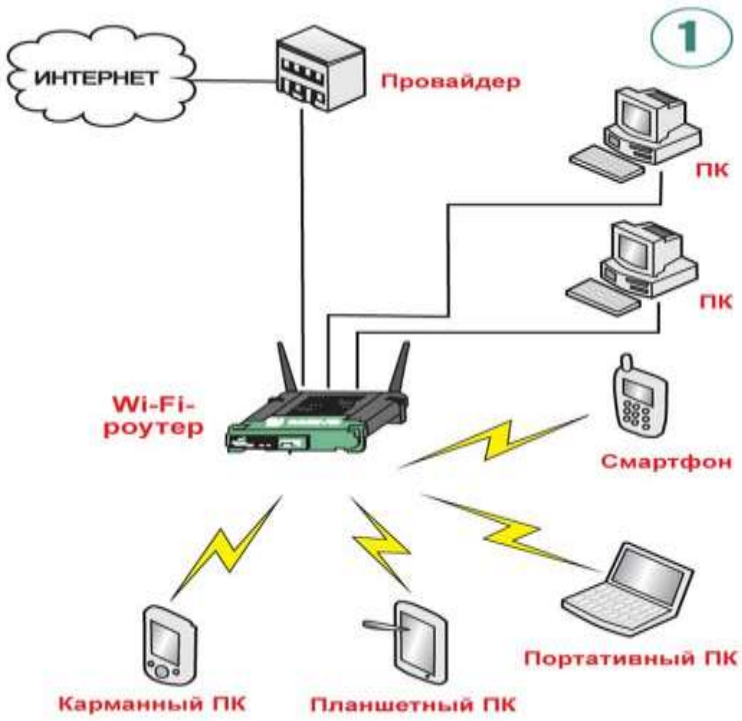


Рисунок 1.21 - Загальна топологія мережі

В даний час технології передачі даних використовують високотехнологічне обладнання та матеріали. Установка таких систем вимагає кваліфікованих установників, знають і вміють застосувати всі нові і передові знання в цій області для якісної інсталяції. Але навіть якщо система була встановлена професіоналами, жодна організація, жоден фахівець не зможе гарантувати, що дана обчислювальна мережа працює на 100 % від заявлених виробником характеристик.

З вигляду, якісно встановлена система, може призвести до часткової або повної непрацездатності підприємства через деяких прихованих дефектів, які можна побачити тільки за результатами високоточного тестування.

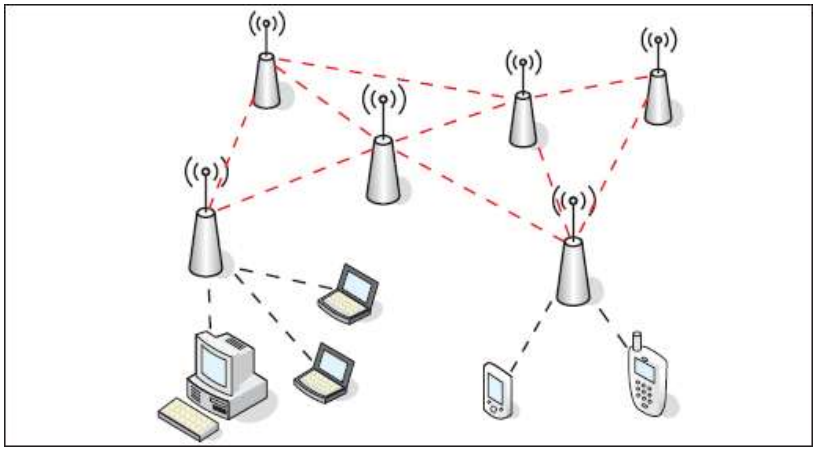


Рисунок 1.22 - Базова архітектура мережі

Після проведення пуско-налагоджувальних робіт, були задіяні фахівці компанії Ланці, для здійснення повного тестування працездатності і надійності мережі. У ході виконання всіх можливих перевірок фахівцями компанії було зроблено висновок про те, що показники мережі на 95 відсотків відповідають вимогам , які закладалися при проектуванні.

Функціонування єлєментів мережі. Мережа головного офісу повинна бути спроектована відповідно таким умовам:

– пропускна здатність мережі повинна бути не менше 0,13 Мб / с (данні отримані на єтапі моделювання інформаційних потоків);

– мережа повинна відповідати сучасним стандартам безпеки (вимоги замовника);

– користувачі мережі повинні мати можливість вільного переміщення по території всієї будівлі (вимоги замовника);

– мережа повинна бути побудована відповідно до стандарту IEEE 802.11g (Wi -Fi).

Стосовно до бездротових мереж топологія - це скоріше архітектура, по якій взаємодіють елементи мережі, розрізняють інфраструктурну архітектуру і однорангову . В рамках кожної з архітектур передбачені наступні режими роботи бездротових пристроїв :

1. Точка доступу (Access Point);

2. Міст (Wi - Fi Bridge);

3. « Точка - багато точок » (Multi- point Bridge);

4. Репітер (Repeater).

Враховуючи поставлені завдання доцільно використовувати інфраструктурну архітектуру для побудови бездротової мережі всередині головного офісу. Така архітектура представлена на малюнку 1.23

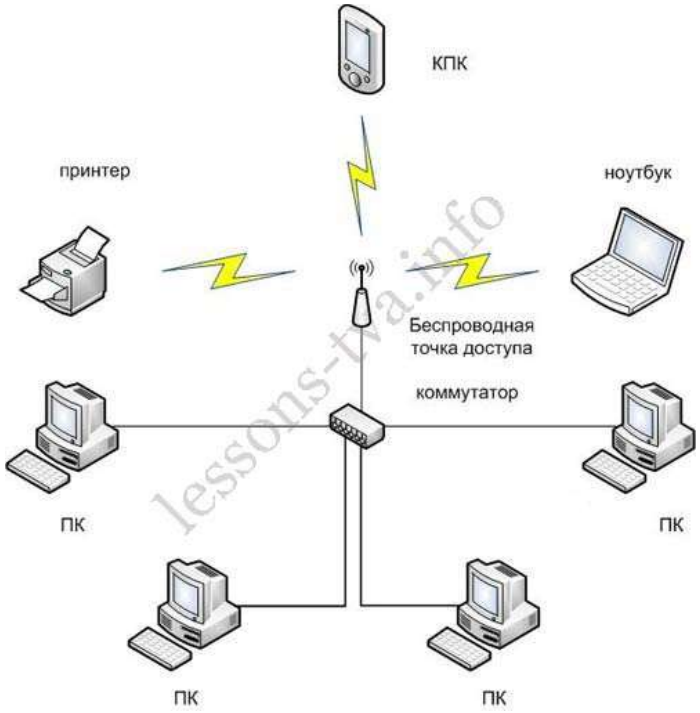


Рисунок 1.23 - Інфраструктурна архітектура

Така архітектура була обрана, оскільки крім організації взаємодії між переносними комп'ютерами вимагалося організувати для них доступ в бездротову мережу підприємства.

Планування бездротового каналу зв'язку. Радіоканали наземного і супутникового зв'язку утворюються за допомогою передавача і приймача радіохвиль і відносяться до технології бездротової передачі даних. Радіорелейні канали зв'язку складаються з послідовності станцій, які є ретрансляторами. Зв'язок здійснюється в межах прямої видимості, дальності між сусідніми станціями - до 50 км. Цифрові радіорелейні лінії зв'язку застосовуються в якості регіональних і місцевих систем зв'язку і передачі даних, а також для зв'язку між базовими станціями.

На попередніх етапах проектування були створені окремі, бездротові ділянки локально обчислювальної мережі масштабу підприємства, так само на підприємстві вже була локальна обчислювальна мережа. Бездротові мережі підключаються до корпоративного маршрутизатора, який інтегрують їх з провідний мережею утворюючи єдиний інформаційний простір, який в свою чергу вимагає управління. На даному підприємстві вже є сервер, який під управлінням ОС Microsoft Windows Server 2003 SP3, який здійснює управління провідний мережею. По суті, сервер не розрізняє, які типи мереж в ньому використовуються, бездротові сегменти представляються для нього точно так само як і дротяні. Узагальнено топологію всієї ЛОМ підприємства можна представити так, як показано на рисунку 1.24

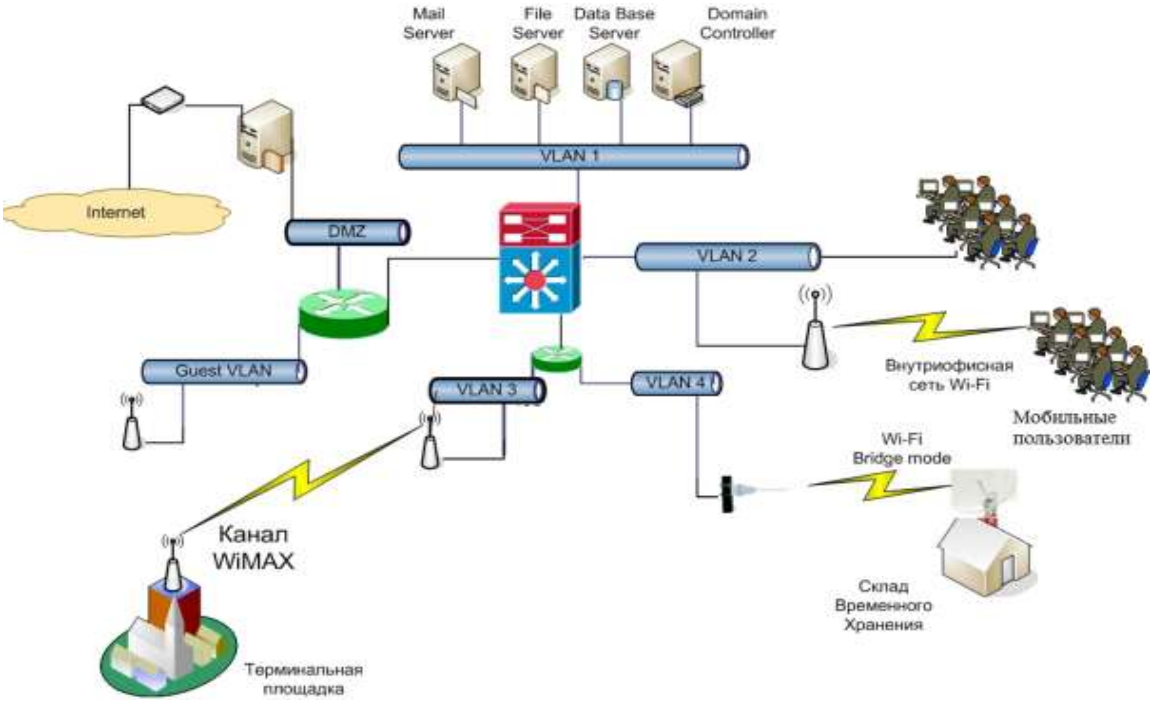


Рисунок 1.24 - Загальна топологія ЛОМ

Загальне тестування локально обчислювальної мережі підприємства. В даний час технології передачі даних використовують високотехнологічне обладнання та матеріали. Установка таких систем вимагає кваліфікованих робітників, які знають і вміють застосувати всі нові і передові знання в цій області для якісної інсталяції. Але навіть якщо система була встановлена професіоналами, жодна організація, жоден фахівець не зможе

гарантувати, що дана обчислювальна мережа працює на 100 % від заявлених виробником характеристик.

Реалізація проекту безпровідної мережі транспортного цеху підприємства це:

– ефективна мережева взаємодія різних відділів організації, що знаходяться за межами адміністративної будівлі, з інформаційними ресурсами підприємства;

– впровадження передових технологій, які дозволяють знизити витрати підприємства на організацію зв'язку по мідному кабелю;

– вирішена проблема організації електронного документо-обороту між віддаленими офісами;

– в умовах кризи, скорочені витрати на кур'єрські послуги між віддаленими офісами;

– підприємство виконало свій громадський обов'язок , внісши свою лепту в боротьбу з зростаючими автомобільними пробками.

Впровадження бездротової мережі в діяльність підприємства, безперечно дозволить поліпшити працездатність персоналу і підвищити якість умов праці. Вивільнення особистого часу сприяє розвитку особистості людини його моральних і моральних якостей , що незаперечно корисно для соціуму в цілому.

2 ЕКОНОМІЧНА ЧАСТИНА

Метою даних розрахунків є обчислення вартості виконаних розробок. Мережі Wireless LAN - це бездротові мережі (замість звичайних проводів в них використовуються радіохвилі). Установка таких мереж рекомендується там, де розгортання кабельної системи неможливе або економічно недоцільне. Бездротові мережі особливо доцільні на підприємствах, де співробітники активно переміщаються по території під час робочого дня з метою обслуговування клієнтів або збору інформації (великі склади, агентства, офіси продажів, установи охорони здоров'я та ін.). На сучасному етапі розвитку мережевих технологій, технологія бездротових мереж Wi-Fi є найбільш зручною в умовах тих, що вимагають мобільність, простоту установки і використання.

Розрахунок трудомісткості. У технологічній структурі науково-дослідних робіт можна виділити декілька самостійних етапів, а саме: розробка технічного завдання, вибір напряму дослідження, теоретичні і експериментальні дослідження, узагальнення і оцінка результатів.

Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців. В разі виконання однієї роботи виконавцями різної кваліфікації, роботу розподілили на ряд паралельних конкретних робіт для кожної категорії виконавця. Розподіл робіт по етапах і видах виконавців вироблений формою, наведено в таблиці 1.

Оцінка тривалості виконання робіт. В умовах відсутності нормативної бази тривалість виконання окремих робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Таблиця 2.1 Очікувана трудомісткість робіт

Вигляд роботи	Очікуване час викон. (дні)
1. Складання і затвердження ТЗ для НДР по розробці «Проект бездротової мережі підприємства».	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	5
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	1
4. Вибір напряму проведення досліджень і способів вирішення поставлених завдань. Розробка плану проведення досліджень для подальшої розробки.	1
5. Огляд технології бездротового доступу Wi-Fi	5
6.Реалізація мережі бездротового доступу	3
7. Узагальнення результатів попередніх етапів роботи. Оцінка повноти вирішення поставлених завдань, тестування продуктивності бездротової мережі	1
8. Розробка рекомендацій по використанню результатів проведення НДР. Захист бездротових мереж.	1
9. Налаштування бездротової мережі.	2
Всього:	21

Розрахунок собівартості і ціни виконання НДР. Результатом виконання НДР є науково-технічна продукція, що є закінчені науково – дослідницькі роботи, виконані відповідно до вимог, передбачених договором, і прийнятими замовником. Виходячи з особливостей створення науково – технічної продукції і її залежності від інтелектуальної праці, розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного

соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1)Витрати на матеріали, купувальні комплектуючі, напівфабрикати визначають на основі розрахунку потреби в них за оптовими цінами, що діють, з врахуванням транспортних – заготовлених витрат у розмірі 7-10% оптової вартості матеріалів, купувальних комплектуючих, і виробів напівфабрикатів. Розрахунок матеріальних витрат приведений в таблиці 2.2.

Таблиця 2.2 Розрахунок матеріальних витрат

Найменування ресурсів	**Одиниця виміру**	**Необхідна кількість**	**Ціна за одиницю, грн.**	**Сума, грн.**
Папір А4	Листи	100	0.50	50.00
Папір А1	Листи	4	8.00	32.00
Друк роботи	Листи	100	1.00	100.00
Разом				182.00
Транспортні – витрати 10%				18.20
Всього				200.20

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$Дз=До/25,4;$$

де До- місячний оклад, грн..;

25,4- середня місячна кількість робочих днів.

Дз дипломника 1450/25,4=57,09 грн.

Дз керівника =1500/25,4=59,05 грн.

Дз консультантів =1500/25,4= 59,05 грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 2.3.

Таблиця 2.3 Витрати на основну заробітну плату

Виконавець	**Місячний посадовий оклад**	**Денна ставка**	**Трудомісткість робочих днів**	**Сума основної зарплати**
Дипломник	1450	57,09	21	1198,89
Керівник	1500	59,05	1	59,05
Консультант по економічній частині	1500	59,05	0,2	11,81
Консультант по охороні праці	1500	59,05	0,2	11,81
Нормоконтроль	1500	59,05	0,2	11,81
Всього				1293,37

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної і враховують виплати за час, що не пропрацював, встановлений законом. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

Зд=10%Зо; Зд=1293,37*0,1=129,33 грн

До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Сума до єдиного соціального внеску складає:

4) Відрахування до єдиного соціального внеску складає:

Зєсв=0,22(Зо+Зд);

Зєсв=0,22(1293,37+129,33) = 312,99 грн.

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР. По цій статті враховується заробітна плата апарату управління і загальногосподарських служб, витрати на потоковий ремонт будов, устаткування і інструментів, амортизаційні відрахування на їх повне відновлення і капітальний ремонт, витрати по охороні праці, витрати на винаходи і раціоналізацію, витрати на науково – технічну інформацію і рекламу, і так далі. Розмір накладних витрат на конкретну НДР визначається у відсотках до її виконання. У наукових закладах накладні витрати складають 60-120% від основної і додаткової заробітної плати.

Рнакл=(З0+Зд)*0,6;

Рнакл=0,6*(1293,37+129,33) =853.62грн.

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4.

Таблиця 2.4 Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	200.20
2. Основна заробітна плата	1293,37
3. Додаткова заробітна плата	129,33
4. Відрахування до єдиного соціального внеску	312,99
5. Накладні витрати	853.62
Планова собівартість (Спл)	2789,51

У наукових організаціях разом з плановою собівартістю визначають величину планового прибутку і договірну ціну НДР.

Плановий прибуток визначений по формулі:

Ппл=0,1*Спл

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Ппл=0,1*2789,51=278,95рн.

Договірна ціна визначається по формулі:

Цнір=Спл+Ппл;

Цнір=2789,51+278,95=3068,46 грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

ПДВ=0,2*Цнір

ПДВ=0,2*3068,46 =613,69 грн.

Звідси:

Цр=Цнір+ПДВ;

Цр=3068,46 +613,69 =3682,15 грн.

3 ОХОРОНА ПРАЦІ

В даному дипломному проекті виконується проектування бездротової мережі підприємства. Мережеві роутери, що забезпечують бездротовий доступ до Internet, розташовані у серверному приміщенні, в квадраті дії мережі. Проектована мережа Wi-Fi підключена до загальної телекомунікаційної мережі міста.

Характер робіт по будівництву та експлуатації мережі визначає правила поведінки для всіх працівників у сфері охорони праці та техніки безпеки. Основні вимоги щодо безпечного виконання робіт містяться в «Правилах техніки безпеки при роботі на кабельних лініях зв'язку і радіофікації».

Організація робочого місця при виконанні монтажу мережі. Умови праці працюючих позначаються на їх фізичному і нервовому напруженні, що не може не відбитися на продуктивності праці. Щоб цього не відбувалося необхідно виконувати заходи щодо ергономічного забезпечення. Ергономіка при будівництві та експлуатації лінійних споруджень пов'язана з продуктивністю і якістю робіт. Розглянемо компоновку робочого місця монтажника мережі.

Організація робочого місця для монтажних робіт повинна забезпечувати безпеку і зручність виконуваних робіт. Так як технологія виконання монтажних робіт носить поетапний характер, конструкція застосовуваних приладів компактна і не потрібне їх одночасне використання на одному робочому місці, а дії оператора-монтажника повинні бути високоточні, основною робочою позою є положення «сидячи».

Набір інструментів для монтажника мережі (чемоданчики, котушки з дротом), дриль, перфоратор, зварювальний апарат, рефлектометр, вимірювач сигналу та ін. має знаходитись в певному порядку, стані, та розміщуватись у робочій зоні з максимальним рівнем зручності та досяжності.

Рівень шуму на робочому місці не перевищує 46 дБА, що відповідає гранично допустимим нормам.

Роботи з монтажу мережі, коли виконуються зовнішні роботи, виходячи з місцевих умов, бажано виконувати в літній період в світлий час доби.

Для попередження, зниження або усунення нервово-психічного, зорового або м'язового напруження, монтажнику обов'язково необхідно виконувати комплекс вправ.

наступним основним вимогам: бути безпечним в роботі Організація подібним чином робочого місця монтажника, дозволяє значно зменшити стомлюваність працівника, підвищити якість монтажу, а отже і параметрів мережі.

Заходи з техніки безпеки під час монтажу мережі. До роботи з електроінструментом під час монтажу мережі допускаються особи, які пройшли навчання безпечним методам праці, перевірку знань правил безпеки та які мають кваліфікаційну групу щодо електробезпеки.

Електроінструмент повинен відповідати та мати недоступні для випадкового доторкання струмоведучі частини.

Роботи виконуються з застосуванням індивідуальних засобів захисту і заземленням корпусу інструмента класу I. При виконанні будівельно-монтажних робіт дозволяється використовувати електроінструмент тільки класів II та III і тільки з індивідуальними засобами захисту.

Заземлення корпусу електроінструмента повинно здійснюватися за допомогою спеціальної жили проводу живлення, яка не повинна одночасно служити провідником робочого струму. Використовувати для цієї мети заземлений нульовий провід забороняється. Конструкція вилки повинна забезпечувати первинний контакт для заземлення та його відключення після відключення інших контактів. Якщо такі штепсельні вилки відсутні дозволяється заземлювати інструмент голим гнучким проводом з поперечним перерізом не менше 4 мм^2, який повинен приєднуватися до спеціальної деталі для заземлення, розташованої на корпусі інструмента.

Під час роботи забороняється натягувати та перегинати кабелі електроінструмента. При припиненні електроживлення під час роботи з електроінструментом, а також на час відсутності працівника на робочому місці, інструмент повинен вимикатися від мережі. При використанні

електроінструмента забороняється: – передавати його хоча б на недовгий час іншим особам, які не мають права працювати з електроінструментом; – доторкатися до його частин що обертаються; –виймати стружку чи тирсу руками під час його роботи; –працювати з ним на висоті більше 2,5 м з приставних драбин.

З метою забезпечення безпеки монтажних робіт необхідно виконання наступних вимог:

- До початку робіт корпус монтажно-вимірювальної лабораторії (машини або модуля) повинен бути заземлений. Дрил, перфоратор, зварювальний апарат повинен бути з'єднаний заземлювальним провідником з клемою заземлення, встановленою на монтажному столі;
- Заземлювальні провідники від заземлювача і заземлюваного обладнання слід підключати до болтів і клем, позначених маркувальними знаками заземлення;
- При виконанні робіт в монтажно-вимірювальній лабораторії або модулі слід керуватися маркуванням клем і гнізд струморозподільних пристроїв, що свідчить про підводиму напругу і її полярність;
- При русі лабораторії, розміщеної в автомобілі, або транспортуванні модуля, монтажно-вимірювальна апаратура, прилади та установчі пристрої повинні бути надійно закріплені, двері закриті на замки.

При забезпеченні безпеки необхідно враховувати кількість пристроїв, що підключаються, розташування мережевого кабелю, поширення сигналу Wi-Fi і типи перешкод для нього.

Щоб уникнути несанкціонованого підключення, при прокладці кабельної мережі треба дбати про захист проводів від механічних пошкоджень, використовувати спеціальні кабель-канали і не допускати ділянок, на яких шнур буде занадто сильно провисати або, навпаки, надмірно натягнутим.

Неможна прокладати кабель поряд з джерелами сильних перешкод або в зоні з поганим середовищем (критичні температури і вологість). Також можна використовувати екранований кабель, що володіє додатковим захистом.

Дротові і бездротові мережі піддані впливу грози, причому в деяких випадках удар блискавки може вивести з ладу не тільки мережеве обладнання або мережеву карту, але і безліч компонентів ПК.

Для зменшення ризику насамперед треба використовувати заземлення електричних розеток і компонентів ПК, а також пристрої типу Pilot, в яких застосовуються захисні схеми від перешкод і стрибків напруги. Крім того, кращим рішенням може стати джерело безперебійного живлення (ДБЖ). Сучасні версії включають в себе як стабілізатори напруги і автономне живлення, так і спеціальні роз'єми для підключення через них мережевого кабелю. Якщо раптом в обладнання інтернет-провайдера вдарить блискавка, такий ДБЖ не пропустить шкідливий стрибок напруги в мережеву карту ПК. Варто пам'ятати, що в будь-якому випадку заземлення розеток або самого устаткування надзвичайно

полів необхідно:

дотримуватися важливо.

- Для зменшення впливу електромагнітних безпечної відстані - не перебувати цілодобово біля роутера Wi-Fi;

- вимикати сигнал роутера Wi-fi, коли не користування ресурсами мережі не потрібне;

- правильно розташовувати роутер Wi-fi, мінімум 2-3 м від голови людини;

- не тримати ноутбуки з включеними приймачами Wi-Fi на колінах.

- за можливості скорочувати час сеансів бездротового доступу.

Електробезпека. Відповідно до ГОСТ 12.1.019-79 під електробезпечністю розуміють систему організаційних і технічних заходів і засобів, що забезпечують захист людей від шкідливого й небезпечного впливу електричного струму, електричної дуги й статичної електрики. На відміну від інших джерел небезпеки електричний струм не можна виявити без спеціального устаткування й приладів, тому вплив його на людину найчастіше зненацька.

Проходячи через організм людини електричний струм робить термічну, електролітичну й біологічну дію. У результаті термічного впливу викликається розігрів організму й виникають опіки ділянок тіла, у результаті електролітичного

впливу розкладається кров і інші органічні рідини в організмі. Біологічний вплив проявляється в порушенні й роздратуванні тканин і мимовільному судорожному скороченні м'язів.

Значення сили струму, що проходить через організм людини, залежить від напруги під яким перебуває людина й від опору ділянки тіла до якого прикладена ця напруга. З огляду на те, що більшість поразок відбувається при напрузі 127, 220 і 380 В, а пробій шкіри починається при напрузі 40-50 В, як безпечна напруга змінного струму в нашій країні обрано 42 В, 110 В для постійного струму.

Основними причинами електротравматизму є:

- випадковий дотик до струмоведучих частин;
- несправність захисних засобів, якими потерпілий доторкався до струмоведучих частин;
- помилкове прийняття устаткування, що перебуває під напругою, як відключеного;
- несподіване виникнення напруги через ушкодження ізоляції там, де в нормальних умовах його бути не повинне;
- контакт струмопровідного устаткування із проводом, що перебуває під напругою;
- замикання фаз на землю тощо;
- поява напруги на струмоведучих частинах устаткування в результаті помилкового включення тоді, коли на ньому виконують роботу;
- замикання між відключеними й проводами, що перебувають під напругою;
- наведення напруги від сусідніх працюючих установок і так далі.

Експлуатація комп’ютерної мережі передбачає використання ПК у якості пристроїв доступу до неї. Джерелом напруги живлення ПК та Wi-Fi-роутерів є мережа змінного струму з напругою 220 В, на яку поширюється ГОСТ 25861-83.

Відповідно до вимог для попередження поразок струмом необхідно:

- чітко й у повному обсязі виконувати правила провадження робіт і правила технічної експлуатації;

- виключити можливість доступу оператора до частин устаткування, що працює під небезпечною напругою, неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення;

- застосовувати ізоляцію, що служить для захисту від поразки електричним струмом, виконану із застосуванням міцного суцільного або багатошарового ізоляційного матеріалу, товщина якого обумовлена типом забезпечуваного захисту;

- підводити електроживлення до ПК від розетки будівлі за допомогою спеціальної вилки із занулюючим контактом;

- захистити від перевантажень по струму, розраховуючи на потужність, споживану від мережі; а також захистити від короткого замикання встаткування, убудоване в мережу будинку;

- надійно підключити до заземлюючих затисків металеві частини, доступні для оператора, які в результаті ушкодження ізоляції можуть виявитися під небезпечною напругою;

- перевірити, що захисний заземлюючий провідник не має вимикачів і запобіжників, а також надійно ізольований.

Висновки по ОТ та БЖД. На підставі вище викладеного можна зробити наступні висновки: правильна організація всіх перерахованих вище заходів по монтажу мережі забезпечує надійність, високу працездатність, безпеку і нормальні умови праці робітників, запобігає нещасним випадкам і виникненню пожеж, а при їх виникненні сприяє їх швидкій ліквідації.

ВИСНОВОК

В даній роботі було вияснено, що будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи пов'язані між собою функціональні, тобто вони виконують окремі види робіт в рамках єдиного бізнес-процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вона не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми.

Також вияснено що безпровідна територіально розподілена мережа це система, що забезпечує передачу інформації між різними додатками, використовуваними в системі корпорації. Мережа являє собою мережу окремої організації. Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP та використовує комунікаційні стандарти Інтернету, а також сервісні додатки, що забезпечують доставку даних користувачам мережі.

Були обговорені питання, що до захисту інформації від несанкціонованого доступу, а також наведені кілька стратегій безпеки які можна примінити дла захисту інформації в бездротовій мережі Wi-Fi та їх розгортання.

Виявлені проблеми безпеки з якими може зіткнутися ствотена мережа.

В роботі була озроблена бездротова мережа (WLAN – wireless LAN) на основі поєднання уніфікованої бездротової інфраструктури (CUWN) Cisco, і доменної інфраструктури Microsoft, яка використовується в офісах для підключення мобільних співробітників у місцях скупчення користувачів. Проведено налаштування бездротової мережі та реалізації захисту на контролері фірми Cisco яке і використовувалось для створення всієї мережі. У висновку можна сказати , що в результаті ретельного підходу до всіх етапів проектування вдалося домогтися досить низького бюджету проекту не економлячи на обладнанні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Швиденко М.З., Матус Ю.В.: Комп’ютерні мережні технології. / Навч.-метод. Посібник/ М.З. Швиденко, Ю.В. Матус – Київ. – ТОВ “Авета”, - 2008. – 524 с.
2. Крейг Хант : Персональні комп'ютери в мережах TCP / IP: Підручник для учнів професійно-технічних навчальних закладів/ Крейг Хант; перев. з англ. - BHV-Київ, 2007. – 463с.
3. Николайчук Я.М.: «Проектування спеціалізованих комп’ютерних систем»: Навчальний посібник/ Я.М. Николайчук: Київ: Навчальна книга, 2010. – 383с.
4. Ботт Э. Эффективная работа: Безопасность Windows. [Текст] / Э. ботт, К. Зихерт - СПб.: Питер, 2009. – 682 с.
5. Воройский Ф.С. Основы проектирования автоматизированных библиотечно-информационных систем. [Текст]: Справочное пособие / Ф.С. Воройский - М.: ФИЗМАТЛИТ, 2005. – 384 с.
6. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. [Текст] / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин - М.: ДМК Пресс, 2004. – 616 с.
7. Курило А.П. Обеспечение информационной безопасности бизнеса. [Текст] / А.П. Курило – М.: ВДС-пресс, 2005. – 512с.
8. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. А.В.Соколов, В.Ф. Шаньгин– М.: ДМК Пресс, 2002. – 656 с.
9. Просис Д. Руководство по TCP/IP для начинающих [Текст] / Д. Просис // Журн. PC Magazine. 2010 р. - № 3. - С. 58-67
10. Семенов Ю.А. Протоколы и ресурсы Internet [Текст] / Ю.А. Семенов. 2002 р. 420 с.
11. Комплексные решения по построению инфраструктуры предприятия. [Электронный ресурс] : - Режим доступа : www/ URL: http:// www.lankey.ru. Загл. с екрану.2013р.