Міністерство освіти і науки України
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем

ГОЛИК Іван Іванович

КОМП'ЮТЕРНА СИСТЕМА МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА НА БАЗІ БЕЗПРОВІДНИХ РОЗПОДІЛЕНИХ МЕРЕЖ / THE COMPUTER SYSTEM OF ENVIRONMENT MONITORING IN DISTRIBUTED WIRELESS NETWORKS

спеціальність: 8.05010203 – Спеціалізовані комп'ютерні системи
магістерська програма – Спеціалізовані комп'ютерні системи

Дипломна робота за освітньо-кваліфікаційним рівнем "магістр"

Виконав студент групи СКСм-21
І.І. Голик
_____

Науковий керівник:
к.т.н., доцент І.Р. Пітух
_____

Дипломну роботу допущено до захисту:
"____"_____20___ р.

Завідувач кафедри
_____ Я.М. Николайчук

Тернопіль 2017

РЕФЕРАТ

Робота виконана на 86 сторінках та містить 26 рисунків, 11 таблиць, 26 джерел за переліком посилань.

Мета роботи. Метою досліджень є вирішення актуальної задачі моніторингу навколишнього середовища на базі безпровідних розподілених мереж.

Методи дослідження. Методологічною основою досліджень є теорія інформації, прикладна теорія цифрових автоматів, теорія алгоритмів, теорія цифрового опрацювання сигналів.

Результати роботи та їх новизна. Розроблено систему моніторингу навколишнього середовища в якій завдяки використанню різних технологій передачі даних досягнуто ряд переваг перед існуючими системами з позиції енергоспоживання та вартості обладнання.

Рекомендації по використанню результатів роботи. Розроблена система дозволяє проводити моніторинг стану земель населених пунктів, територій, зайнятих нафтогазодобувними об'єктами, очисними спорудами, складами паливно-мастильних матеріалів, добрив, стоянками автотранспорту, захороненням токсичних промислових відходів і радіоактивних матеріалів, а також іншими промисловими об'єктами.

Значущість роботи. Новітні технології бездротового зв'язку і прогрес у області виробництва мікросхем дозволили перейти до практичної розробки і впровадження нового класу розподілених комунікаційних систем – сенсорних мереж, за допомогою яких і вдалось створити і систему екологічного моніторингу.

Можливі напрямки розвитку. Подальші дослідження дадуть можливість удосконалення роботи прийомо-передавальної апаратури в умовах інтенсивних промислових завад.

Ключові слова: передавання даних, моніторинг навколишнього середовища, безпровідні розподілені мережі.

ABSTRACT

Work is executed on 86 pages and including 26 illustrations, 11 tables, 26 source after the list of references.

Purpose of work. The purpose of research is to solve the actual problem of environmental monitoring based on wireless distributed networks.

Research methods. The methodological basis of research is information theory, applied theory of digital automata theory algorithms, digital signal processing theory.

Job performances and their novelty. The system of environmental monitoring in which through the use of different data transmission technologies achieved several advantages over existing systems from the perspective of energy consumption and equipment cost.

Recommendations after the use of job performances. The system allows monitoring of land settlements, territories occupied oil and gas facilities, treatment facilities, warehouses lubricants, fertilizers, parking of vehicles, disposal of toxic industrial wastes and radioactive materials, and other industrial facilities.

Meaningfulness of work. The latest wireless technology and progress in the production of chips led to a practical development and implementation of a new class of distributed communication systems - sensor networks through which and could create a system and environmental monitoring.

Possible directions of development. Further research will enable improvement of transceiver and transmitting equipment in heavy industrial noise.

Keywords: data transfer, environmental monitoring, distributed wireless networks

ЗМІСТ

ВСТУП……. 6
1. СТАН ПРОБЛЕМНОЇ ОБЛАСТІ …….……. 9
1.1 Сучасний рівень розвитку систем екологічного моніторингу…….. 9
1.2 Аналіз систем екологічного моніторингу та області їх застосування…….…… 15
1.2.1 Лабораторія Intel…… 17
1.2.2 Сенсорні системи збору інформації……. 17
1.2.3 Самоналагоджувальні безпровідні сенсорні мережі….. 20
1.3 Напрями розвитку сенсорних мереж…….…… 23
1.4 Формування вимог та постановка задачі…….. 26
2. РОЗРОБКА СТРУКТУРИ СИСТЕМИ МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА……. 28
2.1 Технологія сенсорних мереж…….. 28
2.2 Порівняння основних характеристик стандарту ZigBee і платформи MeshLogic…….…….... 36
2.2.1 Фізичний рівень…….. 36
2.2.2 Оцінка стійкості канальної інтерференції……... 37
2.2.3 Обгрунтування вибору топології мережі……. 39
2.2.4 Механізм формування мережі…….. 41
2.2.5 Оцінка стійкості до змін в топології мережі……... 42
2.2.6 Енергетична ефективність системи…….. 43
2.3 Розробка структурної схеми системи екологічного моніторингу……. 44
3. РОЗРОБКА АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА…….. 47
1.1 3.1 Розробка апаратного забезпечення комунікаційної безпровідної мережі…… 47

1.2 3.2 Застосування технології NanoNET в системі моніторигну навколишнього середовища……... 57
1.3 3.3 Опис роботи системи моніторингу навколишнього середовища…… 60
1.4 3.4 Розрахунок показників надійності системи…… 64
1.5 4. ОХОРОНА ПРАЦІ…… 70
1.6 4.1 Аналіз потенційно-небезпечних і шкідливих виробничих факторів……. 70
1.7 4.2. Забезпечення нормативних умов праці…… 72
1.8 4.3 Забезпечення безпеки монтажу, робіт з ЕОМ……. 77
1.9 4.4 Розрахунок занулення…… 80
ВИСНОВКИ…….. 83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….. 85

ВСТУП

Актуальність теми. На сьогоднішній день практично будь-яке підприємство у своїй діяльності використовує комп’ютерну техніку. Це може бути ведення комп’ютерного бухгалтерського обліку, представлення фірми у вигляді сайту в мережі Інтернет, контактування з партнерами за допомогою електронних засобів зв’язку (електронної пошти, чату, месенджерів), автоматизація рутинних елементів робочих процесів і т.д. Відповідно постає задача покращення умов використання наявних апаратних ресурсів та отримання найбільшої ефективності від придбання нових апаратних засобів при адекватних витратах.

Сучасні комп'ютерні технології активно впроваджуються в сферу соціально-культурного сервісу і туристичного бізнесу, їх застосування стає невід'ємною умовою успішної роботи. Оперативність, надійність, точність, висока швидкість обробки і передачі інформації визначають ефективність управлінських рішень. Реалізація цих умов можлива тільки в рамках застосування інформаційних комп'ютерних систем.

Впровадження інформаційних технологій у сферу туристського бізнесу стикається з безліччю проблем, до яких можна віднести недостатнє фінансування, незадовільний рівень підготовленості працівників туріндустрії в області сучасних комп'ютерних технологій, загальний низький рівень комп'ютерної грамотності населення і незначне в порівнянні з світовим рівнем наявність домашніх комп'ютерів, порівняно невелике число користувачів Інтернету та ін. Тим не менш, загальна тенденція впровадження інформаційних технологій у сфері туризму, активна робота ряду комп'ютерних фірм, що спеціалізуються в цій області, свідчать про гарні перспективи цього напряму.

Сучасна індустрія туризму є однією з пріоритетних галузей національної економіки, бізнесу, культурного й духовного життя країни. Одним з напрямків розвитку туристичної галузі є активізація просування

регіонального туристичного продукту на внутрішньому і на міжнародному ринках туристичних послуг, підвищення якості та ефективності інформаційної інфраструктури. Найбільший ефект від їх застосування може бути досягнутий в наступних видах туристичної діяльності:

– створення туристичних Web–продуктів;

– здійснення моніторингу, особливо навколо курортів державного і місцевого значення, контроль за використанням природних лікувальних ресурсів, за забудовою всередині курортних зон.

Будь-які управлінські інформаційні процеси включають в себе процедури реєстрації, збору, передачі, зберігання, обробки, видачі інформації та прийняття управлінських рішень. Інформаційні технології являють собою ті засоби і методи, за допомогою яких реалізуються ці процедури в різних інформаційних системах.

Мета дослідження полягає у розробці комп'ютерної мережі для туристичного комплексу з виходом в Internet.

Предметом дослідження є системи та засоби комп'ютерного моніторингу об'єктів.

Об'єктом дослідження комп'ютерна мережа туристичного комплексу.

Методи дослідження: комп'ютерне моделювання програмно-апаратних засобів розподілених комп'ютерних систем.

Практичне значення одержаних результатів. Створена білінгова система адекватно реагує на зміну кількості інформації, що передається, і тим самим дозволяє проводити точний підрахунок IP-трафіку.

Напрямки подальшого розвитку полягають в розвитку корпоративної мережі, яка підтримує поштовий сервер, VPN-сервер, файловий сервер і сервер маршрутизатора, на якому встановлена створена білінгова система підрахунку IP-трафіку.

1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТУРИСТИЧНОГО КОМПЛЕКСУ ТА СПЕЦИФІКА РОЗРОБКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Характеристика туристичного комплексу «Сокільське»

Івано-Франківська область, як і Карпатський регіон в цілому, характеризуєтеся унікальними природними та рекреаційними ресурсами, які використовуються вкрай нераціонально . Тому невідкладною справою є реєстр національних культурних цінностей краю, їх дослідження, збереження і використання для розвитку Прикарпаття як туристично-оздоровчої зони, яка має унікальне поєднання неповторних ландшафтів, історичних і етнографічних пам'яток, а також пам'яток природи, культури, побуту населення.

Розвитку туризму на Прикарпатті сприяє «Програма розвитку туризму в області до 2015 року». Згідно з документами Гаазької конференції про пріоритетний розвиток внутрішнього (національного) туризму та з урахуванням його великого виховного потенціалу і можливостей у формуванні особистості громадянина, поліпшенні організації активного відпочинку населення, в тому числі дітей та молоді, першочергове значення надається розвитку екскурсійної справи, маршрутно-пізнавальному та спортивно-оздоровчому туризмові. З цією метою передбачається будівництво у цьому районі санаторіїв, лікарень, пансіонатів - дворів, виконаних з дерева у традиційно гуцульському архітектурному стилі, спортивних комплексів, кемпінгів сприятиме визначенню нових туристських маршрутів та їх поєднанню в єдиному курортно-туристичному комплексі, розрахованому на повне залучення до цього процесу місцевих природних умов, різноманітних мінеральних вод, лікарських рослин та ягід.

Туристичний комплекс "Маєток Сокільське" розмістився на гірському схилі, біля річки Черемош в селищі Тюдів в 12 кілометрах від міста Косів, Івано-Франківської області. Туристична зона, в якій розташований комплекс,

є унікальною за своїми природно-кліматичними умовами. Гори, які оточують “Сокільське”, захищають його від холодних зимових вітрів, що створює комфортні умови для відпочинку. Мальовничий вигляд з вікна, чисте повітря, сервіс на високому рівні, що ще потрібно для незабутнього відпочинку в Карпатах.

На території туристичного комплексу є свої гірськолижні траси (200, 600 і 800 метрів), для підйому на які, побудовано новий бугельний підйомник. Поруч готується до запуску крісельний підйомник і траса на 1500 м. Всі траси мають освітлення і дозволяють кататися в пізній час.

Крім цього, тут пропонують безліч додаткових послуг, які гостинно надає туристичний комплекс:

– ресторан з класичним інтер'єром запропонує страви української та європейської кухні;

– руська парна, фінська сауна, басейн, джакузі, більярд;

– конференц-зал для проведення конференцій та бізнес засідань;

– для дітей пропонується: ігровий майданчик, відкритий басейн, аніматор та дитячі екскурсії;

– екстремальні види спорту: рафтинг, пейнтбол, сезонне полювання, стрільба з лука, дартс, пневмотир, альпінізм, політ на пароплані, драйв на бричці, а також волейбол, бадмінтон, настільний та великий теніс, риболовля на форельному господарстві, оренда квадроциклів та гірських велосипедів.

Територія, яка передбачає розвиток означеної рекреаційної зони частково захоплює охоронну зону національного природного парку „Гуцульщина”. Згідно „Положення про охоронну зону національного природного парку „Гуцульщина”, у цій зоні забороняються вирубки головного користування, рибальство, влаштування місць для масового відпочинку, прокладання трубопроводів та інших комунікацій, будівництво промислових та інших об’єктів, які можуть негативно впливати на стан навколишнього середовища. Цим „Положенням ...”, також передбачено можливість зміни або ліквідація охоронної зони за розпорядженням

облдержадміністрації. З огляду на зростання популярності серед туристів, туристичний комплекс «Сокільське» має перспективний план розбудови та розвитку своєї інфраструктури. На даний час він є одним з найпопулярніших курортів Косівщини.

Сьогодні туристичний комплекс «Сокільське» має в своєму арсеналі 4-х поверховий готельний комплекс з номерами різної категорії: стандарти, напівлюкси, сімейні, люкси, а також окремо розташовані 2 дерев'яні котеджі для відпочинку компанією або родиною (рисунок 1.1).

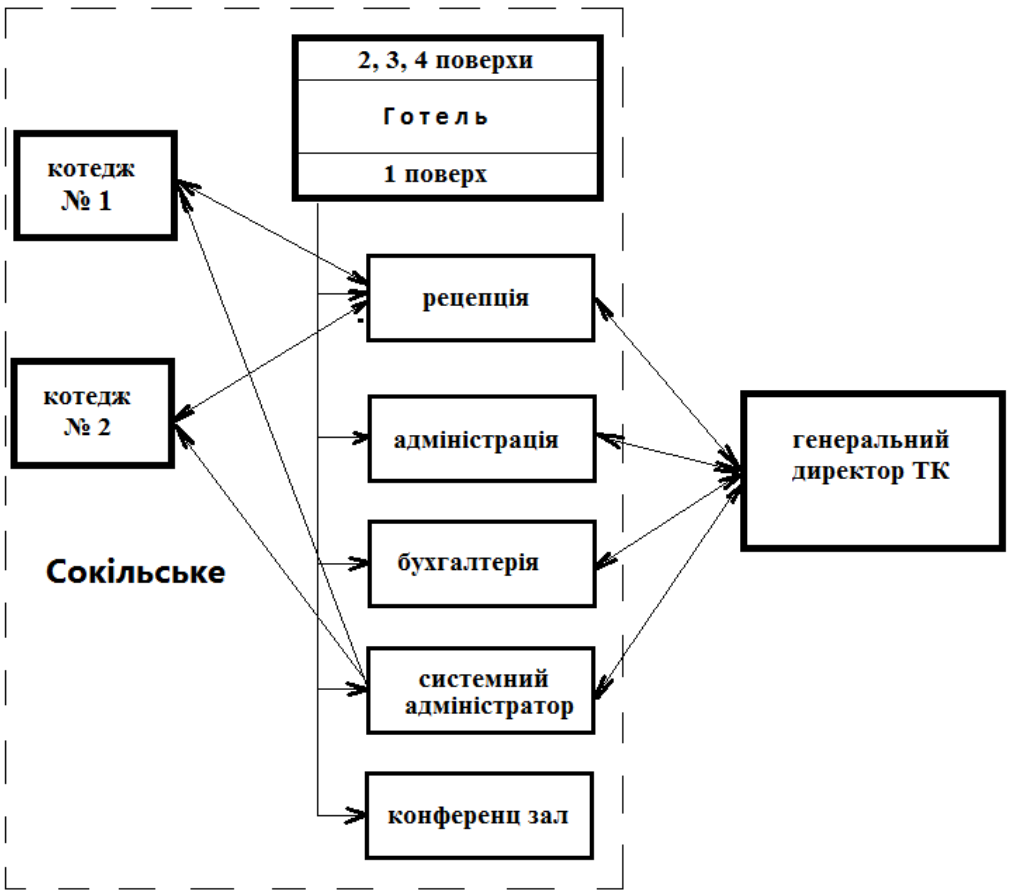


Рисунок 1.1 – Організаційна структура туристичного комплексу

На першому поверсі готелю розміщуються адміністративні приміщення, рецепція, конференц зал, столова і т.д. На кожному з трьох інших поверхах розміщено по 7 номерів. Всього готель розраховано на 21 номер різної категорії. В кожному котеджі знаходиться по 2 двоповерхові номери. «Маєток Сокільське» інтенсивно розвивається та входить до

корпоративної спілки туристичних комплексів «Гуцульщина», що знаходиться на території Косівщини.

1.2 Огляд корпоративних мереж

Розглянемо класифікацію комп’ютерних мереж залежно від характеристичних ознак [1].

Залежно від відстаней між вузлами розрізняють обчислювальні мережі: територіальні, локальні, корпоративні.

Територіальні - що охоплюють значну географічну площу. Територіальні мережі в свою чергу поділяються на регіональні і глобальні, такі, що мають відповідно регіональні або глобальні масштаби. Регіональні мережі іноді називають мережами MAN (Metropolitan Area Network), а загальна англомовна назва для територіальних мереж - WAN (Wide Area Network). Особливо виділяють єдину у своєму роді глобальну мережу Інтернет (реалізована в ній інформаційна служба World Wide Web (WWW)).

Локальні - що охоплюють обмежену територію (зазвичай в межах віддаленості станцій не більше ніж на декілька десятків або сотень метрів один від одного, рідше на 1 - 2 км). Локальні мережі (ЛМ) позначають LAN (Local Area Network).

Корпоративні (масштабу підприємства) - сукупність зв'язаних між собою ЛМ, таких, що охоплюють територію, на якій розміщено одне підприємство або установа в одному або декількох близько розташованих будівлях.

В залежності від топології з'єднань вузлів розрізняють мережі шинної (магістральної), кільцевої, зіркоподібної, ієрархічної, довільної структури [2].

Корпоративну мережу необхідно розглядати як складну систему, що складається з декількох взаємодіючих рівнів. В основі піраміди, що представляє корпоративну мережу, лежить рівень комп'ютерів - центрів

зберігання й обробки інформації, і транспортна підсистема, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами.

Над транспортною системою працює рівень мережевих операційних систем, що організовує роботу додатків у комп'ютерах і надає через транспортну систему ресурси свого комп'ютера в загальне користування.

Над операційною системою працюють різні додатки, але через особливу роль систем керування базами даних, що зберігають в упорядкованому вигляді основну корпоративну інформацію й виробляють над нею базові операції пошуку, цей клас системних додатків, як правило, виділяють в окремий рівень корпоративної мережі.

На наступному рівні працюють системні сервіси, які користуючись системами управління базами даних (СУБД), як інструментом для пошуку потрібної інформації серед мільйонів і мільярдів байт, збережених на дисках, надають кінцевим користувачам необхідну інформацію в зручній для ухвалення рішення формі, а також виконують деякі загальні для підприємств всіх типів процедури обробки інформації. До цих сервісів відноситься служба World Wide Web, система електронної пошти, системи колективної роботи та й інші сервіси.

Верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для даного підприємства або підприємств даного типу. Прикладами таких систем можуть служити:

- системи автоматизації банку;
- організації бухгалтерського обліку;
- автоматизованого проектування;
- керування технологічними процесами [1, 3].

Мета корпоративної мережі втілена в прикладних програмах верхнього рівня, але для їхньої успішної роботи необхідно, щоб підсистеми інших рівнів виконували свої функції.

1.2.1 Intranet – корпоративна мережа

Історія Intranet почалася восени 1994 р., коли Стів Теллін (фірма Amdahl) запропонував термін Intranet для визначення корпоративних інформаційних систем, побудованих на принципах мережі Internet.

Intranet – це територіально обмежена локальна обчислювальна мережа (LAN), у якій застосовується технологія побудови і сервіси представлення інформації мережі Internet. Тому базовим протоколом управління передачі інформації є TCP/IP. Для повноцінного функціонування Intranet необхідна підтримка таких протоколів:

- HTTP – протокол передачі гіпертекстів;
- SMPT, POP3 – протоколи електронної пошти;
- FTP – протокол передачі файлів;
- NNTP – протокол групи новин Usenet.

Якщо немає можливості перейти на TCP/IP, то можна використовувати спеціальні шлюзи TCP/IP компаній Firelor чи Perfomance Technologies. Шлюзи перетворюють формати пакетів між протоколами TCP/IP і IPX (міжмережевий обмін пакетами) фірми Novell або NetBIOS, спрощуючи проблему переносу TCP/IP у корпоративну LAN.

Intranet дозволяє значно підвищити ефективність праці за рахунок спільного використання інформаційних ресурсів усередині компанії (фірми, корпорації тощо) і використання технологічних концепцій Internet (Web-технології). В Intranet задачі зв’язку, виробничі завдання і процеси (наприклад, робочі взаємовідносини, інфраструктури, проекти, бюджет і графіки) визначаються в режимі он-лайн (on-line) через єдиний інтерфейс. Таким чином, Intranet – це інтелектуальний потенціал організації, де кожний окремий комп’ютер використовується оперативно з максимальною результативністю, мінімальними грошовими і трудовими видатками. Відомо, що традиційна архітектура корпоративної мережі, яка існувала до 1994 року, базувалася на сукупності сегментів LAN, пов’язаних між собою через маршрутизатор (рисунок 1.2).

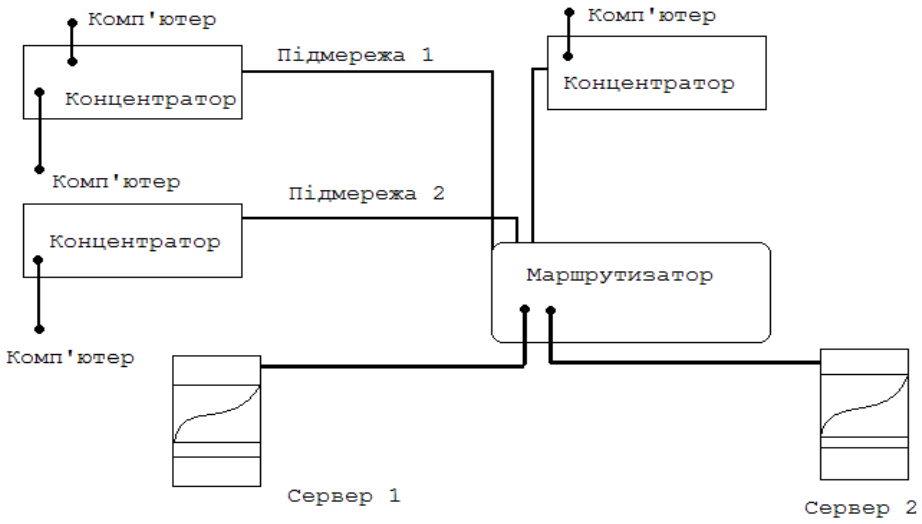


Рисунок 1.2 - Традиційна архітектура корпоративної мережі

Продуктивність мережі у такому випадку обмежується пропускною можливістю і продуктивністю магістрального маршрутизатора. В Intranet ситуація змінюється на інше (рисунок 1.3). Розглянемо деякі особливості такої архітектури. У традиційній моделі мережі “клієнт-сервер” 80 % трафіка займав обмін даними з локальним сервером і 20 % трафіка припадало на міжмережевий обмін даними. У моделі “клієнт-сервер” на основі Intranet уже не діє старе правило “80/20”, бо не можна передбачити звернення користувачів до Web-серверів, які розподілені по всій організації. Це потребує якіснішого планування Intranet.

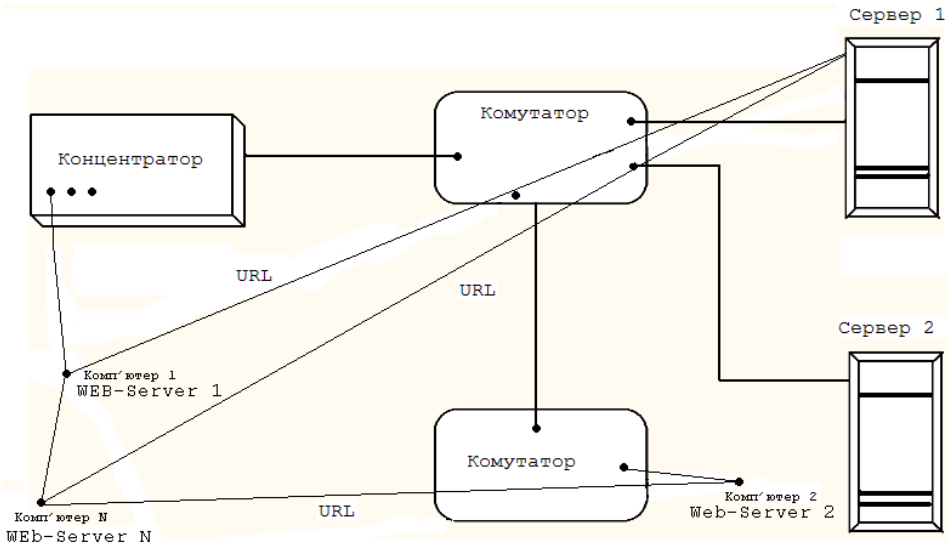


Рисунок 1.3 - Потоки трафіку в Intranet

Розповсюдження мережевих орієнтованих додатків заснованих на Web викликає експоненціальне збільшення мережевого трафіка, що вимагає підвищення вимог до швидкості і надійності пристроїв у мережі. Зростання кількості критично важливих додатків на основі Intranet, що використовують мультимедіа-інформацію зумовлює зміну структури трафіка, зокрема викликає потреби в створенні служби якості обслуговування підтримки групових додатків з інтенсивним трафіком.

Тобто, з упровадженням технології Intranet у корпоративній мережі актуальною стає потреба в зміні архітектури існуючих корпоративних чи локальних мереж.

Корпоративні мережі часто використовуються для:

– підтримки оперативних (щодня) ділових функцій, наприклад, ведення складського обліку, діловодство тощо;

– надання співробітникам компанії доступу до корпоративних документів, баз даних, друку необхідної інформації;

– ефективної підтримки внутрішньо – корпоративних інформаційних служб;

– органічного вбудовування внутрішньої інформаційної структури у загальну мережу Internet (за необхідності).

Головна перевага Intranet – це можливість доступу до будь-якої інформації, додатку, програмного забезпечення (ПЗ) в одному і тому ж “вікні” за рахунок єдиного універсального інструментарію. Це технології WAN/LAN, C1ient/Server, системи PC, UNIX, Apple тощо, але на єдиній концепції. Intranet дозволяє створювати Web-сайти відділів, груп фахівців та окремих спеціалістів для інтелектуального спілкування. Відмінність Intranet від LAN полягає у тому, що корпоративна мережа дозволяє вирішити проблему сумісності різних технологій і ПЗ різних фірм (наприклад, HP, IBM, SUN, Apple, Novell, Banyan тощо, які використовуються для побудови LAN) на рівні одного об’єкта. Модель Intranet – це універсальна надбудова над LAN. Сучасні Intranet базуються на внутрішніх корпоративних Web-

серверах, які доступні працівникам корпорації через будь-які мережі на основі протокола TCP/IP (LAN чи з'єднання Dial-Up). Web-сервери дають різну інформацію через єдиний інтерфейс (Web-броузер) за допомогою зв'язків з корпоративними базами даних, файловими серверами і сховищами документів. Web-броузер використовується для доступу до множини корпоративних Web-сторінок з гіпертекстовими зв'язками. Переваги Intranet перед платформою групових технологій groupware (наприклад, Lotus Notes, Novell Groupwise): простота, менша вартість, відсутність необхідної спеціальної підготовки обслуговуючого персоналу, універсальність (тобто незалежність від конкретного розробника ПЗ), незалежність від ОС (за рахунок використання Web-броузера), відкритість архітектури.

Основні компоненти Intranet: сервер системи; навігатор системи; гіпертекстові редактори; інструментарії для організації спільної роботи, обслуговування архівів, організації документообігу. Сервер системи чи "павутини" (стандартний, універсальний) використовується для розподілу ресурсів інформаційної системи. Він зчитує необхідні файли з дисків, запускає програми і передає клієнтським програмам (навігаторам) гіпертекстовий документ. Для цього сервер системи використовує URL (Uniform Resource Locator – уніфікований вказівник на ресурс). URL має таку інформацію для сервера:

- файлом є програма чи документ;
- якою мовою написаний файл-програма;
- які параметри передаються у файл-програму.

Для зв'язку системи з базою даних сервер використовує спеціальну програму перетворення формату бази даних у формати мови HTML за допомогою шлюзового інтерфейса Web-CGI (Common Gateway Interface).

Крім універсального використовуються і спеціалізовані сервери. Так, наприклад, усі основні виробники випустили власні Web-сервери, які можуть без CGI звертатися до бази даних. Такі сервери ефективніше використовують можливості обладнання. Сервер системи має ще одну важливу

функціональну особливість: він спостерігає за правом (паролем) доступу до документів, тобто забезпечує простий і надійний контроль за діями користувачів, що підвищує безпеку і надійність Intranet. Навігатор системи (“павутини”), чи броузер. Підтримує інтерфейс користувача з системою, отримує з різних серверів документи з графікою, які представлені у форматі HTML, і видає їх на екран чи принтер. Навігатор дозволяє використовувати різні протоколи для зв’язку з серверами, наприклад, HTTP, FTP, NNTP, SMTP. З його допомогою легше посилати повідомлення e-mail, запускати програми для перегляду визначених документів різних форматів, гіпертекстові редактори чи HTML-редактори. Використовуються для створення нових документів. Вважається, що сервер, навігатор і редактор створюють ядро Web-технології, без якого неможливо побудувати справжню Intranet – мережу.

Інструментарій узгодження Intranet з вже існуючим програмним забезпеченням має такий вигляд. Інструментарій для організації спільної роботи – це програми, які дозволяють створювати умови для спільної роботи службовців, організовувати дискусії сервер системи (наприклад, Web Crossing, Workgroup Web Forum, netThread).

Інструментарій обслуговування архівів використовується для пошуку інформації у великих базах даних корпорації, перетворення (за необхідності) форматів архівних документів у HTML, створення каталогів документів і їх пошуку. Інструментарій організації документообігу використовується для ”дроблення” документообігу об’єкта за рахунок використання стандартних процедур обробки документів, які дозволяють користувачеві заповнювати тільки стандартні спеціальні форми, а весь подальший процес оформлення документа буде виконувати програма Intranet. Наприклад, InterNotes Web Publisher, Basis Document Manager, Infobase Web Publisher, Dyna Web.

Можна виділити такі вимоги до корпоративної мережі підприємства:

– поєднання в структурованій і керованій замкненій системі всіх інформаційних пристроїв, що належать підприємству: окремих комп’ютерів і

локальних обчислювальних мереж (LAN), хост-серверів, робочих станції, телефонів, факсів, офісних АТС, онлайнових терміналів;

– забезпечення надійності функціонування та потужні системи захисту інформації; гарантування безвідмовної роботу системи як при помилках персоналу, так і у випадках спроби несанкціонованого доступу;

– забезпечення налагодженої системи зв'язку між відділеннями підприємств різного рівня (як з міськими, так і філіями в інших містах).

На сьогодні найбільш розповсюдженою в європейських країнах та актуальною для вітчизняних підприємств є топологія "зірка" – проста або багаторівнева, з головним офісом у центрі, з'єднаним із регіональними відділеннями. Її перевага визначається такими факторами:

– структурою організацій (наявністю регіональних відділень і великим обсягом інформації, що передається між ними);

– високою вартістю оренди каналів зв'язку. Але при організації зв'язку з віддаленими філіями практично не використовуються комутовані телефонні канали. Тут необхідні високошвидкісні, якісні та надійні лінії зв'язку;

– у країнах Східної Європи і СНД на користь застосування топології "зірка" впливає додатковий фактор – недостатньо розвинена інфраструктура телекомунікацій та пов'язані з цим труднощі в отриманні підприємством великого числа каналів зв'язку. У цих умовах особливо важливим стає впровадження економічних рішень, що існують на світовому ринку, а інколи і спеціально доопрацьованих до умов країн, що розвиваються.

Отже, коли виникає необхідність зв'язувати регіональні офіси один з одним безпосередньо, набуває актуальності топологія "кожен з кожним". За своїм змістом ця топологія відрізняється підвищеною надійністю і мінімальним ризиком перевантажень. Практично реалізуються численні змішані варіанти топологій, як у випадку "децентралізованого головного офісу", коли різноманітні відділи центрального офісу знаходяться в різних будинках. У деяких європейських країнах існують загальнонаціональні

конфігурації, коли корпоративні мережі окремих офісів створюють “суперзірку” із міжофісним центром, який виступає вершиною телекомунікаційної ієрархії [4-7].

1.2.2 Технологія Fast Ethernet

З розвитком інформаційних технологій пропускної здатності мережі, забезпечуваної технологією Ethernet, стало не вистачати. Мережа стала не встигати передавати дані для комп'ютерів, швидкість роботи яких істотно зросла. Мережеве середовище стало вузьким місцем, негативно позначаючись на продуктивності системи в цілому. У результаті наукових розробок був створений стандарт Fast Ethernet, розширення Ethernet із пропускною можливістю до 100 Мбіт/с. Цей стандарт одержав назву 802.3i. Стандарт Fast Ethernet містить три типи фізичного середовища: 100Base-tx, 100Base-T4, 100Base-fx. Розглянемо їх докладніше:

– 100Base-tx використовує 2 пари кабелю UTP або STP (Shielded Twisted Pair — екранована вита пара). Максимальна довжина сегмента мережі 100 м. Стандарт розрахований на застосування мережевої топології типу зірка. Центром мережі є концентратор. З'єднання кабелю з портом концентратора або мережевою картою здійснюється за допомогою роз’єму RJ-45;

– 100Base-T4 використовує 4 пари кабелю UTP третьої категорії. Трьома парам іде обмін даними: одна задіяна для розпізнавання колізій. Максимальна довжина сегмента мережі 100 м. Цей стандарт був розроблений спеціально для організації мереж зі швидкістю 100 Мбіт/с при кабелі UTP третьої категорії. Стандарт розрахований на застосування топології зірка. З'єднання кабелю з портом концентратора або мережевою картою здійснюється за допомогою роз’єму RJ-45;

– 100Base-fx стандарт визначає побудову фізичного середовища на основні багатоходового оптичного кабелю в напівдуплексному (half duplex, одночасно робота можлива тільки в одному напрямку: на передачу або на

приймання) і повнодуплексному режимах (full duplex, можлива робота відразу у двох напрямках: і на передачу, і на приймання). Довжина сегмента в повнодуплексному режимі до 2 км, у напівдуплексному до 412м.

При використанні вищевказаних мережевих протоколів, швидкість передачі даних визначається автоматично. Процес починається при включенні пристрою в мережу. Пристрою пропонується працювати у "верхньому" режимі, якщо він не підтримує, то у відповідь вказується той режим, у якому він може працювати.

У зв'язку зі збільшенням затримки повторювачами, правило 4-х хабів вироджується в правило 2-х хабів або навіть 1-го хаба. Точніше, в одному домені не може бути більш 1-го хаба (I класу) і не більш 2-х хабів (II класу). Повторювачі I і II класів відрізняються затримкою в розповсюдженні сигналу:

- для класу I затримка становить 70 бітових інтервалів;
- для класу II затримка становить 46 бітових інтервалів.

Якщо порушити встановлені вимоги, то сумарні затримки сигналу у кабелі й хабах перевищать час подвійного оберту і мережа не зможе працювати [8, 9].

1.2.3 Технологія Gigabit Ethernet

У листопаді 1993 р. була створена група для розробки специфікацій з підвищення швидкості передавання Ethernet до 100 Мбіт/с. У червні 1995 р. прийнято стандарт 100BaseT. Після підвищення швидкості доступу тісною для клієнтів стала магістраль. Тому групі з вивчення швидкісних технологій було доручено розглянути наступний рівень Ethernet.

У липні 1996р. інженерна група IEEE-802.3z почала розробку стандарту Ethernet зі швидкістю 1000 Мбіт/с. Стандарт Gigabit Ethernet IEEE-802.3z у частині, яка регламентує використання волоконно-оптичного кабелю, затверджено 25 червня 1998 р.[10]

Специфікація застосування скрученої пари виділена в окремий стандарт IEEE-8023ab. Головна організація підтримки технології Gigabit Ethernet Alliance (GEA), об'єднує понад 80 фірм.

Fast Ethernet та Gigabit Ethernet є логічним розширеннями Ethernet. Однак обидві технології грунтуються на вирішеннях інших швидкісних технологій. Наприклад, фізичний рівень FDDI був запозичений та адаптований для Fast Ethernet. Аналогічно Gigabit Ethernet планує скористатися фізичним рівнем технології Fiber Channel, що дає змогу досягти швидкості передавання близько 800 Мбіт/с, однак завдяки збільшенню швидкості передавання сигналу до 1.25 Гбіт/с потенційна швидкість передавання становитиме 1 Гбіт/с.

Первинною специфікацією передбачено волоконне-оптичні кабелі Gigabit Ethernet (одно- та багатомодові) для магістралей, сполучення комутаторів, серверів. Довжина сегмента для багатомодового кабелю - 500 м, для одномодового - 2000 м. Залежно від місця застосування окремо визначені специфікації для коаксіальних кабелів витої пари.

Для передавання інформації волоконно-оптичним кабелем запропоновано два вирішення:

– 1000Base-SX. Використання багатомодового волоконно-оптичного кабелю, передавання даних на максимальну відстань 275 м (або 550 м з застосуванням повторювача);

– 1000Base-LX. Використання як багатомодового, так і одномодового волоконно-оптичного кабелю. В останньому випадку можна передавати дані на відстань до 5000 м.

Мідні кабелі можна застосувати в таких специфікаціях:

– 1000Base-CX. Для передавання на відстань до 25 м застосовують коаксіальний кабель;

– 1000Base-T. Використовують виту пару категорій 6,7. Максимальна відстань передавання - 100м. Максимальний розмір домену - 200 м [11 - 13].

1.3 Постановка завдання

У зв’язку зі зростанням туристичного потенціалу Прикарпаття та збільшенням обсягів надання туристичних послуг виникає проблема у комфортному розміщенні туристів та наданні їм відповідних умов. Вплив інформаційних технологій на розвиток туризму величезний, оскільки прямо пов’язаний з підвищенням ефективності роботи як кожного туроператора окремо, так і усього туристичного бізнесу в цілому. Це прямо впливає на конкурентоздатність фірми на сьогоднішньому ринку. Використання комп'ютерних мереж, Інтернету та інтернет-технологій, програмні продукти наскрізної автоматизації всіх бізнес-процесів туристичного бізнесу сьогодні не просто питання лідерства і створення конкурентних переваг, але і виживання на ринку в найближчому майбутньому. Аналізуючи стан та враховуючи просторовий аспект туризму, дуже перспективним є застосування сучасних інформаційних технологій.

Метою даного проекту є розробка локальної мережі з виходом в Internet. Враховуючи специфіку діяльності туристичного комплексу та розміщення приміщень необхідно передбачити декілька точок доступу з безпровідним інтернетом. Для контролю та моніторингом за отримані послуги необхідно передбачити впровадження білінгової системи рахунку трафіку. Для розв’язку поставленої мети, необхідно вирішити ряд взаємопов’заних задач. Для розробки та проектування мережі необхідно визначити:

- архітектуру мережі;
- середовище передачі даних (тип кабелю);
- топологію мережі;
- метод доступу до середовища;
- метод передачі даних;
- спосіб управління мережею.

2 РОЗРОБКА КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Структурна схема мережі

Комплекс «Сокільське» є складовою частиною туристичного комплексу національного природного парку «Гуцульщина». Він складається з 4-х поверхового готелю (рисунок 2.1) та 2-х котеджів, які знаходяться в гірські місцевості на деякій відстані один від одного. Його інфраструктура постійно розвивається та розбудовується, тому необхідно спроектувати комп'ютерну мережу, яка б задовольняла вимогам ведення сучасного бізнесу, дозволяла надавати якісні послуги в сфері ІТ-технологій та мала можливості подальшого розвитку та удосконалення.

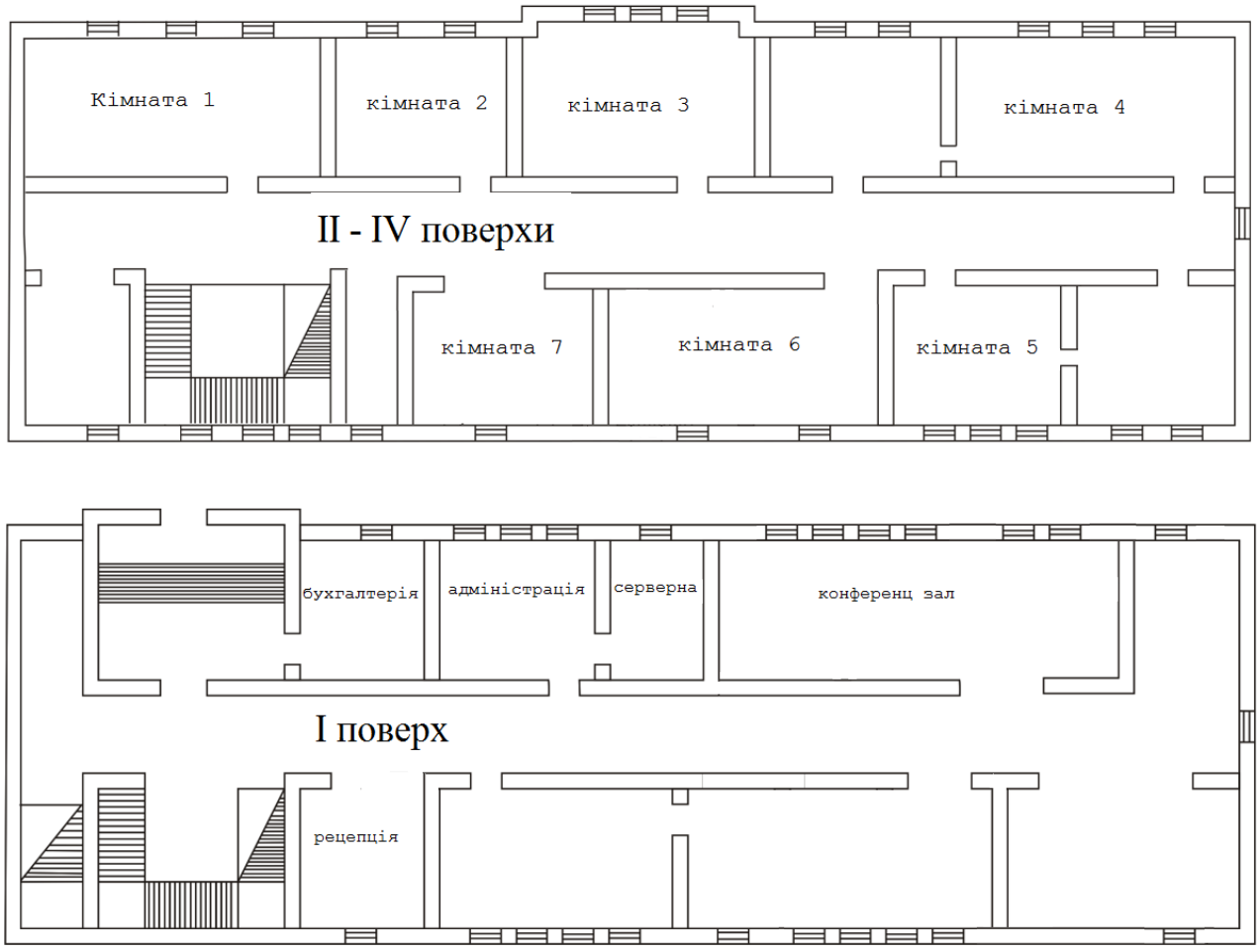


Рисунок 2.1 – План готелю

Виходячи з вищенаведеного комп'ютерна мережа ТК «Сокільське» буде складатися з двох частин: локальна комп'ютерна мережа готелю та безпровідна мережа, яка має на даний момент 2 зовнішні точки доступу в котеджах. Структурна схема мережі комплексу показана на рисунку 2.2.

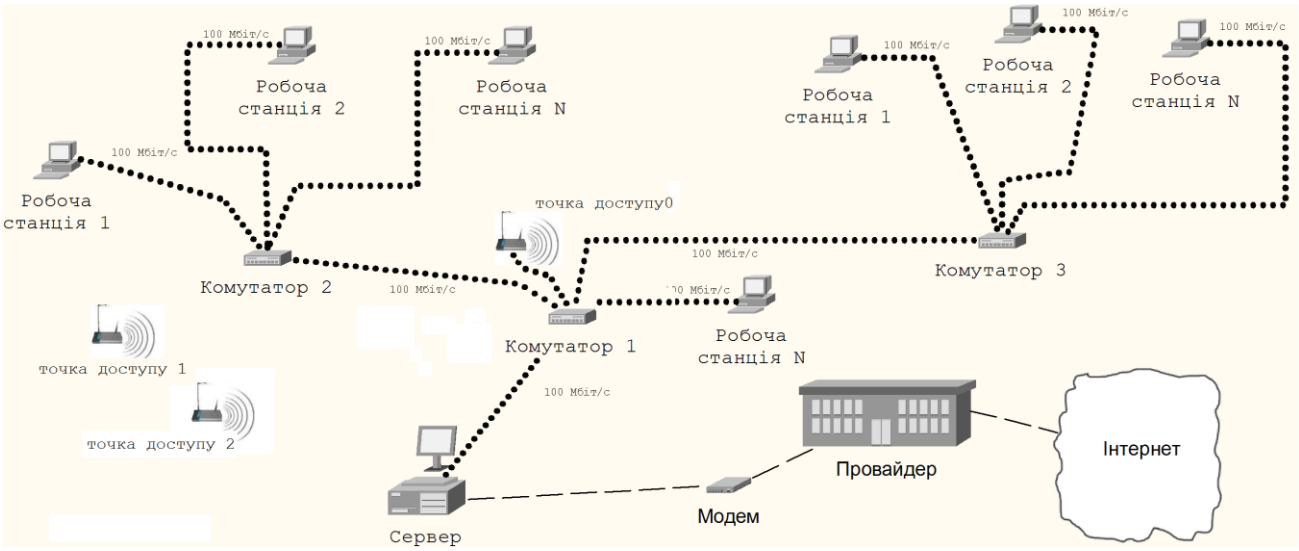


Рисунок 2.2 – Структурна схема комп'ютерної мережі

Локальна комп'ютерна мережа використовує стандарт 100 BASE-TX, має 21 робочу станцію, 4 комутатори, 1 сервер і 1 модем.

Класичною проблемою мережі зображеної на рисунку 2.2 є високий рівень трафіку, який наближується до 50% пропускної здатності, і зумовлює цим збільшення колізій. Вищевказане в свою чергу призводить до збільшення часу доступу до ресурсів. Для більшості підприємств плата за трафік є важливою. Тому існує проблема підрахунку трафіку, що витрачається кожним користувачем, і встановлення цілей, на які цей трафік був витрачений [14].

2.2 Вибір мережевого обладнання

При побудові локальної мережі туристичного комплексу було використано неекрановану виту пару п'ятої категорії. Вита пара 5 категорії

придатна для передачі даних у комп'ютерних мережах зі швидкістю не більш 100 Мбіт/с і частотою до 300 Мгц включно. Використовується при прокладці мереж класу 100Base–TX і 1000Base-T. Застосування оптоволокна виправдане тільки при застосуванні для зв’язку всередині та між будинками.

Також потрібно врахувати, що довжина одного сегмента мережі для кабелю на витій парі на може перевищувати 100м. Це значить, що реально в кабельному каналі довжина кабелю не повинна перевищувати 90 м. Запас 10м необхідний для з’єднань розетка – комп’ютер, запасу у крос-панелі й монтажній шафі. При проектуванні мережі потрібно враховувати заземлення загального для всіх комп’ютерів мережі, а якщо не врахувати, то між різними ми контурами заземлення, що не мають загального заземлюючого елементу, виникає різниця потенціалів. Оскільки єдиним провідним елементом між цими пристроями є кабель корпоративної мережі, то потенціали зрівнюються шляхом протікання електричного струму через UTP кабель. Якщо в одному із заземлень відбулося коротке замикання, то може призвести не тільки до збоїв у роботі мережі, але і до виходу з ладу устаткування [15, 16].

При проектуванні локальної мережі варто особливу увагу звернути на наявність загального заземлення всієї мережі.

Мережа повинна забезпечувати швидкість передачі даних 100 Мбіт/с і 1000 Мбіт/с. При такій організації, мережа працюватиме в режимі мікросегментації - це означає, що знімаються обмеження на час подвійного оберту і залишаються тільки обмеження на максимальну довжину сегменту.

2.2.1 Активне обладнання комп’ютерної мережі в приміщенні

Комутатор 3 Com Office connect Switch 8, призначений для використання в мережах підприємства.

Із можливостей комутатора можна виділити такі:

– механізм автоматичного вибору швидкості 10/100 Мбіт/с і 10/100/1000 Мбіт/с для всіх портів комутатора дозволяє без яких-небудь

настроювань визначити швидкість підключеного пристрою й забезпечити оптимальну продуктивність мережі;

– простота установки: комутатор може функціонувати відразу після першого підключення, не вимагаючи додаткового настроювання;

– пріоритет трафіка IEEE 802.1p, дозволяє забезпечити ефективне функціонування мережевих додатків, що передають аудіо чи відеодані;

– автоматичне визначення режиму MDI/MDIX для всіх портів комутаторів, спрощує розширення мережі, дозволяючи виключити типові помилки при розведенні мережевих кабелів.

Мережева карта 3Com EtherLink 10/100 PCI вибрана для мережі, в зв'язку з тим, що вона забезпечує високу швидкість передачі даних, просте адміністрування, стабільну роботу.

Для з'єднання вузлів мережі використовується:

– 3 комутатори в Office connect Switch 8 для мережі;

– один центральний управляючий комутатор 3Com Switch 5500G-EI 48-Port.

Комутатор 3Com Switch 5500G-EI вибрано центральним управляючим комутатором в зв'язку з тим, що він продемонстрував малий показник загублення пакетів, велику швидкість пересилки пакетів, вміння автоматично розпізнавати IP – телефони і в динамічному режимі переміщувати їх у виділену голосову віртуальну мережу.

2.2.2 Пасивне обладнання комп'ютерної мережі

Виті пари проводів використовуються в найдешевших і на сьогоднішній день, мабуть, самих популярних кабелях. Кабель на основі витих пар являє собою пару скручених ізольованих мідних проводів у єдиній діелектричній оболонці. Він досить гнучкий і зручний для прокладки.

Звичайно в кабель входить дві виті пари або чотири виті пари. Неекрановані виті пари характеризуються слабкою захищеністю від зовнішніх електромагнітних перешкод, а також слабкою захищеністю від

підслуховування з метою, наприклад, промислового шпигунства. Перехоплення переданої інформації можливе як за допомогою контактного методу (за допомогою двох голок, уткнутих у кабель), так і за допомогою безконтактного методу, що зводиться до радіоперехоплення випромінюваних кабелем електромагнітних полів. Для усунення цих недоліків застосовується екранування. У випадку екранованої витої пари STP кожна із витих пар міститься в металевій плівці - екрані для зменшення випромінювань кабелю, захисту від зовнішніх електромагнітних перешкод і зниження взаємного впливу пар проводів один на одного (crosstalk - перехресні наведення). Природно, екранована вита пара набагато дорожча, ніж неекранована, а при її використанні необхідно застосовувати й спеціальні екрановані рознімання, тому зустрічається вона значно рідше, ніж неекранована вита пара. Основні переваги неекранованих витих пар - простота монтажу роз'ємів на кінцях кабелю, а також простота ремонту будь-яких ушкоджень у порівнянні з іншими типами кабелю. Всі інші характеристики в них гірше, ніж в інших кабелів. Наприклад, при заданій швидкості передачі загасання сигналу (зменшення його рівня в міру проходження по кабелі) у них більше, ніж у коаксіальних кабелів.

Якщо врахувати ще низьку перешкодозахищеність, то стає зрозумілим, чому лінії зв'язку на основі витих пар, як правило, досить короткі (звичайно в межах 100 метрів). У цей час вита пара використовується для передачі інформації на швидкостях до 100 Мбіт/з і ведуться роботи з підвищення швидкості передачі до 1000 Мбіт/с.

Патч-корд - це засіб для комутації телекомунікаційних ліній і каналів в кросовій шафі або на патч-панелі, сполучає одну лінію зв'язку з іншою, а також використовується для підключення мережного адаптера комп'ютера до кабельної системи. Патч-корд і комп'ютерні розетки є найуразливішими місцями при експлуатації комп'ютерних мереж. Тоді як магістральний кабель і механізми розеток заховані в кабельні канали або закладені в стіну, патч-корд залишається незахищеними для зовнішніх дій.

Для того, щоб уникнути порушення геометрії патч-корду в місці з'єднання кабелю з коннектором, використовуються спеціальні ковпачки з подовженими хвостовиками, що збільшують радіус вигину кабелю при провисанні.

Інформаційні розетки призначені для підключення кінцевого устаткування (наприклад, локальних комп'ютерів) до комп'ютерної мережі. В комутаційних розетках використовується з'єднання типу 110 або KRONE з технологією заміщення ізоляції (IDC), дозволяє проводити більше 200 перекомутацій без погіршення фізичних і електричних характеристик розетки. Також розетки розрізняються за способом монтажу - внутрішні і зовнішні. Дуже зручні модульні розетки, що дозволяють швидко міняти модуль і додавати нові порти у встановлений корпус, і комбінувати порти (комп'ютерний і телефонний в одному корпусі) на робочому місці для підключення різного устаткування (комп'ютери, телефони, принтери і факси) [7, 16].

2.3 Структура корпоративної мережі

Використовуючи вибране вище мережеве обладнання, було розроблено структуру комп’ютерної мережі (рисунок 2.3), яка відповідає вимогам поставленим завданням проекту.

На рисунку 2.4 наведено схему розведення кабелів в туристичному комплексі (ТК). На першому поверсі знаходиться сервер та 4 робочі станції. Крім того, до центрального управляючого комутатора підключено зовнішню точку доступу для бездротового з’єднання, антена якої поставлена на 4 поверсі готелю для безперебійного передавання сигналу. На 2, 3, 4-му поверхах розміщується 7 робочих станцій, кожну з яких під’єднано до комутатора Office connect Switch 8. Тип мережі 100Base-TX, розмір приміщення 18м х 12м.

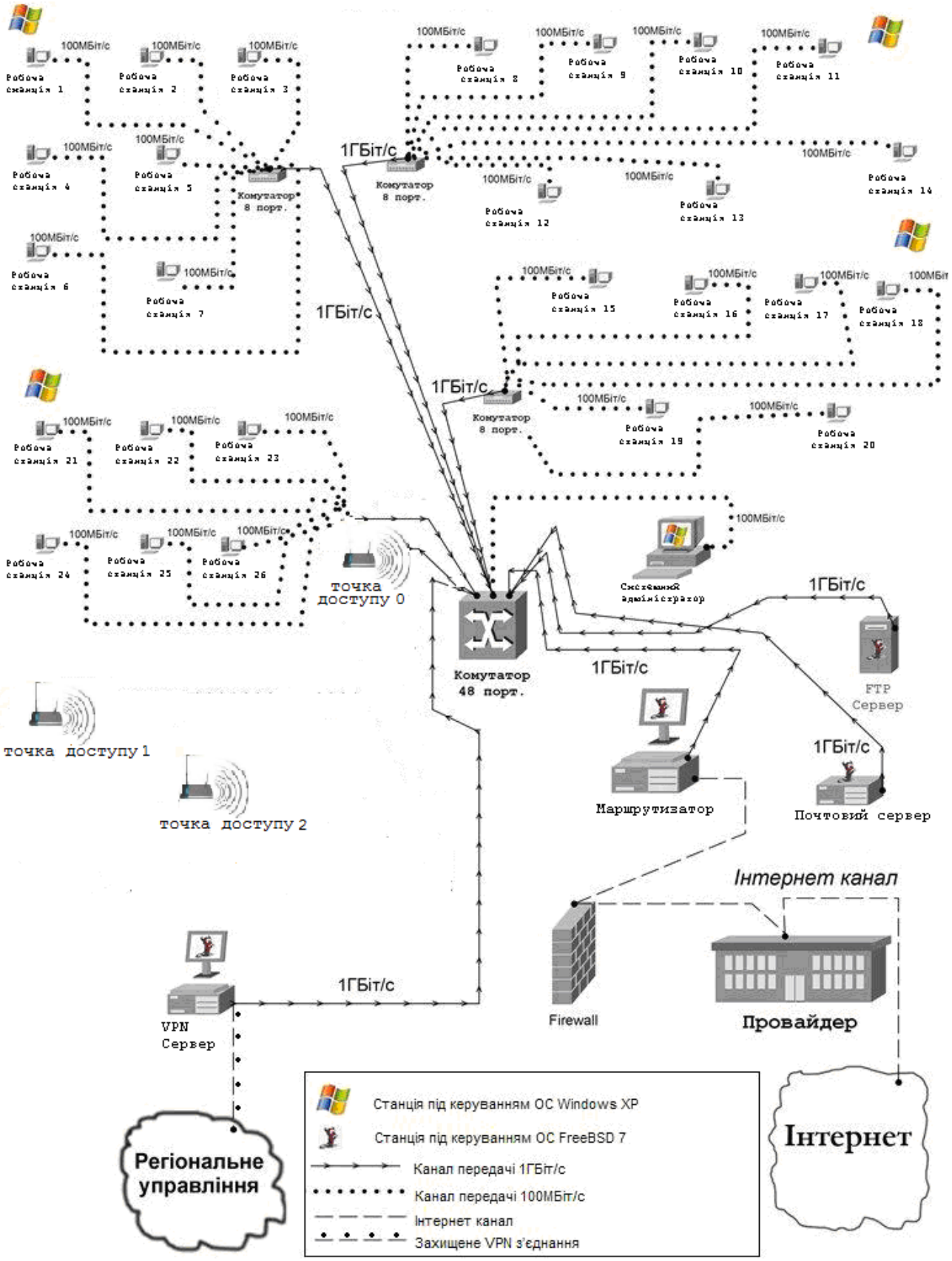


Рисунок 2.3 – Структура розробленої комп'ютерної мережі ТК

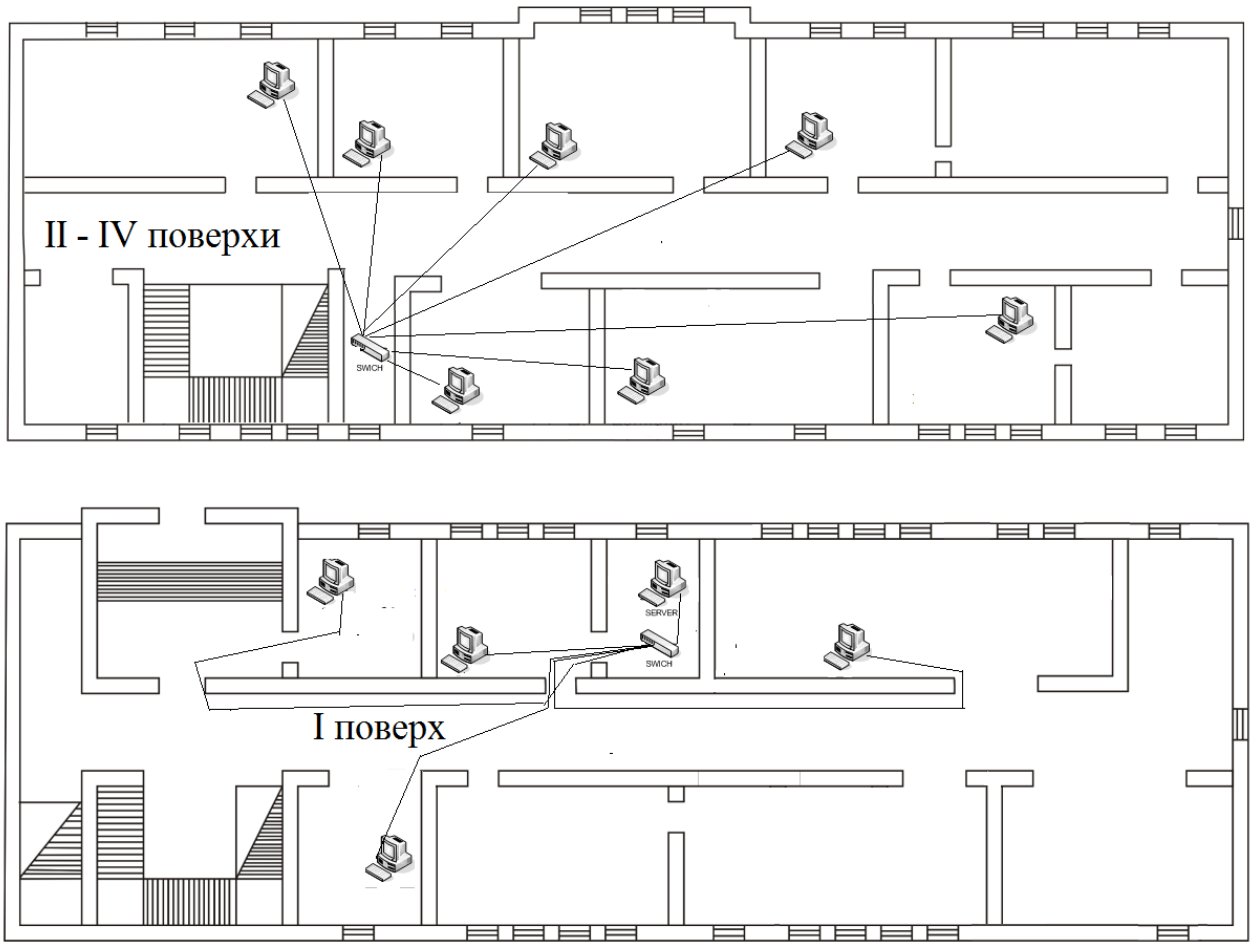


Рисунок 2.4 – Схема розведення кабелів в приміщенні ТК

Необхідна довжина кабелю розраховується з використанням наступного емпіричного методу [1]. Виходячи із припущення, що робочі місця розподілені рівномірно, обчислюється середня довжина ($L_{ср}$) кабельних трас по формулі:

$$L_{ср} = (L_{max} + L_{min})/2, \quad (2.1)$$

де L_{min} й L_{max} – відповідно довжини кабельної траси від точки розміщення кросового обладнання до інформаційного роз'єму найближчого й самого далекого робочого місця, пораховані з урахуванням технології прокладки кабелю, всіх спусків, підйомів, поворотів й особливостей будинку. При визначенні довжини трас необхідно додати технологічний запас величиною 10% від $L_{ср}$ і запас X для процедур розведення кабелю в розподільному вузлі й інформаційному роз'ємі.

Отже, довжина трас L складе:

$L= (1,1L_{ср}+X)\cdot N$ де N – кількість розеток на поверсі.

Розрахуємо кількість кабелю, необхідну для кожного поверху, і просумуємо. Дробові значення округляємо до цілих.

Для першого поверху L_{min} ,L_{max} рівні відповідно 12 й 26 метрів.

$L_{ср} = (12+26)/2 = 19$ м.

$L = (1,1\cdot 19+2)\cdot 5= 114,5$ м.

Для другого та вищих поверхів L_{min1} ,L_{max1} рівні відповідно 15, 32 метрів.

$L_{ср1} = (15+32)/ 2= 23,5$ м.

$L1 = (1,1\cdot 23,5+2)\cdot 7 = 195$ м.

Разом для мережі необхідно:

Lзаг = 114,5+3*195= 699,5 м кабелю.

Кабелі при заведенні в кімнату укладаються в захисні пластикові короби фірми Legrand, лідера в даній галузі. Найбільший пучок, заведений у кімнату, складає 5 кабелів.

Площа такого пучка складає

$P=(0.0052\cdot 0.0052\cdot 3.14/4)\cdot 5=0.00010632$(м2).

Максимальне заповнення коробів приймемо за 60 %. Тоді короб 20Х12,5 має корисну площу 0,00025 м2.

Співвідношення площі пучка до площі короба складе 0,4252. Відповідно, для прокладання в кімнаті буде використовуватись короб з розмірами 20Х12,5.

Розрахунок метражу коробів ведеться за схемою прокладки кабелів із запасом 20%, тому що можливі відхилення на місці. При заводі в кімнату вважаємо, що витрачається 2,5 метра на зниження до рівня розеток - 0.5 м.

Розрахунок кутів і заглушок також виконується за схемою розміщення коробів і кабель-каналів.

Кабельні канали забезпечують можливість одночасної прокладки в них силової й інформаційної проводки, гарантуючи захист кабелів від зовнішніх механічних впливів і впливу навколишнього середовища. Забезпечують

збереження презентабельного виду офісних приміщень, у тих випадках, коли прокладка кабелів прихованим способом недоцільна або неможлива.

Для переходу від одних коробів до інших в стінках робочих приміщень свердляться отвори, в які встановлюються заставні труби.

Комутаційний шнур, комутаційний кабель або патч-корд (від англ. patching cord - з'єднувальний шнур) - використовуються для підключення робочих станцій до інформаційних розеток або для комутації на патч-панелях. Доступні довжини від 1 до 10 метрів, але не варто забувати, що максимальна довжина патч-корду, використовуваного на підприємстві, обмежена стандартом ISO 11801 до 5 метрів. Патч-корди розраховані на 2000 циклів підключення.

Комутаційні шнури (пасивне) є невід'ємною частиною структурованих кабельних систем. Їх функціональність набагато серйозніша, ніж це здається з першого погляду. Патчкорд є сполучною ланкою між кабельної системою, що знаходиться в кабельних каналах і кінцевим обладнанням.

Фізично він являє собою фрагмент кабелю довжиною до 5 метрів, що має з обох сторін роз'єми (коннектори). Існують комутаційні шнури для мереж на основі витої пари, на основі волоконно-оптичного кабелю, також пасивне для телефонних мереж.

Патч-корд - це засіб для комутації телекомунікаційних ліній і каналів в кросовому шафі або на патч-панелі. Він з'єднує одну лінію зв'язку з іншою. Також використовується для підключення мережевого адаптера комп'ютера до кабельної системі.

Комутаційні шнури - як і будь-який інший компонент спеціалізованої комп’ютерної системи (СКС), є продуктом з гарантовано високим терміном служби. Але, на відміну від інших компонентів, пасивне і гнізда комп'ютерних розеток є найбільш вразливими місцями при експлуатації СКС. У той час як магістральний кабель і механізми розеток заховані в кабельні канали або забиті в стіну, патчкорди залишаються незахищеними для зовнішніх впливів. Для того щоб уникнути порушення геометрії патч-

корду в місці з'єднання кабелю з коннектором, використовуються спеціальні ковпачки з видовженими хвостовиками, що збільшують радіус вигину кабелю при провисанні.

Патч-корди EvroMedia виготовляються з багатожильного кабелю перетином 24 AWG. На контакти конекторів, що використовуються в патч-кордах, нанесено 50-мікронне золоте покриття. Робиться це для того, щоб уникнути окислення контактів в місці стику конектора патч-корду і гнізда розетки. Конектори для патч-кордів поставляє компанія EvroMedia, відома у всьому світі, як виробник якісних з'єднань.

Готові патч-корди EvroMedia відповідають категорії 5e (Category 5 Enhanced) і призначені для роботи в сучасних високошвидкісних мережах, таких як 100Base-TX, Gigabit Ethernet, Voice, ATM і інших.

У приміщенні серверної встановлюється 19” шафа 26U 600x1000 мм ServerMax. В ній розміщуватимуться сервер та комутатор 3Com Switch 5500G-EI.

2.4 Устаткування для віддаленого зв’язку

Для організації віддаленого зв’язку між серверною та котеджами використовується Wi-Fi технологія.

На сучасному етапі розвитку мережевих технологій, технологія бездротових мереж Wi-Fi є найбільш зручною в тих умовах, що вимагають мобільність, простоту установки і використання. Wi-Fi (від англ. wireless fidelity - бездротовий зв'язок) - стандарт широкосмугового бездротового зв'язку сімейства 802.11. Як правило, технологія Wi-Fi використовується для організації бездротових локальних комп'ютерних мереж та корпоративних мереж, а також створення так званих гарячих точок високошвидкісного доступу в Інтернет [16].

У бездротовій локальній мережі є два типи обладнання: клієнт (звичайно це комп'ютер, укомплектований бездротовою мережевою картою,

але може бути і інший пристрій) і точка доступу, яка може виконує і роль моста між бездротовою і кабельною мережами. Точка доступу містить приймач-передавач, інтерфейс дротяної мережі, а також вбудований мікрокомп'ютер і програмне забезпечення для обробки даних [17].

В нашому випадку потрібно об’єднати два сегмента кабельної мережі в єдину мережу з використанням радіоканалу. Таке об’єднання в єдину мережу здійснюється за допомогою режиму бездротового мосту між двома точками доступу. Прості в установці і настройці мости використовують основний для них тип зв'язку “точка-точка”, дозволяючи з'єднати (point-to-point) їх в єдину мережу.

Отже, для того, щоб розширити збут точок доступу, виробники вирішили зробити їх більш універсальними і зручними у використанні - додали в них функції мостів, що дозволило точку доступу з'єднуватися з іншими точками доступу, утворюючи тим самим аналог підключення через бездротові мости. Тому точка доступу може працювати в одному з режимів:

– точка доступу (класичний, з можливістю підключення клієнтів для створення бездротової мережі);

– міст в режимі “точка-багато точок”;

– міст між точками доступу (для об’єднання LAN-мереж);

– клієнт (здатний перетворити будь-який Ethernet-пристрій на клієнтський для з’єднання з точкою доступу в режимі “інфраструктура” або, рідше, “точка-багато точок”).

Останні два режими при настройці з’єднання можуть потребувати значення MAC-адреси головної та віддаленої точок доступу. При використанні функцій бездротового моста слід застосовувати однакові продукти по обидві його сторони - більшість компаній не дають гарантій роботи своїх точок доступу у всіх режимах при підключенні до них пристроїв інших виробників.

Тому в нашому випадку потрібно до кожної з кабельних мереж підключати точку доступу одного виробника, які з’єднуються одна з одною по радіоканалу.

Для зв'язку типу “точка-точка” потрібно використовувати направлені антени. Вони мають різний коефіцієнт підсилення і відрізняються одна від одної шириною формованого променя і конструктивного виконання. Правильний підбір антени для точки доступу забезпечує ефективне покриття всієї обслуговуваної площі і підвищує надійність зв'язку.

Розглянемо питання організації бездротової мережі на основі обладнання компаній D-Link, яка є лідером у виробництві бездротового обладнання. Розглянувши продукцію даної фірми ми обираємо точку доступу D-Link DAP-1160 (рисунок 2.5).

Рисунок 2.5 - Зовнішній вигляд точки доступу D-Link DAP-1160

Важливою характеристикою даного пристрою, є його здатність передавати дані на швидкості 150Мбіт/с.

DAP-1160 може бути налаштована для різних режимів роботи, включаючи такі режими:

- як точка доступу - для роботи в якості концентратора для підключення бездротових користувачів;
- бездротового роутера - для одночасного підключення кількох бездротових користувачів з мережі ISP;
- повторювач - для збільшення радіусу дії бездротової мережі .

Таблиця 2.1

Специфікація точки доступу DAP-1160

Інтерфейси пристрої	+ 802.11n бездротова LAN + 1 порт 10/100Base-TX Ethernet LAN
Стандарти	+ 802.11g + 802.11b + 802.11n + 802.3/802.3u 10Base-T/100Base-TX Ethernet + ANSI / IEEE 802.3 NWay auto-negotiation
Діапазон частот	2,4 - 2,4835 ГГц
Кількість каналів	+ FCC: 11 + ETSI: 13
Робочі режими	+ Точка доступу + Маршрутизатор + Повторювач
Антена	Знімна односпрямована антена з коефіцієнтом посилення 2dBi (з роз'ємом RP-SMA)
Швидкість передачі даних	+ 802.11n: до 150 Мбіт / с + 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Мбіт / с + 802.11b: 1, 2, 5.5, 11 Мбіт / с
Безпека	+ 64/128-бітное WEP-шифрування даних + WPA-PSK, WPA2-PSK + WPA-EAP, WPA2-EAP + TKIP, AES + Фільтрація MAC-адрес + Функція SSID broadcast disable
Управління пристроєм	+ Web-інтерфейс управління на основі Internet Explorer v.6 або вище, Netscape Navigator v.6 або вище або іншого браузера з підтримкою Java.
Розміри	144 x 109 x 30 мм

Для зв'язку типу “точка-точка” ми використаємо направлені антени D-Link ANT24-1801 – це антена типу Yagi (хвильовий канал) з підсиленням сигналу 18dBi. Зовнішній вигляд точки доступу D-Link DAP-1160 представлено на рисунку 2.6.

Рисунок 2.6 - Зовнішній вигляд антена точки доступу D-Link ANT24-1801

Антена працює в діапазоні частот 2,4 -2,5 ГГц. Антена ANT24-1801 підключається до бездротових пристроїв, що мають RP-SMA-роз'єм і надає можливість розширення площі покриття існуючої бездротової мережі, що працює в діапазоні 2,4 ГГц.

У комплект поставки антени входить кріплення для монтажу, кабель-перехідник для роз'єму RP-SMA і модуль грозозахисту.

2.5 Проектування WI-FI мережі

Крім готелю, в якому спроектовано комп’ютерну мережу, на території комплексу знаходиться 2 котеджі. Отже, слід налаштувати радіоканал передачі даних між котеджами та серверною в готелі. Розглянемо схему бездротового з’єднання (рисунок 2.7).

Для забезпечення бездротового зв’язку між сегментами мережі використаємо точки доступу D-Link DAP-1160. Точку доступу в серверній та котеджах налаштовуємо на роботу в режимі WDS “точка-точка”. Для цього в

обох будівлях встановимо по точці доступу, та під’єднаємо їх до існуючої кабельної мережі, налаштуємо їх для виконання передачі даних.

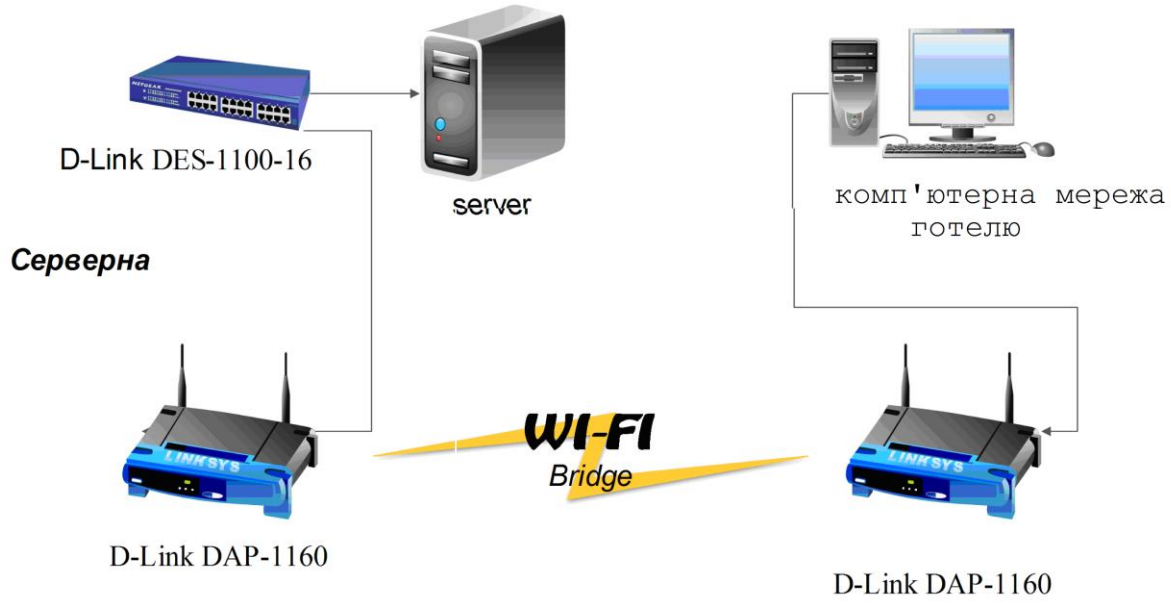


Рисунок 2.7 - Схема бездротового з’єднання

D-Link DAP-1160 закріпимо на стіні за допомогою спеціальних гнізд на корпусі. Підключення D-Link DAP-1160 є чи не найпростішим підключенням подібних пристроїв. Насамперед, під’єднаємо антену D-Link ANT24-1801 до роз’ємну RP-SMA. Підключаємо живлення через відповідний порт на точці доступу на корпусі спалахує відповідна лампочка. Потім за допомогою кабелю, сполучаємо LAN-порти точки доступу і центрального комутатора провідникової мережі. Спалахує лампочка “LAN”.

2.6 Налаштування точки доступу

Для управління DAP-1160 реалізований достатньо зручний веб-інтерфейс. Пристроєм можна керувати буквально з будь-якого комп'ютера, що знаходиться в локальній мережі, за допомогою звичайного браузера.

Для входу в меню настройок (рисунок 2.8) необхідно поставити перемикач на задній панелі пристрою в положення AP. Підключити пристрій

до комп'ютера кабелем, що поставляється в комплекті. Відкрити Internet Explorer і набрати у рядку адресу: dlinkap. Ім'ям користувача за замовчуванням – “admin”, пароль – порожній.

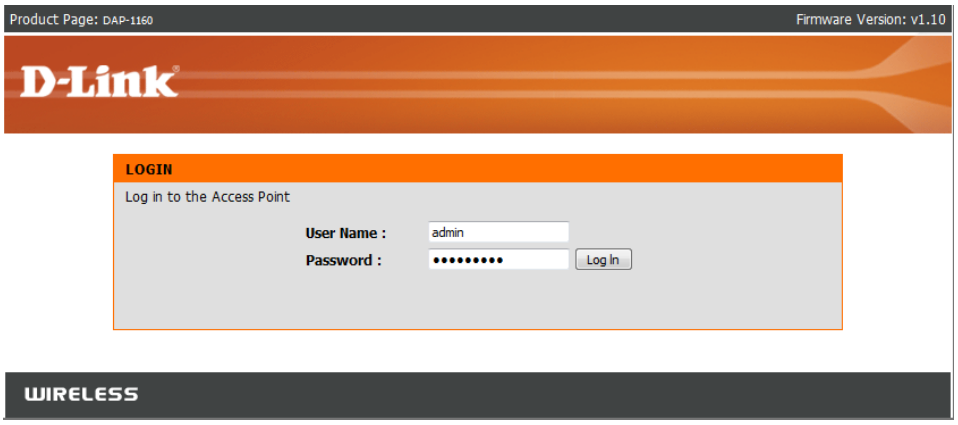


Рисунок 2.8 – Вхід в меню настройок DAP-1160

У нашому випадку потрібно налаштувати дві точки доступу в режимі міст „точка-точка”.

Для налаштування точок доступу котеджу і серверної необхідно виконати наступне (рисунок 2.9): вказати тип мережі, режим її роботи, в полі SSID вказати назву безпровідної мережі, наступне поле дозволяє або забороняє SSID.

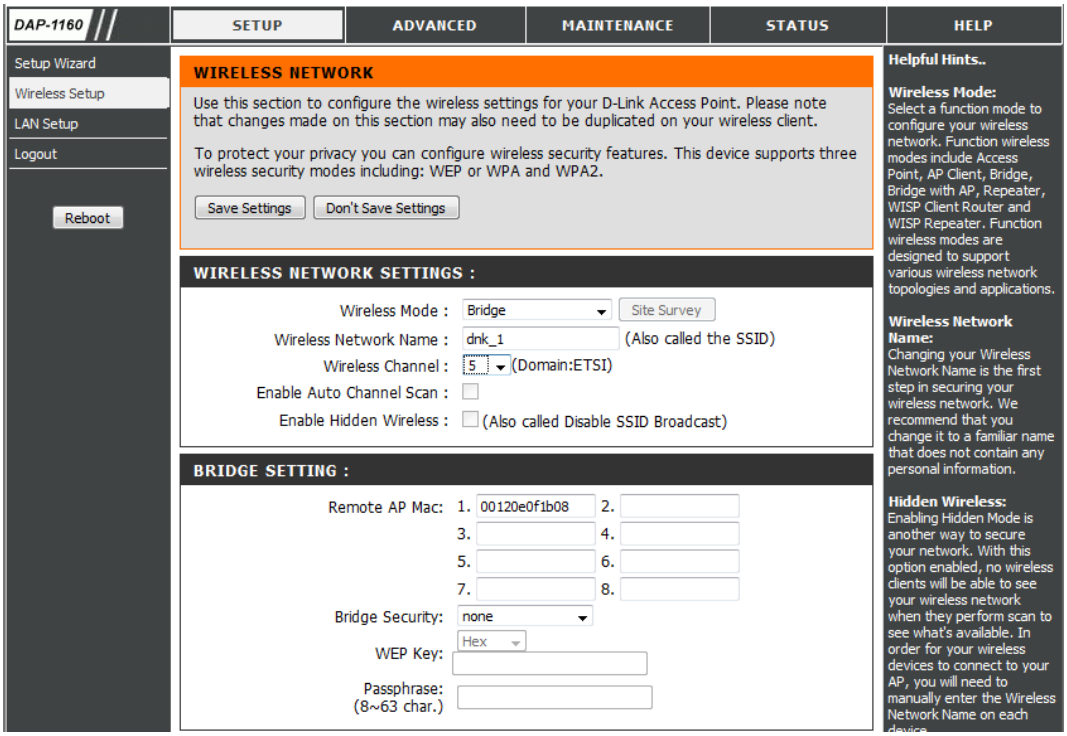


Рисунок 2.9 – Налаштування точки доступу

Далі необхідно вказати номер каналу, на якому працюватиме точка доступу. Для всіх бездротових пристроїв даної мережі це поле повинно бути однакове. Далі необхідно вказати MAC адресу іншої точки доступу тобто на точці доступу в котеджі вказуємо MAC адресу точки із серверної, та навпаки на точці з серверної вказуємо MAC адресу з котеджу.

Далі налаштовуємо шифрування даних, які передаватимуться по Wi-Fi мережі (рисунок 2.10). В полі аутентифікації вибираємо режим захисту безпровідної мережі; вибираємо тип ключа – шіснадцятковий (HEX) або ASCII , розмір 64 біти (128біт, 152біт). Вводимо чотири ключі в відповідних полях.

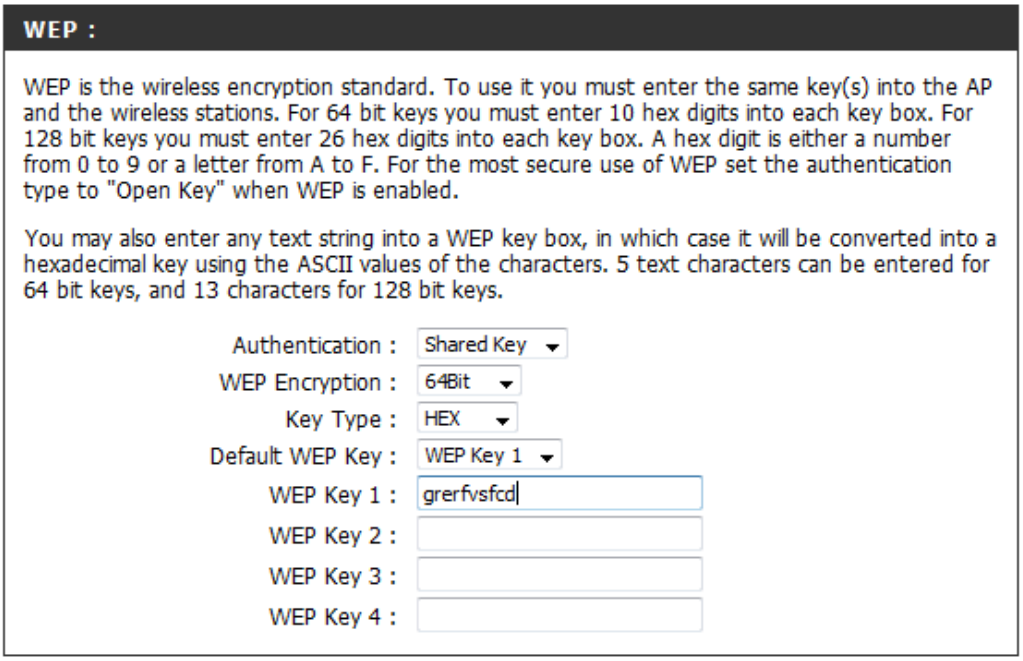


Рисунок 2.10 – Налаштування шифрування

DAP-1160 дозволяє настроювати параметри, що впливають на швидкість роботи: швидкість передачі (TX Rate), Beacon interval, RTS Threshold, Fragmentation, DTIM interval, тип преамбули, аутентифікація, режим тільки-11g.

Для контролю безпеки DAP-1160 можна налаштувати на збереження всіх подій в журналі, причому можливе сумісне використання пристрою з сервером журналів, для цього необхідно вказати лише його IP-адресу, далі журнали автоматично зберігатимуться на сервері.

Перегляд поточного стану пристрою можна здійснити на закладці “Статус”. Всі параметри пристрою, такі як фізичні (MAC) адреси, логічна (IP) адреса, маска підмережі, шлюз, параметри сервера DHCP, SSID, шифрування, канал і режим роботи, завжди можна дізнатися тут.

2.7 Операційна система комп’ютерної мережі

Мережева операційна система (ОС) управляє всіма ресурсами і відповідає за оптимальну роботу мережі. Задача мереженої ОС полягає в тому, щоб створити платформу доступу для усіх користувачів до сервера і роботи в мережі. ОС повинна бути багатозадачною і виконувати такі функції – підтримку роботи програм, забезпечувати захист даних, керувати роботою мережі, керувати роботою усіх пристроїв, які підключені до сервера тощо. До таких систем можна віднести: Net Bios, PC LAN, OS/2, Windows NT, UNIX, Net Ware [1].

UNIX – має багато модифікацій, але однакові принципи роботи, модульна структура, легко розширюється і налагоджується, широкий вибір послуг (текстовий редактор, СУБД тощо). Застосовується як для роботи відокремленого ПК, так і сервера і робочої станції. Може підтримувати роботу сервера бази даних (БД), обчислювального сервера, мережевого сервера, мережевого маршрутизатора, від 900 до 2000 робочих станцій разом з периферійними пристроями. ОС UNIX існує більше 3-х десятиріч, постійно оновлюється в розвивається та займає одне з лідируючих місць серед ОС .

В новій корпоративній мережі було використано ОС FreeBSD і Windows XP. ОС FreeBSD використовується на серверних системах, адже дана ОС показала стабільну роботу, надійність, простоту використання, а також безплатність у отриманні і адмініструванні (рисунок 2.11). ОС FreeBSD забезпечує сумісність з деякими іншими UNIX-подібними операційними системами, зокрема, з Linux [15].

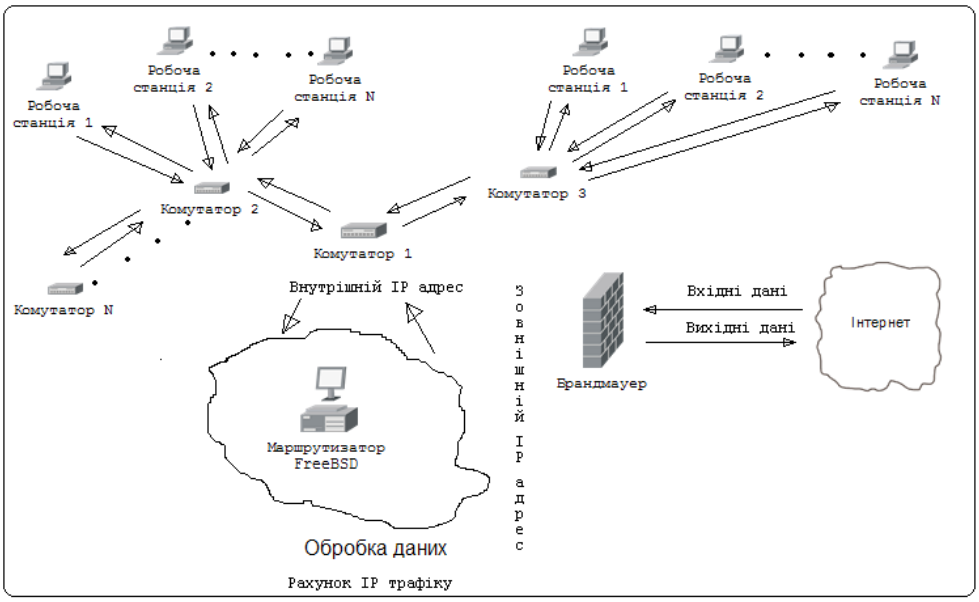


Рисунок 2.11 – Функціональна схема роботи корпоративної мережі

Для робочих станцій використано ОС Windows XP, як систему, котра добре зарекомендувала себе при роботі з офісними додатками, обробкою відео, звуку, а також як система для роботи з бухгалтерським програмним забезпеченням [2, 18, 19].

Вибір сервера. Як сервер доцільно вибрати DHCP (англ. Dynamic Host Configuration Protocol - протокол динамічної конфігурації вузла) - мережевий протокол, що дозволяє комп'ютерам автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP. Даний протокол працює за моделлю «клієнт-сервер». Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережевого пристрою звертається до так званого сервера DHCP, і отримує від нього потрібні параметри. Мережевий адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості мереж TCP / IP. Протокол DHCP надає три способи розподілу IP-адрес:

– ручний розподіл. При цьому способі мережевий адміністратор зіставляє апаратного адресою (для Ethernet мереж це MAC-адресу) кожного

кліентскогокомпьютера певний IP-адресу. Фактично, даний спосіб розподілу адрес відрізняється від ручного налаштування кожного комп'ютера лише тим, що відомості про адреси зберігаються централізовано (на сервері DHCP), і тому їх простіше змінювати при необхідності;

– автоматичний розподіл. При даному способі кожному комп'ютеру на постійне використання виділяється довільний вільний IP-адреса з певного адміністратором діапазону;

– динамічний розподіл. Цей спосіб аналогічний автоматичному розподілу, за винятком того, що адреса видається комп'ютера не так на постійне користування, а на певний термін. Це називається орендою адреси. Після закінчення терміну оренди IP-адреса знову вважається вільним, і клієнт зобов'язаний запросити новий (він, втім, може виявитися тим же самим). Крім того, клієнт сам може відмовитися від отриманої адреси.

2.8 Тестування мережі і пошук несправностей

Тестування мережі проводиться за допомогою спеціального обладнання. Можна виділити дві категорії такого обладнання:

– аналізатори фізичного рівня;

– аналізатори більш високих рівнів моделі OSI.

Кабельна система тестується тільки аналізаторами фізичного рівня. Найбільш відомий з приладів перевірки кабельної системи – це кабельний сканер (рисунок 2.12).

Рисунок 2.12- Кабельний сканер

Мережу можна тестувати за допомогою підручних і недорогих засобів. Це може бути Lan – тестер будь-якої модифікації, що підтримує тестування кабелів, обтиснутих під роз'єм RJ-45. Для тестування кабелю можна також використати звичайний тестер (рисунок 2.13) з функцією звукового тестування.

Рисунок 2.13– Пристрій для тестування фізичного каналу зв'язку

Перевірити правильність оброблення контактів можна візуально або за допомогою тестера.

Візуальний метод полягає в послідовній перевірці обтиснення всіх розеток, патч-панелей і патч кордів, метод простий і дешевий. Недоліком є громіздкість і більша ймовірність помилитися при перевірці великого числа розеток.

Перевірка за допомогою Lan-тестера діагностує правильність з'єднання, але не оцінює характеристики каналу.

Перевірка надійності з'єднання в контактах виконується за допомогою lan-тестера, він перевіряє правильність розведення контактів, але не перевіряє якість з'єднання в контактах. Коли внаслідок поганого обтиснення або дефекту кабелю, механічних дефектів розетки або патч-панелі має місце, нестійкий контакт, то виявити такий контакт можна за допомогою тестера. Оскільки потрапити в роз'єми патч-панелі тестера досить складно. Та й контактні групи можна погнути, необхідно застосувати дві однакові панелі. З однієї сторони цієї панелі будуть роз'єми RJ-45, а з другої сторони – контакти з підписаними номерами.

В зв’язку з вищевказаним, необхідно провести тестування розробленої корпоративної комп’ютерної мережі за допомогою lan – тестера і звичайного тестера.

Важливою складовою частиною повсякденної роботи є моніторинг стану мережі. Моніторинг здійснюється як на основі даних активного мережного устаткування, так і на основі вбудованих програм діагностики мережі. Перевірку передачі пакетів по мережі здійснюється за допомогою команди `ping –a ip-адрес комп’ютера`, перевіркою маршруту командою `traceroute` , переглядом таблиці маршрутизації – командою `netstat –nr`.

При цьому необхідно пам'ятати, що колізії в мережі в середньому не повинні перевищувати 20 %. А в піку допускається рівень колізій до 40-50 %. Причина в тому, що з ростом числа колізій пропускна здатність каналу знижується [17, 20, 21].

3 СТВОРЕННЯ БІЛІНГОВОЇ СИСТЕМИ ПІДРАХУНКУ ТРАФІКУ

3.1 Налаштування серверної системи для роботи з мережею

Підключення внутрішньої корпоративної мережі підприємства до мережі Internet зазвичай проходить через маршрутизатор, встановлений між внутрішньою мережею підприємства і мережею Internet.

В якості маршрутизатора використовуємо комп'ютер з двома мережевими адаптерами і спеціальним чином налаштованої ОС FreeBSD.

3.1.1 Використане програмне забезпечення

Для побудови системи рахунку IP трафіку було використано безкоштовний програмний продукт BPFT (Berkley Packet Filter Traffic). Система побудована на основі бібліотеки libpcabi використовує механізм BPF (Berkley Packet Filter "pseudo-device") для захвату IP – трафіку.

При виборі СУБД було вибрано MySQL 5, яка зарекомендувала себе, як стабільна при роботі з базами даних система. Вищевказане СУБД підтримує багатопотоковість, декілька одночасних запитів, оптимізацією зв'язків при з'єднанні багатьох даних за один захід, записи фіксованої і змінної довжини, ключові поля та спеціальні поля в операторі CREATE.

Для роботи з базою даних була вибрана мова програмування - PHP (Hypertext Preprocessor). Однією з основних переваг PHP є написання скриптів, працюючих на стороні сервера. PHP підтримує можливість обробляти дані різних форм, генерувати динамічні сторінки, відсилати та приймати, а також створювати скрипти на стороні сервера для виконання їх в командному рядку.

Одним із значних переваг PHP є підтримка широкого кола баз даних і різних операційних систем.

3.1.2 Система підрахунку IP - трафіку

Функціонально в системі білінгу можна умовно виділити три модуля: рахунок трафіку, вивід інформації про використаний трафік, модуль доступу і заборони користувачам користуватися мережею Internet.

В базі “traffic” створюємо дві таблиці: ‘IP’ – дані про IP адреса і ‘Log’ – дані про трафік.

```
CREATE DATABASE traffic
    DEFAULT CHARACTER SET koi8r
    DEFAULT COLLATE koi8r_general_ci;
USE traffic;
CREATE TABLE Ip (
    IP              VARCHAR(15) NOT NULL PRIMARY KEY,
    QUOTA           INTEGER,
    PCNAME          VARCHAR(100),


    FNAME           VARCHAR(100),
    MNAME           VARCHAR(100),
    LNAME           VARCHAR(100),
    EMAIL           VARCHAR(200),
    INDEX(IP)
) ENGINE = MyISAM;

CREATE TABLE Log (
    NN          INTEGER(12) UNSIGNED AUTO_INCREMENT NOT NULL
PRIMARY KEY,
    IP_FROM     VARCHAR(15) NOT NULL,
    IP_TO       VARCHAR(15) NOT NULL,
    SRC_PORT    VARCHAR(5) NOT NULL,
    DEST_PORT   VARCHAR(5) NOT NULL,
    PROTO       VARCHAR(4) NOT NULL,
    DATA_BYTES  INTEGER NOT NULL,
    ALL_BYTES   INTEGER NOT NULL,
    FIRST_TIME  TIMESTAMP NOT NULL,
```

```
        LAST_TIME   TIMESTAMP NOT NULL,
        INDEX(IP_FROM), INDEX(IP_TO), INDEX(SRC_PORT),
    INDEX(DEST_PORT),      INDEX(PROTO),      INDEX(ALL_BYTES),
INDEX(FIRST_TIME),
        INDEX(IP_FROM,FIRST_TIME), INDEX(IP_TO,FIRST_TIME)
    ) ENGINE     = MyISAM
      ROW_FORMAT = fixed;
```

З скрипта видно, що в якості формату бази була вибрана – MyISAMI, яка забезпечує велику швидкість роботи за рахунок відсутності транзакцій. Параметр "ROW_FORMAT" визначає, яким чином потрібно зберігати рядки в файлі бази даних. Задавши цьому параметру значення "fixed", ми в MySQL під кожну змінну типу VARCHAR виділяємо не реально зайняте її значенням місце, а максимально можливе.

3.1.3 Налаштування ОС FreeBSD

Для роботи маршрутизатора на ОС FreeBSD в ядрі ОС було включено підтримку pseudo-device BPF, і в файлі конфігурації додано рядок:

```
device  bpf  #Berkeley packet filter
```

Також установлено і налаштовано trafd, MySQL, PHP та інші програмні продукти із портів.

Налаштування основних параметрів trafd проведене в файлі rc.conf, наступним чином:

```
trafd_enable="YES"
trafd_ifaces="nfe0 rl0"
trafd_flags="-p -r"
trafd_log="/var/log/traffic.log"
trafd_pid="/var/run/trafd"
```

Білінг в якості аналізатора трафіку використовує пакет trafd, тому непотрібно писати свою утиліту для запису log файлів. В склад пакету trafd

входить утиліта traflog, яка може експортувати дані трафіка в будь-який текстовий файл відповідно до формату, що заданий в його конфігураційному файлі – traflog.format. В traflog.format був прописаний формат sql – команди вставки для розробленої бази:

```
my_sql {
from:"insert into log (ip_from,ip_to,src_port,dest_port,proto,data_bytes,all_bytes,first_time,last_time) values('%s',"to:"'%s',"
sport:"'%s',"
dport:"'%s',"
proto:"'%s',"
bytes:"'%ld',"
psize:"'%ld',"
ltime:"'%y-%m-%d %T',"
ltime:"'%y-%m-%d %T');\n"
```

Для зв’язки trafd і MySQL було написано два командні файли: trafd_dump і trafd_to_mysql.

```
#!/bin/sh
. /etc/rc.conf

for iface in ${trafd_ifaces}; do
    if [ -f ${trafd_pid}.${iface} ]; then
      kill -INT `cat ${trafd_pid}.${iface}`
      logger -t trafd_dump "signaling trafd on ${iface} dump to file"
    else
      logger -t trafd_dump "trafd on ${iface}: file ${trafd_pid}.${iface} not found (trafd don't listen on ${iface}?)"
    fi
done
```

Скрипт ‘trafd_to_mysql’ імпортує дані трафіка на всіх прослуховуючих trafd інтерфейсах з тимчасових файлів, створених trafd_dump, в базу MySQL, а інформація про успішне або неуспішне передавання команди зберігається в syslog:

```
#!/bin/sh

. /etc/rc.conf

for iface in ${trafd_ifaces}; do
    if [ -f /var/trafd/trafd.${iface} ]; then
      logger -t trafd_to_mysql "inserting traffic data
for ${iface} into mysql"
      /usr/local/sbin/traflog -a -o my_sql -n -i
/var/trafd/trafd.$iface | /usr/local/bin/mysql --
host=${trafd_db_server} --user=${trafd_db_user} --
password=${trafd_db_password} traffic
      rm /var/trafd/trafd.$iface
    else
      logger -t trafd_to_mysql "failed to insert traffic
data for ${iface} into mysql: file /var/trafd/trafd.${iface} not
found"
    fi
done
```

Для того, щоб ці два скрипта запускалися регулярно кожні 5 хвилин в налаштуваннях ОС потрібно зайти в директорію /etc/ у файл crontab і записати:

```
*/5 * * * *
  root/usr/local/sbin/trafd_dump && sleep 30 &&
/usr/local/sbin/trafd_to_mysql
```

Доступ до мережі Internet в корпоративній мережі організовуємо за допомогою PPOE. Крім того встановлюємо і налаштовуємо аналізатор трафіку IPFW.

Налаштування PPOE для доступу до Internet :

```
default:
set log Phase tun command


set ifaddr 10.0.0.1/0 10.0.0.2/0
enable dns
nat enable yes


Provaider:
 set device PPPoE:nfe0:
 set authname login
 set authkey password
 set dial
 set login
 set ifaddr 0 0
 add default HISADDR
```

3.1.4 Веб-інтерфейс системи підрахунку трафіку

Перегляд статистики, як для користувачів так і для адміністраторів здійснюється будь-яким браузером через веб - інтерфейс, реалізований у вигляді HTML-сторінки з кодом на мові програмування PHP.

При відкритті в браузері ресурсу, який є розміщений по назначеному адміністратором мережі для сторінки статистики адресу, користувач побачить існуючу базу даних статистики по свому IP-адресу (рисунок 3.1).

Захист інтерфейсу адміністратора від несанкціонованого доступу може бути реалізований різними способами. Наприклад якщо в якості веб-сервера використано Apache, можна використати файли `.htaccess` і `.htpasswd`.

За допомогою цих файлів можна керувати доступом до ресурсів веб-інтерфейсу. На сторінці адміністратора можна переглядати IP - статистику усіх користувачів мережі (рисунок 3.2).

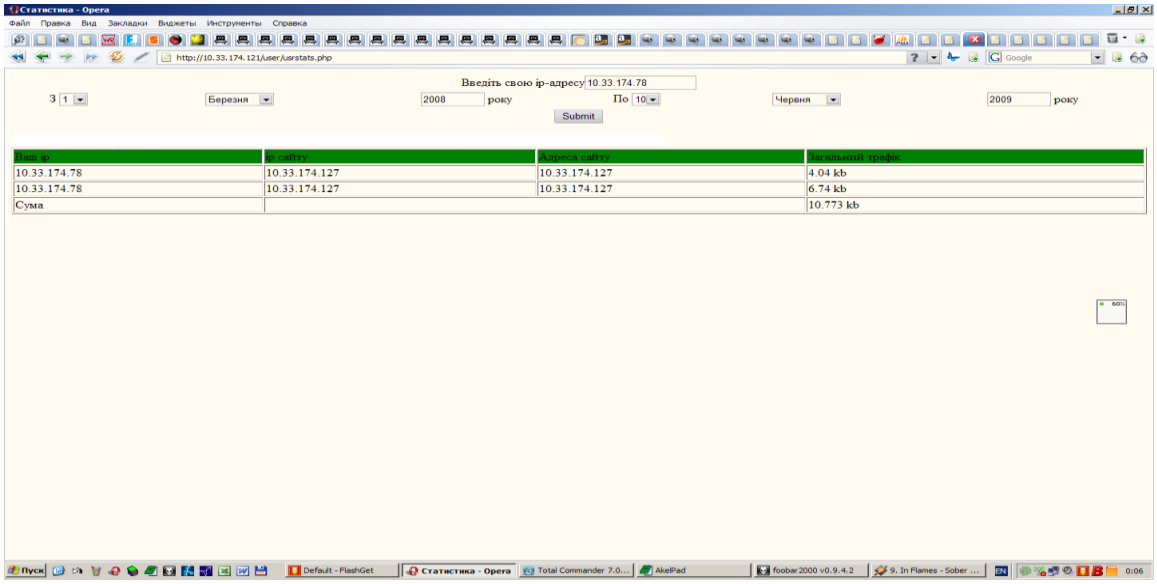


Рисунок 3.1 – Статистика використання трафіка користувачем мережі

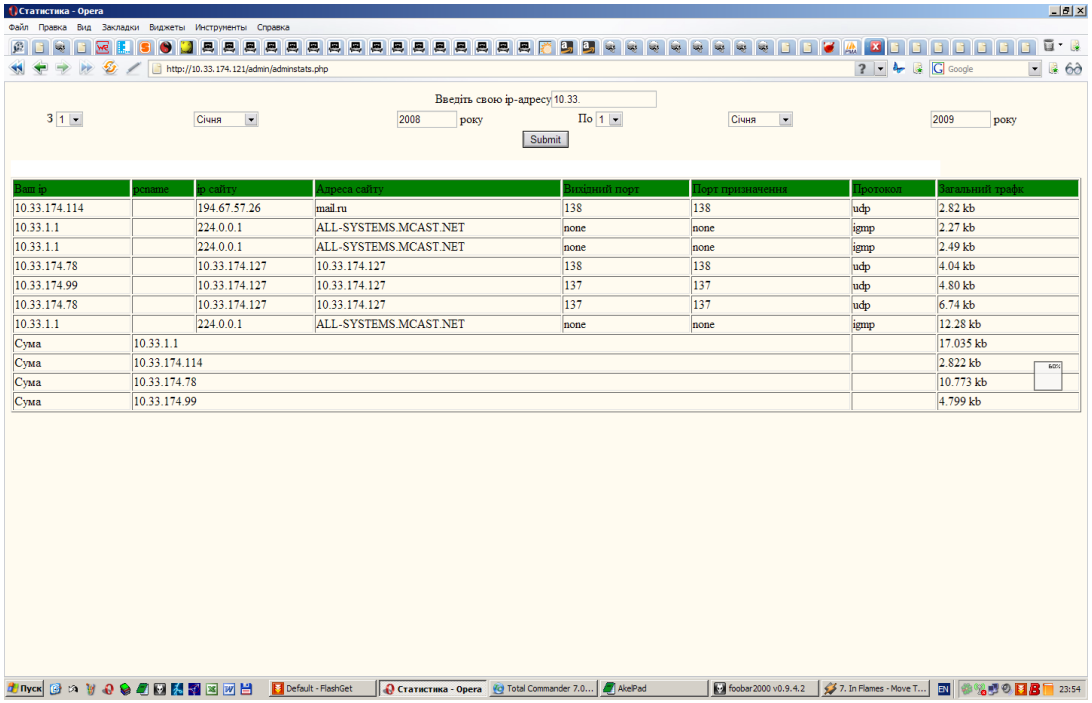


Рисунок 3.2 – Статистика використання трафіка користувачами мережі з підсумованим трафіком для кожного IP адреса в мережі

Адміністратор має доступ до папки admin на веб-сервері, а також до веб-орієнтованої системи управління базою даних MySQL, безкоштовного програмного пакету phpMyAdmin (рисунок 3.3), де він має можливість редагувати інформацію в базі даних, стежити за стабільною роботою БД, і створювати нові БД, також редагувати і створювати таблиці в БД.

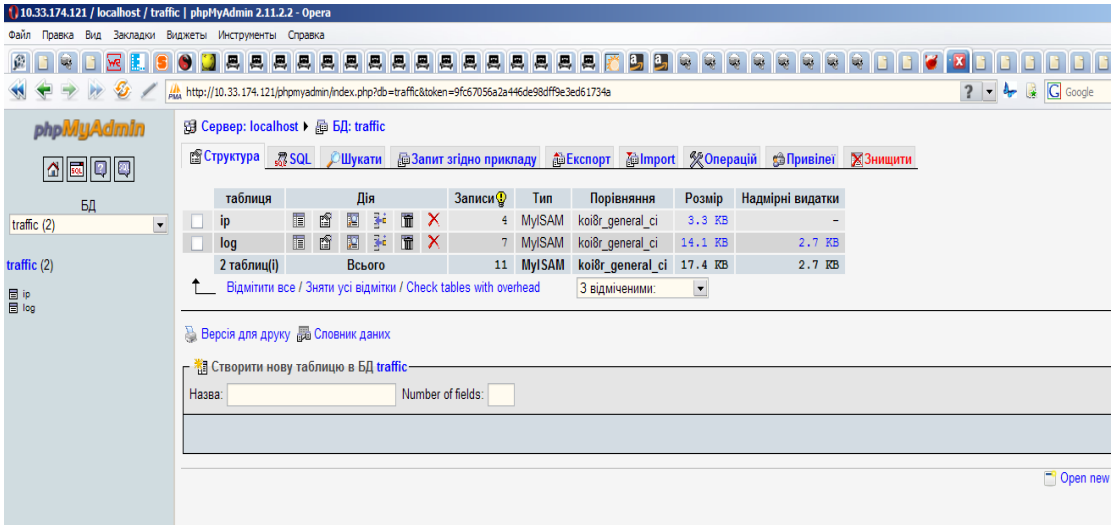


Рисунок 3.3 – Робота phpMyAdmin

Phpmyadmin користується великою популярністю у веб-розробників, тому що дозволяє управляти СУБД MySQL без безпосереднього введення SQL команд, надаючи дружній інтерфейс.

Інформацію про користувачів і ліміт для доступу в Internet можна додавати до БД через веб - інтерфейс, реалізований на HTML і PHP (рисунок 3.4).

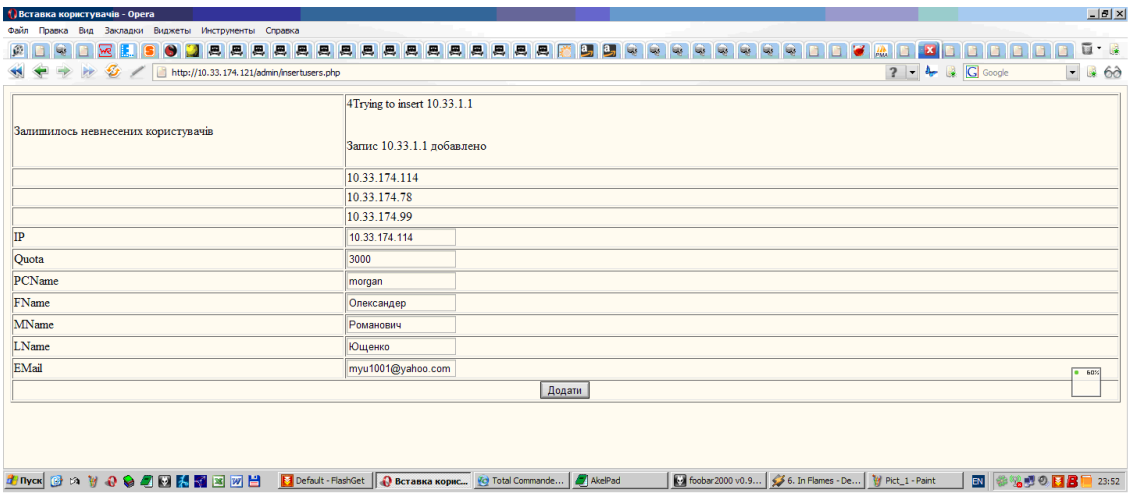


Рисунок 3.4 –Додавання користувачів у БД

IP – адреса яка не була додана у базу даних, відображаються на екрані монітора. Якщо IP – адрес не є доданий у базу даних, тоді користувач зі своєї робочої станції не зможе вийти в Internet, адже після додавання користувача у БД, система через 5 хвилин завантажує скрипт `block.php` , який перевіряє у базі даних у таблицях “IP” і “Log” IP – адреси користувачів, які є в БД, і їхній ліміт.:

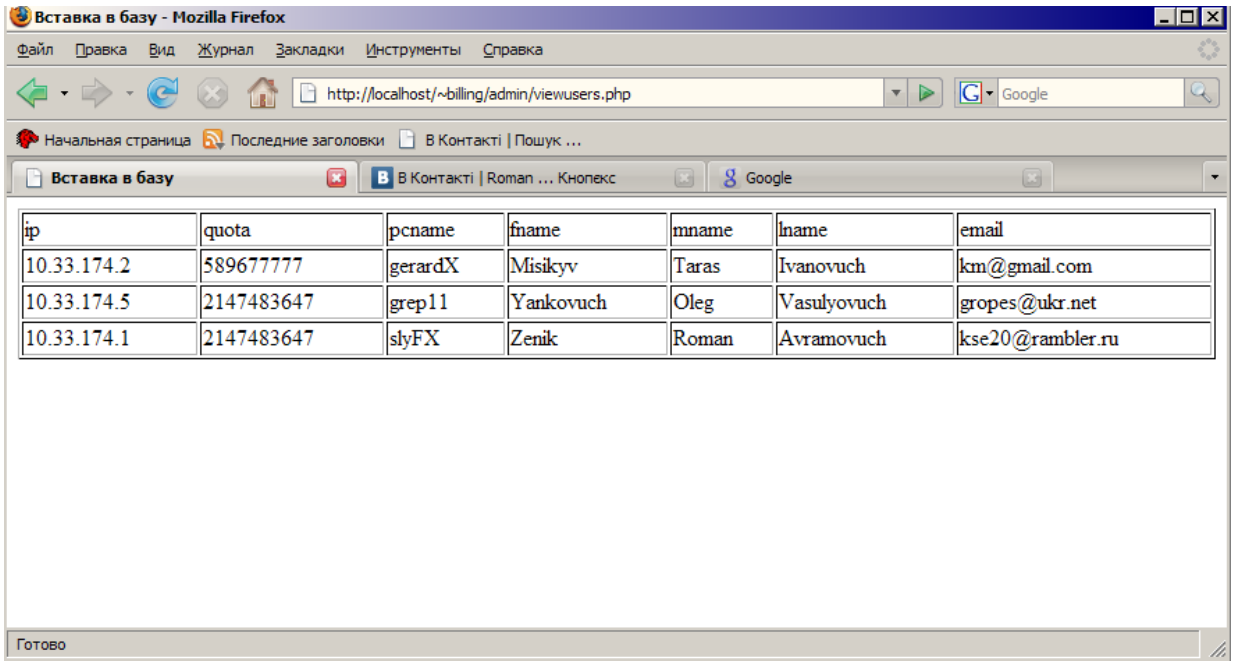
```
<?php
  include("db.php");
  $mydb = new DB('localhost', 'root', '', 'traffic');
  $mydb->open();
  $query = "SELECT  distinct log.ip_from
            FROM Log left join ip on

log.ip_from=ip.ip
            WHERE  ((select  sum(log.all_bytes)  from  log)  >
ip.quota)";
  if(!$mydb->query($query))
        {
            die($mydb->error());
        }
        else
        {
            $fl = fopen("res","w");
           system(“/sbin/ipfw table 0 flush”);

            while($result = $mydb->fetchArray())
            {
                  fprintf($fl,"$result[0]\n");
system(“/sbin/ipfw table 0 add $result[0]”);
            }
            fclose($fl);
        }
  ?>
```

Якщо користувач немає зареєстрований у БД, або він перевищив ліміт, то робота такого користувача блокується. Користувачі, які є у базі даних і їх ліміт не перевищений допускаються для користування мережею Internet, а їх IP – адрес записується у файл res, де зберігаються усі дозволені IP – адреси.

Файл res використовується для наочного відображення дозволених IP – адресів користувачів, а також додається в таблицю дозволених IP - адрес IPFW, який і дозволяє IP – адресам виходити в Internet.

Перегляд користувачів, які є у БД здійснюється за допомогою веб - інтерфейсу (рисунок 3.5), по посиланню

http://ipserver/~billing/admin/viewusers.php.



ip	quota	pcname	fname	mname	lname	email
10.33.174.2	589677777	gerardX	Misikyv	Taras	Ivanovuch	km@gmail.com
10.33.174.5	2147483647	grep11	Yankovuch	Oleg	Vasulyovuch	gropes@ukr.net
10.33.174.1	2147483647	slyFX	Zenik	Roman	Avramovuch	kse20@rambler.ru

Рисунок 3.5 – Перегляд зареєстрованих користувачів

3.2 Налаштування поштової служби

Система FreeBSD постачається з програмним пакетом для роботи з електронною поштою Sendmail, яка уже налаштована. Для запуску Sendmail потрібно зайти в конфігураційний файл rc.conf, в каталозі /etc/ і внести такі зміни:

```
sendmail_enable - "YES"
```

Після внесених змін потрібно перезапустити сервер, щоб запустився Sendmail, або запустити його вручну за допомогою команди:

```
/etc/rs/d/Sendmail start
```

Після запуску системи повідомлення можна буде відправляти будь-якому користувачу в Internet. В системі є чотири місця, які мають відношення до Sendmail :

- `/etc/mail` - конфігураційний файл Sendmail;
- `/usr/mail` - поштові скриньки користувачів;
- `/var/spool` - файли черги вхідних повідомлень;
- `/var/spool/clientmqueue` - файли черги вихідних повідомлень.

Одна з важливих переваг пакету Sendmail – це захист від спаму, шляхом встановлення правил антиретрансляції. На рисунку 3.6 показано, як відбувається ретрансляція повідомлень через SMTP сервер.

Якщо спамери і легітимні користувачі не знаходяться на S1, потрібно використовувати S1, як ретранслятор для переадресації своїх повідомлень на S2. Така конфігурація відмінно підходить для мережі підприємств, які володіють повномаштабними мережами.

Для того, щоб пошта потрапила від одного користувача до іншого, потрібно ще один процес – це завантаження пошти через поштовий протокол POP (Post Office Protocol).

Цей протокол дозволяє користувачам звертатися до своїх робочих станцій і завантажувати адресовані їм повідомлення.

Для запуску POP3, потрібно встановити пакет Qpopper з колекції портів FreeBSD: `/usr/ports/mail/qpopper` . Сервер POP3 запускаємо через `inetd`. Він слухає всі з'єднання TCP і UDP і при одержанні пакету TCP на порт 110, шукає ім'я служби в `/etc/services/`і визначає, як обробляти запит для служби цього типу, запускає процес Qpopper з `/usr/local/libexec/qpopper`.

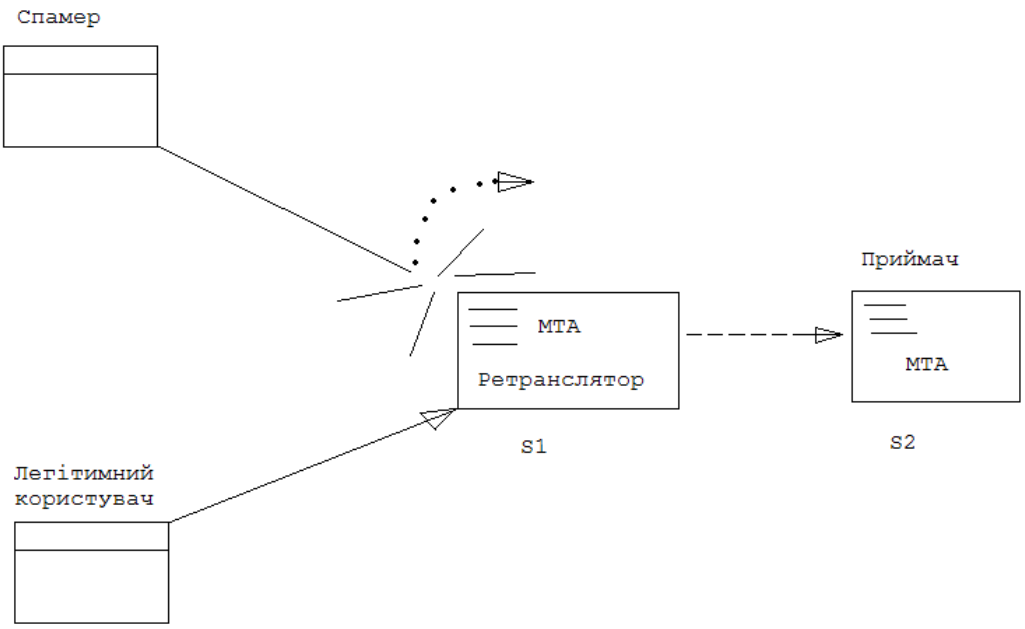


Рисунок 3.6 – Ретрансляція повідомлень

Цей процес обробляє транзакції аутентифікації користувача, блокує його поштову скриньку, визначає, які повідомлення мають бути завантаженні і обробляє їх. Якщо сервер сильно завантажений Qpopper передбачає досить багато опцій конфігурації, в більшості випадків яких потрібно для підналаштовування продуктивності сервера.

Для запуску POP3 – сервера заходимо в конфігураційний файл `inetd.conf` в каталозі `/etc/` і дописуємо :

```
pop3 stream tcp nowait root /usr/local/libexec/qpopper qpopper -s.
```

Тепер перезапускаєм `inetd`, використовуючи сценарій `/etc/rc.d/inetd:`

```
#kill -HUP inetd
#/etc/rc.d/inetd start
```

Тепер ми можемо перевірити доступність служби POP3, підключившися до порту 110 через telnet:

```
#telnet localhost 110
```

Після завершення сеансу введему команду :

```
QUIT.
```

3.3 Конфігурація WEB-сервера Apache

Конфігурація WEB-сервера Apache здійснюється у каталозі `/usr/local/etc` у конфігураційному файлі `apache`. На рисунку 3.7 представлено карту файлів конфігурації Apache, яка показує відношення конфігураційних файлів, корінь документів сервера і бінарних файлів підтримки.

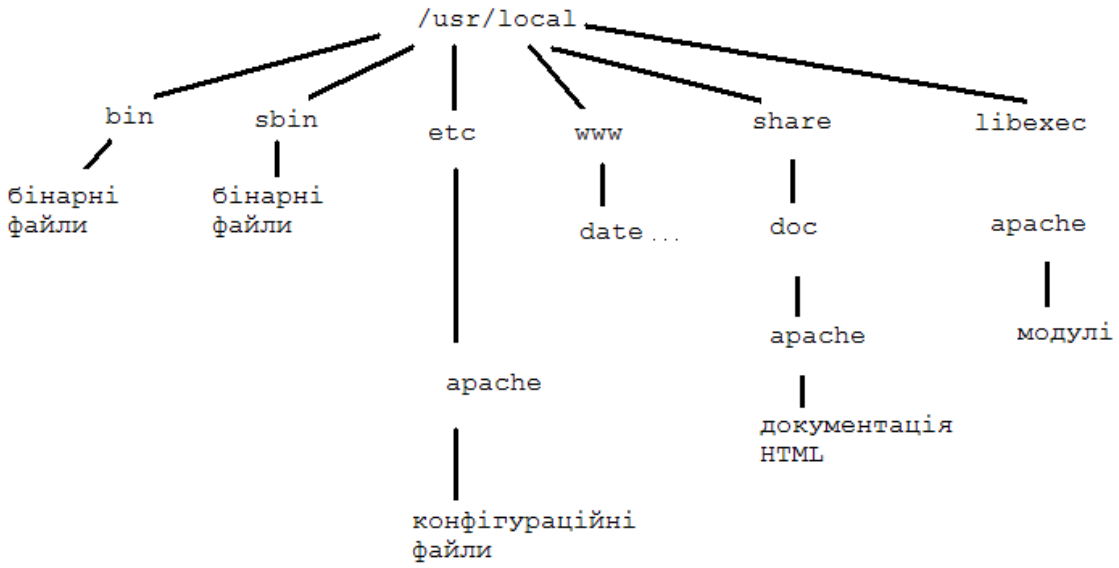


Рисунок 3.7 – Карта файлів конфігурації Apache

Налаштування сервера Apache здійснюється у конфігураційному файлі httpd.conf. Запуск, зупинку та перезавантаження сервера здійснюємо командами:

```
#apachectl start
/usr/local/sbin/apachectl start: httpd запущений

#apachectl stop
/usr/local/sbin/apachectl stop:httpd зупинений
```

Після внесення будь-яких змін у `/usr/local/etc/apache`, необхідно здійснити перезавантажити для того, щоб зміни вступили в дію.

```
#apachectl restart
```

```
/usr/local/sbin/apachectl restart:httpd    перезавантаження
```

Додавання користувачів здійснюється за допомогою команди :

```
# htpasswd –c /usr/local/www/.htpasswd viktor,
```

після чого буде видано запрошення на ввід паролю користувача, який необхідно ввести два рази.

3.4 Налаштування файлового сервера FTP

Для запису, зберігання і читання даних було вибрано файловий сервер ProFTPD. Управління сервером здійснюється через конфігураційний файл `proftpd.conf`, схожий на файл конфігурації Apache. Сервер має засоби заборони доступу, високу степінь конфігурації, встановлюється з пакетів або портів з дерикторії `/usr/ports/ftp/proftpd`. Одна різниця від подібних йому аналогів – це запуск в режимі автономного сервера.

У файлі конфігурації `proftpd.conf` вносимо наступні зміни:

```
ServerName                      "ftpslyfox"
ServerType                      standalone
DefaultServer                   on
Port                            21
Umask                           022
MaxInstances                    30

User                            knp_ux
Group                           proftpd

<Directory /*>
  AllowOverwrite                on
</Directory>
<Anonymous ~proftpd>

  User                          proftpd
  Group                         proftpd
  UserAlias                     anonymous proftpd
```

```
MaxClients                    7
DisplayLogin                  welcome.msg
DisplayFirstChdir             .message
```

Після внесених змін можна завантажувати дані з сервера. Сервер ProFTPD буде корисний при обслуговувані великих файлових архівів через мережу.

3.5 Захист мережі

Як і будь-яку іншу систему FreeBSD потрібно так само захищати від зазіхань на неї. Реалізація тієї або іншої погрози безпеки може переслідувати наступні цілі:

– порушення конфіденційності інформації. Інформація, збережена й опрацьована в корпоративній мережі, може мати більшу цінність для її власника. Її використання іншими особами завдає значної шкоди інтересам власника;

– порушення цілісності інформації. Втрата цілісності інформації - погроза близька до її розкриття. Коштовна інформація може бути втрачена або знецінена шляхом її несанкціонованого видалення або модифікації. Збиток від таких дій може бути багато більший, чим при порушенні конфіденційності;

– порушення (часткове або повне) працездатності корпоративної мережі (порушення доступу). Вивід з ладу або некоректна зміна режимів роботи компонентів КС, їхня модифікація або підміна можуть привести до одержання невірних результатів, відмові КС від потоку інформації або відмовам при обслуговуванні. Відмова від потоку інформації означає невизнання однієї із взаємодіючих сторін факту передачі або приймання повідомлень. Такі повідомлення можуть містити важливі повідомлення, замовлення, фінансові узгодження. Збиток у цьому випадку може бути досить значним;

– знищення всієї інформації на вінчестері перед відправкою в ремонт або резервне копіювання, відключення від комп'ютера, від мережі або мережі віддаленого доступу при обробці на ньому захищеної інформації, крім випадку передачі її по мережі.

Для захисту мережі було використано програмний продукт (брандмауер) IPFW, з налаштованими правилами для вхідного і вихідного потоку даних. Також було заборонено доступ фізично – це доступ до корпусів комп'ютера, установка механічних ключів.

Брандмауери дозволяють налаштувати систему для фільтрації пакетів, створеної на визначених критеріях, і заборонити небажаний трафік на рівні ядра. Брандмауери також допомагають в адмініструванні системи, підтримці статистики використовуваної у системі і спостереження за об'ємами і направленням трафіка.

Брандмауер IPFW вирішує дві важливі задачі:

– запуск його безпосередньо на комп'ютері з FreeBSD;

– використання його в якості маршрутизатора – шлюза, який захищає багато хостів всередині корпоративної мережі.

На рисунку 3.8 показано маршрутизатор-шлюз під управлінням FreeBSD з трьома мережевими адаптерами Ethernet, який передає пакети між внутрішньою мережею LAN, DMZ, WAN.

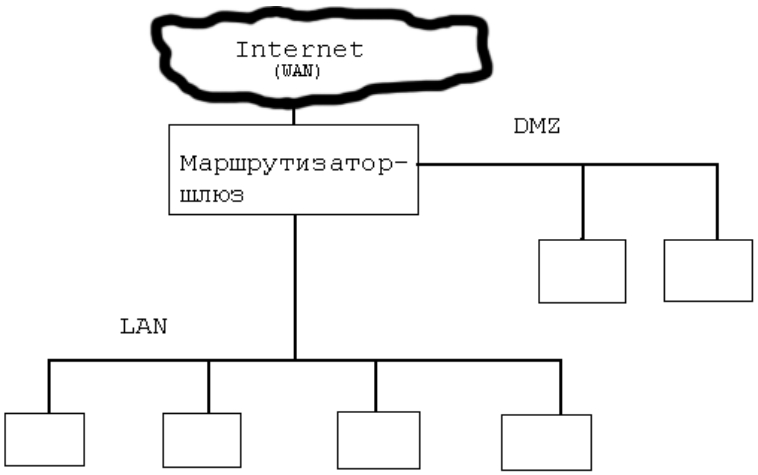


Рисунок 3.8 – Передача пакетів між LAN, DMZ, WAN

Фільтр пакетів IPFW не підтримується стандартним ядром. Треба скомпілювати визначенні опції в спеціалізоване ядро для дозволу IPFW, включаючи такі опції: `IPFIREWALL`, `IPFIREWALL_VERBOSE`, і `IPFIREWALL_VERBOSE_LIMIT=10`.

Щоб включити брандмауер потрібно добавити наступні рядки в `/etc/rc/conf` :

```
firewall_enable=”YES”
firewall_type=”open”
```

POP3 і IMAP ще більш вразливі служби відкритого тексту, ніж Telnet. Якщо користувачі налаштовують свої поштові клієнти для зв’язку з сервером кожні 5 хвилин для перевірки нових повідомлень, то при кожному такому підключенні трапляється повністю відкрита передача реєстраційної інформації і паролів, в результаті чого трапляється ще більша небезпека їх перехвату – особливо тому, що ці служби пересилають свою важливу інформацію через передбачувані регулярні інтервали.

Для того, щоб захистити ці сервіси електронної пошти використовуємо програму stunnel. Програма представляє собою альтернативний спосіб шифрування протоколів POP3 і IMAP. Stunnel централізовано керує сертифікатами SSL, також дозволяє установити універсальний тунель для будь-якої служби системи. Після запуску програми, запуститься процес-слухач на порті 993(для IMAP) і 995 (для POP3), які є зазвичай загальноприйнятими портами для захищених версій цих протоколів, які можна побачити в `/etc/services`. Для того, щоб заборонити підключення до цих портів використовуємо IPFW для заборони доступу до цих портів з будь-яких хостів, крім `localhost`.

Для моніторингу всього вхідного і вихідного трафіку, для виявлення скануючих портів, попередньої атаки хакерів використовуємо безплатний програмний пакет PortSentry. Програма прослуховує порти, які є вказані в списку. Коли програма виявляє трафік, який може вказувати на спробу

сканування порта, він блокує доступ до системи і відправляє його за маршрутом, який за замовчуванням відкидає пакети від заданого IP адреса або діапазону адресів. Всі наступні спроби підключення атакуючого хоста припиняються.

PortSentry спостерігає за трафіком TCP і UDP, динамічно будує таблицю заборонених адресів, яка працює як антитіло проти вірусу. PortSentry відразу реагує на підозрілу активність і блокує її перед тим, як вона нанесе будь-яку шкоду системі. Щоб автоматизувати систему запуску PortSentry використовуємо скрип `portsentry.sh`:

```
#!/bin/sh
PORTSENTRY=”/usr/local/bin/portsentry”
case ”$1” in
start )
${PORTSENTRY} –tcp && echo “Запуск TCP – режиму PS”
${PORTSENTRY} –udp && echo “Запуск UDP – режиму PS”
;;
Stop)
killall ‘basename ${PORTSENTRY}’
;;
*)
echo “”
echo “використання : ‘base $0 ‘ {start|stop}”
echo “”
;;
esac
```

Щоб перевірити, які порти знаходяться в режимі прослуховування, використовуємо програму `sockstat :`

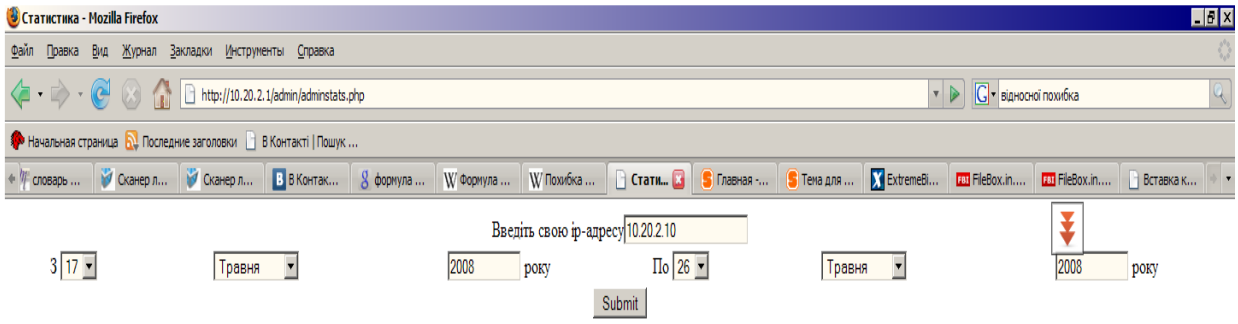
```
#sockstat
```

Кожного разу, коли PortSentry виявляє спроби атаки, він вносить хости і порти ініційовані виявлення, в списки /usr/local/etc/portsentry.blocked.tcp для атак TCP і /usr/local/etc/portsentry.blocked.udp для атак UDP [1, 3, 22, 23].

3.6 Тестування системи підрахунку трафіка

Щоб перевірити точність підрахунку трафіка, закачаємо на файлообмінний сайт http://filebox.in.ua/ контрольний файл Vicente-Feliu-Una-cancion-necesaria.mp3 розмір якого становить 1,927 Кбайт.

Після завантаження файла на сайт, нам буде згенеровано пряму ссилку для загрузки нашого контрольного файл http: // store6.filebox.in.ua /files /bpiisku5kthbst /Vicente-Feliu-Una-cancion-necesaria.mp3 для перевірки роботи білінгу завантажуємо на комп'ютер контрольний файл від імені щойно підключеного до мережі користувача , в якого сума скачаного трафіка рівна 0, як видно з рисунка 3.9, після скачування контрольного файлу розмір становить 1,994 Кбайта. Сума збільшилася приблизно на 67 Кбайт. Збільшення трафіка відбувається за рахунок команд запитів до HTTP сервера та інших сервісних пакетів.



Ваш ip	pcname	ip сайту	Адреса сайту	Вихідний порт	Порт призначення	Протокол	Загальний трафк
10.20.2.10		77.120.102.162	162.102.120.77.colo.static.dc.volia.com	clien	80	tcp	1.99 Mb
10.20.2.10		10.20.2.1	sly.iron.com	clien	80	tcp	5.85 kb
10.20.2.10		62.80.178.134	banner-134.colo.cyfra.net	clien	80	tcp	2.82 kb
Сума	10.20.2.10						1.994 Mb

Рисунок 3.9 – Результат тесту системи підрахунку IP - трафіка

При цьому відносна похибка не перевищує 0,03 %, що є допустимим для системи такого рівня. Слід враховувати, що при скачуванні файлів великих розмірів, кількість сервісних пакетів не буде зростати пропорційно до розміру файла, і відносна похибка буде ще меншою. Для тестування було використано такий програмний пакет, як броузер Mozilla Firefox, який

використовувався на користувацькій робочій станції, а також програмні пакети TRAFD, MySQL, PHP.

Для перевірки певних змін у файлі до завантаження на файлообмінний сервер і після завантаження файлу з сервера на робочу станцію було використано перевірку контрольної суми. До завантаження на сервер контрольна сума файлу становила 0109f60e8642cdf3af9d960d3b6181a5 *Vicente-Feliu-Una-cancion-necesaria.mp3. Після завантаження її на робочу станцію сума не змінилася.

Із наведеного вище тестування можна побачити, що система працює стабільно, дані передаються без втрат та зміни файлу, контрольні суми співпадають. При цьому трафік рахується з достатньою, для вирішення поставленого завдання, точністю. Крім того, розроблена білінгова система (додаток А) забезпечує :

– єдину базу даних по IT - ресурсах підприємства;

– можливість кожному користувачу мережі переглядати свою статистику користування Internet;

– підрахунок IP (TCP/UDP) – трафіка;

– ведення списку IP-адрес контролюючої мережі з кількістю байт переданої і прийнятої інформації за довільний проміжок часу;

– відключення IP - адрес від Internet згідно таблиці лімітів;

– легкість розширення системи, написання нових модулів на мові програмування PHP.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Значення охорони праці в забезпеченні безпечних умов праці

Основним завданням охорони праці є розробка і впровадження організаційних і технічних заходів, які б забезпечували попередження травмування та захворювання персоналу при високій ефективності всіх служб туристського комплексу. Туризм – одне з важливих соціально-економічних явищ сучасності, у багатьох країнах він перетворився в одну з провідних галузей економіки, став надійним джерелом поповнення бюджету. Туризм, за своїми основними характеристиками, не має принципових відмінностей від інших форм господарської діяльності. Тому всі вимоги щодо безпечної організації праці застосовуються й у даній сфері. Крім того, всі працівники, в тому числі ІТ-спеціалісти та обслуговуючий персонал туристського комплексу повинні створювати умови для безпечного та нешкідливого проживання туристів.

Ця специфіка покладає особливу відповідальність на персонал туристського комплексу не тільки особистого дотримання вимог охорони праці, а й також проведення роз'яснювальної, пропагандистської роботи серед мешканців готелів, а за необхідності - уміння надати туристам долікарську допомогу, проведення евакуаційних заходів, попереджування та ліквідації небезпечних ситуацій.

Методологічною основою охорони праці є науковий аналіз умов праці, виробничого обладнання з точки зору можливості виникнення небезпечних 1 шкідливих виробничих факторів.

4.2 Аналіз шкідливих факторів виробничого середовища

Згідно з ГОСТ 12.0.003-74 всі небезпечні й шкідливі виробничі фактори підрозділяють за способом дії: на фізичні, хімічні, біологічні й

психофізичні. Групу фізичних небезпечних і шкідливих виробничих факторів поділяють на такі підгрупи: машини й механізми, які рухаються; незахищені рухомі елементи виробничого устаткування; вироби, заготовки й матеріали, які рухаються; підвищена запиленість і загазованість повітря робочої зони; підвищена або знижена температура поверхні устаткування й матеріалів; підвищена або знижена температура, вологість, швидкість руху повітря, підвищена або знижена іонізація повітря, недостатня освітленість робочої зони та. ін. Групу хімічних небезпечних і шкідливих виробничих факторів ділять: 1) за характером дії на організм людини – на загальнотоксичні, подразнюючі, сенсибілізуючі, канцерогенні, мутагенні фактори і ті, які впливають на репродуктивну функцію; 2) за здатністю проникнення в організм людини – на фактори, які діють через органи дихання, через травну систему, через шкіру. Група біологічних небезпечних і шкідливих виробничих факторів включає біологічні об'єкти, дія яких на працюючих викликає травми або захворювання. До цієї групи належать: мікроорганізми, бактерії, віруси, рикетсії, спірохети, грибки, макроорганізми. Групу психофізичних небезпечних і шкідливих виробничих факторів за характером дії поділяють на фізичні й нервово-психічні перенапруги. Фізичні перенапруги, в свою чергу, поділяють на статичні, динамічні. Нервово-психічні перенапруги поділяють на: розумові, перенапруги аналізаторів, монотонність праці й емоційні перенавантаження. Один і той же небезпечний і шкідливий виробничий фактор за природою своєї дії може відноситися одночасно до різних груп, перерахованих вище [24].

Потенційні небезпечні та шкідливі виробничі фактори не завжди проявляють свою дію. При проведенні відповідних санітарно-технічних та інших заходів вони можуть бути максимально усунені.

Професійну або виробничу шкідливість можна розділити на три групи.

Перша група – шкідливості, які пов'язані з неправильною організацією праці (надмірна напруженість нервової системи, надмірна або однобічна

напруженість м’язового або кісткового апарата, напруга зору й слуху, тривале змушене одноманітне положення тіла, неправильний режим праці).

Друга група – шкідливості, пов’язані з особливостями виробничого процесу: а) фізичні фактори – висока або низька температура, теплове випромінювання, підвищена вологість повітря, пил, шум, вібрація; б) хімічні фактори – різні гази й шкідливі випари, отрути; в) біологічні фактори – мікроорганізми, цвілі, грибки, збудники інфекційних і інвазійних захворювань.

Третя група – шкідливості, пов’язані безпосередньо з умовами праці; недостатність вентиляції, освітлення, площі й кубатури робочих приміщень і та ін [25].

У результаті дії на організм працюючих шкідливих умов праці в них можуть розвиватися так звані професійні захворювання. Професійне захворювання – це патологічний стан організму, обумовлений негативним впливом на нього шкідливого виробничого фактора.

При виконанні роботи IT-спеціаліст туристичного комплексу піддається впливу багатьох шкідливих і небезпечних факторів. Серед яких необхідно відзначити небезпеку ураження електричним струмом, вплив різних видів випромінювання від ЕОМ та периферійних пристроїв (таблиця 2.1). Електротравма — це травма, викликана дією електричного струму або електричної луги. Електротравми поділяються на два види: електротравми, котрі виникають при проходженні струму через тіло людини, і електротравми, поява котрих не пов'язана з проходженням струму через тіло людини. Ураження людини в другому випадку пов'язується з опіками, засліпленням електричною дугою, падінням, а відтак — суттєвими механічними ушкодженнями. Існує також поняття „електротравматизм". Електротравматизм — це явище, яке характеризується сукупністю електротравм, котрі виникають та повторюються в аналогічних виробничих, побутових умовах та ситуаціях. Осередок, джерело електротравматизму — та чи інша тимчасова або навіть постійна ситуація при експлуатації

електроустановок, коли мають місце аналогічні випадки ураження людини струмом [15].

Проходячи через тіло людини, електричний струм справляє термічну, електричну та механічну (динамічну) дію. Ці фізико-хімічні процеси притаманні живій та неживій матерії. Одночасно електричний струм здійснює і біологічну дію, яка є специфічним процесом, властивим лише живій тканині. Термічна дія струму проявляється через опіки окремих ділянок тіла, нагрівання до високої температури кровоносних судин, нервів, серця, мозку та інших органів, які знаходяться на шляху струму, що викликає в них суттєві функціональні розлади. Електролітична дія струму характеризується розкладом органічної рідини, в тому числі і крові, що супроводжується значними порушеннями їх фізико-хімічного складу.

Механічна (динамічна) дія — це розшарування, розриви та інші подібні ушкодження тканин організму, в тому числі м'язової тканини, стінок кровоносних судин, судин легеневої тканини внаслідок електродинамічного ефекту, а також миттєвого вибухоподібного утворення пари від перегрітої струмом тканинної рідини та крові. Біологічна дія струму проявляється через подразнення та збудження живих тканин організму, а також через порушення внутрішніх біологічних процесів, що відбуваються в організмі і котрі тісно пов'язані з його життєвими функціями.

На наслідки ураження електричним струмом впливають певні умови та фактори. зокрема до них належать:

- сила струму;
- вид та частота струму;
- тривалість проходження струму через організм людини;
- індивідуальні властивості людини;
- шлях протікання струму через людину;
- опір тіла людини проходженню струму.

Електричний опір тіла людини — це опір струму, котрий проходить по ділянці тіла між двома електродами, прикладеними до поверхні тіла. Він

складається з опору тонких зовнішніх шарів шкіри, котрі контактують з електродами, і з опору внутрішніх тканин тіла. Найбільший опір струму чинить шкіра. На місці контакту електродів з тілом утворюється своєрідний конденсатор, однією обкладкою котрого є електрод, другою — внутрішні струмопровідні тканини, а діелектриком — зовнішній шар шкіри. Електричні властивості конденсатора характеризуються напругою, на котру він розрахований, та його ємністю. Ємність конденсатора — відношення його заряду до напруги, при котрій він може отримати даний заряд. Таким чином, опір тіла людини складається з ємнісного та активного опорів. Величина електричного опору тіла залежить від стану рогового шару шкіри, наявності на її поверхні вологи та забруднень, від місця прикладання електродів, частоти струму, величини напруги, тривалості дії струму. Ушкодження рогового шару (порізи, подряпини, волога, потовиділення) зменшують опір тіла, а відтак — збільшують небезпеку ураження. Опір тіла людини в практичних розрахунках приймається рівним 1000 Ом [20].

Визначимо небезпеку ураження людини електричним струмом для таких умов: задано питомий опір шкіри $\rho_e=10^5$ Ом·м; товщина епідермісу $d_e=0{,}8\cdot10^{-4}$ м; площа контакту струмопровідного елемента з людиною $S=5\cdot10^{-4}$ м^2; електрична постійна ε становить $8{,}85\cdot10^{-12}$ Ф/м; електрична проникність шкіри $\varepsilon_o=150$; частота струму f=50 Гц; опір внутрішніх тканин людини $R_в=600$ Ом. Відомо, що проходження електроструму через людину має місце при одночасному торканні двох фаз. Лінійна напруга електроструму становить 380 В; тривалість проходження струму через тіло людини t=0,2 с.

Небезпека проходження електричного струму через людину.

1 Активний опір шкіри:

$$R_{ША}=\frac{\rho_e d_e}{S}=\frac{10^5\cdot0{,}8\cdot10^{-4}}{5\cdot10^{-4}}=1{,}6\cdot10^4 \text{ Ом}.$$

2 Ємність зовнішнього шару шкіри:

$$C=\frac{\varepsilon\varepsilon_0 S}{d_e}=\frac{8{,}85\cdot10^{-12}\cdot150\cdot5\cdot10^{-4}}{0{,}8\cdot10^{-4}}=5{,}81\cdot10^{-9}\text{ Ф}.$$

3 Ємнісний опір шкіри:

$$R_{ШЄ} = \frac{1}{2\pi f C} = \frac{1}{2 \cdot 3{,}14 \cdot 50 \cdot 5{,}81 \cdot 10^{-9}} = 5{,}48 \cdot 10^5 \text{ Ом}.$$

4 Повний опір людини:

$$R_л = \sqrt{\frac{4R^2{}_{ША}}{1+\left(R_{ША}/R_{ШЄ}\right)^2}} + R_B = \sqrt{\frac{4 \cdot (1{,}6 \cdot 10^4)^2}{1+\left(1{,}6 \cdot 10^4 / 5{,}48 \cdot 10^5\right)^2}} + 600 = 1{,}10 \cdot 10^5 \text{ Ом}$$

.

5. Гранично допустима сила струму [12, 15, 21]:

$$I_{доп} = \frac{50}{t} = \frac{50}{0{,}2} = 250 \quad мА.$$

о

згідно закону Ома:

$$I_л = \frac{U_л}{R_л} = \frac{380}{1{,}10 \cdot 10^5} = 0{,}0038 \ \ A = 3{,}8 \ \ мА.$$

Фізіологічний вплив струму на організм людини проявляється сильним тремтінням пальців рук та судомними скороченнями м'язів рук.

Оскільки фактична сила струму не перевищує гранично допустиму $I_л < I_{доп}$, то даний струм при заданій його тривалості дії та значеннях параметрів, що характеризують шкіру людини, не є небезпечним для людини.

Таблиця 4.1

Аналіз потенційних небезпек виробничих факторів

Джерело небезпеки	**Характеристика потенційно-небезпечних факторів та їх допустимі значення**
1 ЕОМ Рентгенівське випромінювання	Діапазон – понад 1,2 кеВ, Фактичні дані – 5-10меВ/год, Гранично допустима експозиційна доза:100мкР/год.
Ультрафіолетове випромінювання	Діапазон: 280-315нм – УФ-В, Фактичні дані: 0,001 Вт/м^2 Допустима інтенсивність: 0,01 Вт/м^2 – УФ-В.
Інфрачервоний діапазон (видимий)	Діапазон: 400-700 нм., верхня межа:2,5 Вт/м^2. Фактичне значення:10000 ко/м^2
Ближнє ІЧ випромінювання	Діапазон: 700нм - 1050нм ; Верхня межа:35-70 Вт/м^2; Фактичне значення:2,5 Вт/м^2

Продовження таблиці 4.1

Джерело небезпеки	**Характеристика потенційно-небезпечних факторів та їх допустимі значення**
Дальнє ІЧ випромінювання	Діапазон: 1050нм – 1мм; Верхня межа: 35-70 Вт/м^2; Фактичне значення:4 Вт/м^2
Яскравість	Фактичні дані: 35-80кд/м^2. Допустиме значення - 40 кд/м^2
Електростатичне поле	Фактичні дані: 15 кВ/м (0 Гц) Допустима напруженість поля: 20 -60 кВ/м
2 Напруженість праці Увага: тривалість зосередження (% до тривалості зміни)	Дійсне значення 76,6 % Нормативне значення ≤75 %
3 Комп'ютерно-інформаційна система туристичного комплексу – електричний струм	Фактичні (середні) дані вимірів: напруга 220-230 В, струм 25 А, частота 50 Гц. Можливість ураження електричним струмом.
– електромагнітне поле	Діюче значення напруженості ЕМП: Е=30 А/м в діапазоні частот 50 Гц-100кГц ГДР: Ен=50 В/м в діапазоні частот 60 Гц-3МГц Н=30 А/м в діапазоні частот 50 Гц-100кГц ГДР: Нн=5 А/м в діапазоні частот 60 Гц-3МГц

4.3 Забезпечення нормальних умов праці

Визначення загальної оцінки умов праці базується на диференційованому аналізі умов праці для окремих факторів виробничого середовища і трудового процесу. До факторів виробничого середовища належать: показники мікроклімату; вміст шкідливих речовин в повітрі робочої зони; рівень шуму, вібрації, інфра- та ультразвуку, освітленості. Суттєвий вплив на стан організму працівника, його працездатність здійснює мікроклімат (метеорологічні умови) у виробничих приміщеннях, під яким розуміють клімат внутрішнього середовища цих приміщень, що визначається

діючою на організм людини сукупністю температури, вологості, руху повітря та теплового випромінювання нагрітих поверхонь. На відміну від мікроклімату житла та громадських споруд мікроклімат виробничих приміщень характеризується значною динамічністю і залежить від коливань зовнішніх метеорологічних умов, часу доби та пори року, теплофізичних особливостей технологічного процесу, умов опалення та вентиляції.

Мікроклімат виробничих приміщень, в основному, впливає на тепловий стан організму людини та її теплообмін з навколишнім середовищем.

Параметри мікроклімату справляють безпосередній вплив на самопочуття людини та його працездатність. Зниження температури за всіх інших однакових умов призводить до зростання тепловіддачі шляхом конвекції та випромінюванням і може зумовити переохолодження організму. Підвищення швидкості руху повітря погіршує самопочуття, оскільки сприяє підсиленню конвективного теплообміну та процесу тепловіддачі при випаровуванні поту.

При підвищенні температури повітря мають місце зворотні явища. Встановлено, що при температурі повітря понад 30 °С працездатність людини починає падати. За такої високої температури та вологості практично все тепло, що виділяється, віддається у навколишнє середовище при випаровуванні поту.

При підвищенні вологості піт не випаровується, а стікає краплинами з поверхні шкіри. Недостатня вологість призводить до інтенсивного випаровуваннят вологи зі слизових оболонок, їх пересихання та розтріскування, забруднення хвороботворними мікробами.

Робота користувача ПК відноситься за важкістю до легкої 1а категорії робіт. З метою створення нормальних умов для персоналу офісу встановлені наступні норми виробничого мікроклімату, згідно ДСН 3.3.6.042 - 99 "Державні санітарні норми мікроклімату виробничих приміщень", які наведені в таблиці 4.2.

Таблиця 4.2

Оптимальні та допустимі значення метеорологічних умов в робочих зонах виробничих приміщень

Назва приміщення	Категорія важкості фізичних робіт	Період року	Температура повітря, ºС		Відносна вологість повітря, %		Швидкість руху повітря, м/с	
			Оптимальна	Допустима	Оптимальна	Допустима	Оптимальна	Допустима
Лабораторія	Легка 1а	Холодний	22-24	21-25	40-60	<75	0,1	<0,1
	Легка 1а	Теплий	23-25	22-28	40-60	<65	0,1	0,1-0,2

Створення оптимальних метеорологічних умов у приміщеннях з ЕОМ є складною задачею, вирішити яку пропонується наступними заходами та засобами:

- удосконалення технологічних процесів та устаткування;
- раціональне розміщення устаткування;
- раціональна вентиляція, опалення та кондиціювання повітря;
- раціоналізація режимів праці та відпочинку;
- застосування теплоізоляції устаткування та захисних екранів;
- використання засобів індивідуального захисту.

Найважливішим засобом нормалізації повітряного середовища приміщень з ЕОМ є вентиляція – сукупність заходів та засобів, призначених для забезпечення на постійних робочих місцях та зонах обслуговування приміщень метеорологічних умов та чистоти повітряного середовища, що відповідають гігієнічним та технічним вимогам (таблиця 4.3).

Таблиця 4.3

Характеристика вентиляції приміщення

Приміщення	**Тип вентиляції (витяжна, притічна, комбінована, місцеве відсмоктування)**	**Вентиляційне обладнання (тип вентилятора, продуктивність $м^3$/год, напір, мм.вод.ст., потужність кВт)**	**Кратність повітряного обміну, 1/год**
Приміщення, де експлуатуються комп'ютери (робочий кабінет)	витяжна	Осьовий канальний вентилятор, продуктивність - 790 $м^3$/год.	2

Серед факторів зовнішнього середовища, що впливають на організм людини в процесі праці, світло займає одне з перших місць. Адже відомо, що майже 90% всієї інформації про довкілля людина одержує через органи зору. Світло впливає не лише на функцію органів зору, а й на діяльність організму в цілому. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, зростає потенційна небезпека помилкових дій і нещасних випадків. Врешті, погане освітлення може призвести до професійних захворювань, наприклад, таких як робоча міопія (короткозорість), спазм акомодації.

Для створення оптимальних умов зорової роботи в приміщенні, де експлуатуються комп'ютери дотримуються норм штучного освітлення (таблиця 4.4), що стосуються поверхонь, які розміщені на відстані 0,8 м від підлоги в горизонтальній площині. Для освітлення приміщень слід використовувати, як правило, більш економічні газорозрядні лампи типу ЛБ, які мають найвищу світловіддачу. Пропонується використовувати світильники таких класів світлорозподілу: прямого світла (П), переважно прямого (Н), переважно відбитого (В). Вибираємо світильник для люмінесцентних ламп ЛСП 02 з дифузним відбивачем для загального і місцевого освітлення.

При аварійному режимі найменша освітленість робочих поверхонь виробничих приміщень та територій підприємств, які вимагають обслуговування, має становити 5% від освітленості, що нормується для

робочого освітлення в системі загального освітлення. Евакуаційне освітлення має забезпечувати найменшу освітленість на підлозі основних проходів (чи на землі) та на сходинах сходів: в приміщеннях – 0,5 лк, на відкритих територіях - 0,2 лк (таблиця 4.4).

Таблиця 4.4

Характеристика штучної освітленості робочих місць

Назва приміщення	**Розряд зорової роботи**	**Освітленість, лк**			**Тип світильника**
		Загальне освітлення	**Аварійне освітлення**	**Евакуаційне освітлення**	
Приміщення, де експлуатуються комп'ютери (робочий кабінет)	А-2	300	15	0,5	ЛСП 02

Для забезпечення захисту і досягнення нормованих рівнів комп'ютерних випромінювань необхідно застосування приекранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

4.4 Забезпечення безпеки монтажу, пусконалагоджуючих, ремонтних робіт та експлуатації ЕОМ і комп'ютерних мереж

Монтаж, обслуговування, ремонт та налагодження ЕОМ, заміна деталей, пристроїв, блоків здійснюються тільки при повному відключенні живлення. Забороняється з'єднувати та роз'єднувати кабелі при підключеній напрузі. У тих випадках, коли монтаж, обслуговування, ремонт та налагодження ЕОМ або її пристроїв, блоків при відключеному живленні неможливі, виконання цих робіт допускається за умови додержання таких вимог:

- устаткування, допоміжна апаратура та прилади повинні бути заземлені;

- роботи виконуються не менше ніж двома працівниками;

- працівники повинні виконувати роботу інструментом з ізольованими ручками, стоячи на діелектричному килимку, або бути в діелектричних калошах.

Засоби захисту та інструмент щоразу перед застосуванням оглядають і при виявленні несправностей негайно замінюють. Користування несправними захисними засобами та інструментом є неприпустимим.

Під час виконання ремонтних робіт користуються електроінструментом, напруга живлення якого не перевищує 36 В.

Враховуючи велику щільність монтажу в пристроях ЕОМ, при їх технічному обслуговуванні забезпечуються шляхи витоку, повітряні зазори і відстані по ізоляції в ланцюгах, пошкодження ізоляції яких може призвести до ураження електричним струмом. При кожному регламентованому технічному обслуговуванні шляху витоку в ланцюгах напругою вище 42 В здійснюється очищення від пилу шляхом протирання спиртом або іншим нейтральним розчинником, а пошкоджені місця ізоляції покриваються ізоляційним лаком. При заміні елементів в цих ланцюгах витримуються повітряні зазори між струмоведучими частинами і не допускаються гострі виступи припою і виводів елементів.

При технічному обслуговуванні пристроїв ЕОМ підлягає обов'язковій перевірці справність зовнішнього підключення ЕОМ до мережі і підключених пристроїв. Проводи і кабелі не мають пошкоджень ізоляції і захисної оболонки, обривів жил у місцях приєднання. В місцях введення у вхідні пристрої проводи і кабелі закріплені так, щоб не створювати натягу струмопровідних жил. З’єднувальні пристрої, зокрема вбудовані в ЕОМ, мають справні контакти, в з’єднувальних пристроях релейно-контактного типу контактний зазор у відключеному стані є не меншим 3 мм.

Стан внутрішньої проводки в пристроях ЕОМ підлягає перевірці при регламентованому технічному обслуговуванні. Внутрішня проводка має трасування, опорне кріплення для запобігання натягу проводів і їх з'єднань,

додаткову ізоляцію або екранування для відділення проводів, що знаходяться під основною напругою, від ланцюгів малої напруги. Внутрішня проводка має ефективний захист від дотику з рухомими частинами. Жорсткі ізольовані провідники розташовуються так, щоб забезпечувати повітряні зазори і шляхи витоку, не нижче допустимих.

При регламентованому технічному обслуговуванні, обов'язковій перевірці з періодичністю не рідше 1 разу на рік, підлягають захист пристроїв ЕОМ від перевантажень по струму і виконаний на базі реле максимального струму, захист від коротких замикань.

4.5 Пожежна безпека та безпека в надзвичайних ситуаціях

Приміщення, в яких розміщені персональні комп’ютери, повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20м^2 площі приміщення з урахуванням гранично допустимих концентрацій вогнегасної рідини відповідно вимог “Правил пожежної безпеки в Україні”. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Вид та кількість первинних засобів пожежегасіння наведено у таблиці 5.5. Підходи до засобів пожежогасіння повинні бути вільними.

Забороняється:

- розміщати комп’ютерні зали у підвалах;
- проводити роботи з ремонту ПК безпосередньо в операторному залі;
- зберігати постійно в комп’ютерних залах перфокарти та перфострічки, магнітні стручки та дискети, інші носії інформації, запасні блоки та деталі (зберігатися там можуть лише носії інформації, необхідні для поточної роботи);
- залишати без нагляду ввімкнену в мережу електронну апаратуру, яка використовується для випробування та контролю ПК.

При експлуатації захисних споруд у мирний час повинна бути забезпечена цілісність:

- захисних властивостей як споруди в цілому, так і її окремих елементів (входів, аварійних виходів, захисних герметичних і герметичних дверей, пристроїв проти вибухів);
- герметизація і гідроізоляція всієї захисної споруди;
- інженерно-технічне обладнання і можливість переводу його в будь який час на експлуатацію за призначенням.

Для розміщення первинних засобів пожежогасіння у виробничих, складських, допоміжних приміщеннях, будівлях, спорудах, а також на території туристичного комплексу, як правило, слід встановлюватися спеціальні пожежні щити (стенди) [24].

Пожежні щити (стенди) встановлюються на території туристичного комплексу з розрахунку один щит (стенд) на площу 5000 $м^2$.

До комплекту засобів пожежогасіння, які розміщаються на ньому, слід включати:

- вогнегасники – 3 шт.,
- ящик з піском – 1 шт.,
- покривало з негорючого теплоізоляційного матеріалу або повсті розміром 2х2 м – 1 шт.,
- гаки – 3 шт.,
- лопати – 2 шт.,
- ломи – 2 шт.,
- сокири – 2 шт.

Ящики для піску повинні мати місткість 0,5, 1,0 або 3,0 $м^3$ та бути укомплектованими совковою лопатою.

Вмістилища для піску, що є елементом конструкції пожежного стенду, повинні бути місткістю не менше 0,1 $м^3$. Конструкція ящика (вмістилища) повинна забезпечувати зручність діставання піску та виключати попадання опадів.

Таблиця 4.5

Первинні засоби пожежегасіння

Споруда, приміщення, установа	Категорія згідно з санітарними нормами та правилами	Захищена площа, $м^2$	Первинні засоби пожежегасіння			
			Вуглекислотний вогнегасник	Хімічнопінний, вогнегасник	Пороковий вогнегасник	Волок, кішма
Приміщення, де експлуа-туються комп'ютери	Категорія Д	50	2	-	-	-

При роботі ІТ-спеціаліста туристичного комплексу важливими факторами, які окреслюють безпечні та нешкідливі умови праці є оптимальні параметри мікроклімату, освітлення, шуму, вентиляції, проте важливими є також ергономічні показники, саме їхні відповідні параметри забезпечують високу ефективність роботи операторів ПК, програмістів та інших користувачів ЕОМ. Досліджено небезпеку ураження людини електричним струмом, та запропоновано заходи щодо забезпечення електробезпеки та пожежної безпеки.

ВИСНОВКИ

Здійснена розробка комп’ютерної мережі для туристичного комплексу, яка складається з 25 робочих станцій, 1 робочої станції для системного адміністратора, 4 комутаторів, 1 сервер, яка надає наступні сервіси для користувачів:

- спільний доступ до серверів зберігання інформації;
- централізована система електронної пошти;
- VPN сервер для з’єднання з регіональним управління;
- доступ до мережі Internet;
- система підрахунку IP трафіку.

Крім того, для котеджів було розроблено безпровідну мережу на основі передачі даних радіоканалу, яка складається з двох точок доступу. Точку доступу в серверній та котеджах налаштовано на роботу в режимі WDS “точка-точка”.

Створено білінгву систему для підрахунку IP-трафіку. Розроблено програму тестування системи. Тестування комп’ютерної мережі та білінгової системи показало, що система працює стабільно, дані передаються без втрат та змін.

Точність підрахунку трафіку становить 99,97 %, що задовольняє вимогам, які були представлені підприємством.

Розроблено ряд заходів по охороні праці персоналу, які дозволять забезпечити нормальні умови праці. Досліджено небезпеку ураження людини електричним струмом, та запропоновано заходи щодо забезпечення електробезпеки та пожежної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пролетарский А. Беспроводные сети Wi-Fi [Текст]/А.В Пролетарский, И. В. Баскаков, Д. Н. Чирков. – М.: БИНОМ, 2007. – 178с.

2. Шахнович И . Современные беспроводные технологии [Текст] / И.Шахнович. – М.: Техносфера, 2006. – 288 – ISBN 5-94836-070-9.

3. Кульгин М. Компютерные сети. Практика построения. Для профессионалов. 2-е изд [Текст] / М. В.Кульгин. – СПб.: Питер, 2003. – 462с.

4. Олифер В. Компьютерные сети. Принципы, технологии, протоколы. 2-е узд [Текст] / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер-пресс, 2002. – 432с.

5. Ваш собственный сервер: установка Windows Server 2008 [Електронний ресурс] / Д. Чеканов, Режим доступу:

6. Немет Е. Руководство администратора Linux. Установка и настройка. 2-е издание [Текст] / Э. Немет, Г. Снайдер, Т. Рейн. – М.: Вільямс, 2008. – 1072с.

7. Расчет экономической эффективности в дипломных и курсовых проектах [Текст] / под общей ред. Н.Н. Фонтанина – М.: Высшая школа, 1984. – 126с.

8. Новиков Ю. Локальные сети: архитектура, алгоритмы, проектирование [Текст] / Ю. Новиков. – М.: ЭКОМ, 2000. – 412с.

9. Семенов А. Структурированные кабельные системы АйТи-СКС, издание 3-е [Текст] / А. Б. Семенов, С. К. Стрижаков, И. Р. Сунчелей. – Москва, АйТи-Пресс, 2001. – 365с.

10. Столлингс В. Современные компьютерные сети, 2-е издание. [Текст] / В. Столлингс. – Спб. Питер, 2003. – 269с.

11. Буров Є. Комп'ютерні мережі. 2-е видання [Текст] / Є. Буров– Львів: БаК, 2004.– 584с.

12. Жидецький В. Основи охорони праці [Текст] / В.Ц. Житецький, В.С.Джигирей , О.В. Мельников. – Львів.: Афіша, 2000.

13. Мюллер С. Модеризация и ремонт ПК. 11-е издание. [Текст] / М.: Вильямс, 2001. – 1184 с.

14. Основы современных комп'ютерных технологий [Текст] / под. ред. А.Д. Хомоненко. – СПб.: Корона, 1998 – 265 с.

15. Паневник Г. Охорона праці в галузі: методичні вказівки [Текст] / О.В.Паневник , Г.М. Кривенко Г.М. – Івано-Франківськ, ІФНТУНГ, 2004. – 36с.

16. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров [Текст] / Х. Остерлох. – М.: Мир, 1998. – 365 с. – ISBN 5-93772-039-3.

17. Костроми В. Самоучитель Linux для пользователя [Текст] / В.А.Костроми.– СПб.: BHV-Петербург, 2003. – 672 с.

18. Рошан П. Основы построения беспроводных локальных сетей стандарта 802.11 [Текст] / П. Рошан, Л. Джонатан. – К.: Вильямс, 2004. – 304с. – ISBN 5-8459-0701-2.

19. Гейер Дж. Беспроводные сети. Первый шаг. Пер. с англ.[Текст] / Дж.Гейер.– М.: Вильямс, 2005. – 192с.

20. Жидецький В. Основи охорони праці [Текст] / В.Ц.Жидецький – Львів: Афіша, 2004.

21. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

22. Назаров А.Н. АТМ: технология высокоскоростных сетей [Текст] / А.Н. Назаров, М.В. Симонов. – М.: Радио и связь, 1997. – 319 с.

23. Андерсон К. Локальные сети [Текст] / К. Андерсон, М. Минаси - М: Корона, 1999. - 624 с.

24. Катренко Л. Охорона праці в галузі освіти. [Текст] / Л.А.Катренко, І.П.Пістун. – Суми.: Універ.книга, 2001. – 344с.

25. ДСанПІН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.