Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Аналіз продуктивності пропускної здатності захищених каналів у мультисервісній мережі
(тема)

Виконав:

студент *2* курсу, групи *ІМІм-22-3*

Смірнов Є.А.
(прізвище, ініціали)

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва спеціальності)

Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва освітньої програми)

Керівник *доц. Харченко Н.А.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Смірнов Є.А. /

Керівник / Харченко Н.А. /

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва)

Тип програми *освітньо-наукова*

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Смірнову Євгену Андрійовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Аналіз продуктивності пропускної здатності захищених каналів у мультисервісній мережі*

затверджена наказом університету від 18 березня 2024 р. № 232 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 червня 2024 р.

3. Вихідні дані до роботи *Побудувати мультисервісну мережу готельного комплексу. Визначити інформаційну інфраструктуру готельного комплексу. Розглянути можливості побудови мультисервісної мережі з інтеграцією різнорідного трафіку на базі технології Ethernet, вибрати операційні системи та необхідне обладнання для роботи мережі. Провести аналіз забезпечення безпечної передачі даних у мережі за допомогою VPN. Провести оцінку продуктивності роботи мережі у разі використання захищених каналів.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Постановка задачі на розробку мультисервісної мережі готельного комплексу
2. Аналіз ресурсів побудови мультисервісної мережі та вибір технічного рішення
3. Розробка кампусної мультисервісної мережі готельного комплексу
4. Моделювання, продуктивність та масштабованість захищених каналів
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; логічна інфраструктура мультсервісної мережі готельного комплексу; фізична інфраструктура мультисервісної мережі першого корпусу; моделювання зон покриття точок доступу Wi-Fi; оцінка продуктивності захищеного каналу для варіанта: Windows Server 2008 із клієнтами Windows 8; оцінка продуктивності захищеного каналу для варіанта: Ubuntu з клієнтами Windows 8; пропускна здатність захищеного каналу корпоративної мережі для двох серверних ОС; завантаження центрального процесора для двох серверних ОС; розробка моделі функціонування мережі. Метод групового урахування аргументів; тестування 1С Підприємства; продуктивність технологічної платформи для Windows Server 2008+Ms SQLserver 2008; продуктивність технологічної платформи для Ubuntu + PostgreSQL, висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*18.03.24*	*виконано*
2	*Підбір літератури за темою роботи.*	*19.03-01.04.24*	*виконано*
3	*Постановка задачі на розробку мультисервісної мережі готельного комплексу*	*02.04-20.04.24*	*виконано*
4	*Аналіз ресурсів побудови мультисервісної мережі та вибір технічного рішення*	*21.04-30.05.24*	*виконано*
5	*Розробка кампусної мультисервісної мережі готельного комплексу*	*31.05-10.06.24*	*виконано*
6	*Моделювання, продуктивність та масштабованість захищених каналів*	*11.06-13.06.24*	*виконано*
7	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*14.06-18.06.24*	*виконано*

Дата видачі завдання _18_ ___березня__ 2024 р.

Студент _____
(підпис)

Керівник роботи _____ _____доц. Харченко Н.А._
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка 113 с., 20 рис., 9 табл., 23 джерела, 4 додатки.

Об'єкт дослідження – мультисервісна мережа готельного комплексу.

Мета роботи – аналіз продуктивності роботи мультисервісної мережі при використанні захищених каналів передачі даних.

Робота спрямована на розробку кампусної мультисервісної мережі з інтеграцією різнорідного трафіку на базі технології Ethernet і Wi-Fi та захистом даних за допомогою шифрування каналів VPN.

У роботі проаналізовано принципи побудови логічної й фізичної інфраструктури мультисервісної мережі готельного комплексу, існуючі операційні системи та сучасні стандарти технологій Ethernet та Wi-Fi.

Запропоновано задані інформаційні сервіси реалізувати в гетерогенній мультисервісній мережі під управлінням ОС Windows Server і Linux Ubuntu. За такого підходу логічна сегментація мережі проводиться на основі технології VLAN, а фізична сегментація за функціональною ознакою. Для захисту корпоративної частини даних буде використовуватися VPN, відповідно проаналізовано її протоколи та можливості підвищення продуктивності мережі для нівелювання впливу характеристик роботи VPN на загальну роботу мережі та обладнання.

МУЛЬТИСЕРВІСНА МЕРЕЖА, ТРАФІК, ІМІТАЦІЙНА МОДЕЛЬ, КОМУТАТОР, СЕРВЕР, СЕРВІСИ, ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, VPN, ШИФРУВАННЯ ДАНИХ.

THE ABSTRACT

Explanatory slip 113 p., 20 fig., 9 tab., 23 sources, 4 attach.

Object of research - multi-service hotel complex network.

The purpose of the work - analysis of multiservice network performance when using secure data transmission channels.

The work is aimed at the development of a campus multi-service network with the integration of heterogeneous traffic based on Ethernet and Wi-Fi technology and data protection using encryption of VPN channels.

The work analyzes the principles of building the logical and physical infrastructure of a multi-service network of a hotel complex, existing operating systems and modern standards of Ethernet and Wi-Fi technologies.

It is proposed to implement the specified information services in a heterogeneous multi-service network under the management of Windows Server and Linux Ubuntu. With this approach, the logical segmentation of the network is based on VLAN technology, and the physical segmentation is based on a functional feature. A VPN will be used to protect the corporate part of the data, and its protocols and opportunities to improve network performance will be analyzed accordingly to reduce the impact of VPN performance on the overall network and equipment performance.

MULTISERVICE NETWORK, TRAFFIC, SIMULATION MODEL, SWITCH, SERVER, SERVICES, INFORMATION INFRASTRUCTURE, VPN, DATA ENCRYPTION.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

DVR – Digital Video Recorder – цифровий контролер відеозапису;

ISDN – Integrated Services Digital Network – цифрова мережа з інтеграцією служб;

NGN – Next Generation Networks – мережа наступного покоління;

OSI – Open Systems Interconnection – моделі взаємодії відкритих систем;

PSTN – Public Switched Telephone Network – комутована телефонна мережа загального користування;

SLA – Service Level Agreement – угода про рівень надання послуги;

QoS – Quality of Service – якість надання послуг;

VLAN – Virtual Local Area Network – віртуальна мережа;

Wi-Fi – (wireless fidelity) безпровідна мережа;

WPAN – Wireless Personal Access Networks – бездротові персональні мережі доступу;

МСМ – мультисервісна мережа;

ОС – операційна система;

СКС – структурована кабельна система;

СОВС – система охоронного відео спостереження;

СОС – система охоронної сигналізації.

ВСТУП

Впровадженням інформаційних технологій у ділову стратегію підприємств готельного бізнесу, як відомо, зводиться до необхідності об'єднання різнорідних інформаційних підсистем у єдиному комунікаційному середовищі. Збільшення обсягів медійних послуг, що надаються операторами та Інтернет – провайдерами, зростання потреб клієнтів у таких послугах, а головне, постійна конкуренція в сфері готельного бізнесу, змушують власників готелів приймати рішення на побудову або модернізацію локальної комп'ютерної мережі на принципах мультисервісних технологій. За такого контексту актуальною і значущою стає задача побудови мультисервісної мережі (МСМ) з єдиним каналом для передачі звичайного трафіку (даних) і трафіку реального часу (голосу та відео).

З технічної точки зору МСМ являє собою сукупність пасивного та активного мережевого устаткування, що дозволяє ефективно організувати взаємодію кінцевих пристроїв локальної мережі між собою. В умовах необмежених обчислювальних ресурсів і пропускної здатності каналів проектування МСМ стає суто технічною задачею. Проблеми виникають у випадку деякого обмеження ресурсів. Причому ці проблеми виявляються різними для різних видів трафіку.

Вимоги щодо забезпечення необхідної якості передачі мультимедійного трафіку призвели до зміни ідеологічних основ локальних мереж, зокрема, найбільш поширених – Ethernet, а також удосконалення мережевих операційних систем (ОС), які стали забезпечувати усі сервіси, що необхідні мультимедійним мережам. Розгортання структурованих кабельних систем (СКС) на принципах мультисервісності дозволило сформувати єдину топологію та інтегроване фізичне середовище, що забезпечує роботу всіх затребуваних мультимедійних додатків.

Вплив Інтернету на корпоративні мережі сприяло появі нового поняття – Intranet, у якому способи доставки та обробки інформації, властиві Інтернет, переносяться у корпоративну мережу. Однак Інтранет є очевидною загрозою безпеці мережі підприємства, оскільки внутрішні ресурси корпоративної мережі стають доступними багатьом користувачам Інтернету, а конфіденційний

трафік може бути переглянутий зловмисником. Для забезпечення безпечного мережного з'єднання з розподіленими підрозділами компанії організується віртуальна приватна мережа (Virtual Private Networks, VPN), яка використовує набір технологій, що гарантують секретність, захист та цілісність даних, що передаються мережею загального користування. Слово "приватний" у даному контексті означає, що передача даних між віддаленими користувачами корпоративної мережі компанії здійснюється в зашифрованому вигляді, що дозволяє говорити про створення безпечного каналу зв'язку - "тунелю". Як середовище транспортування шифрованих даних використовується Інтернет.

Це рішення є оптимальним у плані фінансових витрат і дозволяє забезпечити найбільш гнучкий спосіб доступу віддалених користувачів до ресурсів корпоративної мережі .

Мета кваліфікаційної роботи – розглянути можливості побудови мультисервісної мережі готельного комплексу з інтеграцією різнорідного трафіку на базі технології Ethernet та забезпеченням безпечної передачі даних у мережі між співробітниками комплексу. Провести аналіз продуктивності мережі при запровадженні шифрованих каналів, основаних на технології VPN.

1 ПОСТАНОВКА ЗАДАЧІ НА РОЗРОБКУ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ГОТЕЛЬНОГО КОМПЛЕКСУ

1.1 Мультисервісна мережа, її визначення та характеристики

Мережа зв'язку наступного покоління (NGN) – концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями по їх управлінню і створенню нових послуг за рахунок уніфікації мережних рішень, яка припускає реалізацію універсальної транспортної мережі з розподіленою комутацією, винесення функцій надання послуг у кінцеві мережні вузли і інтеграцію з традиційними мережами зв'язку. Мультисервісна мережа – мережа зв'язку, яка побудована відповідно з концепцією мережі зв'язку наступного покоління, що забезпечує надання необмеженого набору послуг [1].

Ріст популярності мультисервісної мережі (МСМ) зв’язку – одна із самих помітних тенденцій ринку телекомунікаційних послуг в останні роки. Послуги такої мережі в першу чергу призначені для компаній, орієнтованих на інтенсивний розвиток бізнесу, оптимізацію витрат, автоматизацію бізнес-процесів, сучасні методи керування й забезпечення інформаційної безпеки. Найбільш ефективне застосування МСМ можуть знайти в традиційних телекомунікаційних операторів, які в такий спосіб значно розширюють сервіс своїх послуг. Для корпоративного ринку об’єднання всіх віддалених підрозділів у єдину МСМ на порядок збільшує оперативність обміну інформацією, забезпечуючи доступність даних у будь-який час. Завдяки можливості обміну більшими обсягами даних між офісами можна влаштовувати селекторні наради й проводити відео-конференції з віддаленими підрозділами. Все це прискорює реакцію на зміни і забезпечує оптимальне керування процесами в реальному часі [2].

Мультисервісні мережі дозволяють підтримувати такі види послуг [3]:

- телефонний і факсимільний зв'язок;
- виділені цифрові канали з постійною швидкістю передачі;
- передача відео зображень, відео конференц-зв'язок;
- телебачення;

– IP-телефонія;

– охорона, контроль доступу, облік робочого часу;

– гучномовний зв'язок;

– системи диспетчеризації;

– широкосмуговий доступ в Internet;

– сполучення віддалених ЛВС, в тому числі які працюють в різних стандартах;

– створення віртуальних корпоративних мереж, комутованих і керованих користувачем.

Застосування МСМ дає можливість одночасно використовувати зазначені вище сервіси на одній побудованій мережі передачі даних.

МСМ представляє собою універсальне багатоцільове середовище, яке призначене для передачі мови, зображень і даних з використанням технології комутації пакетів. Вона відрізняється надійністю, характерною для телефонних мереж і забезпечує низьку вартість передачі інформації. Загалом кажучи, основне завдання МСМ полягає у тому, щоб забезпечити роботу різнорідних інформаційних і телекомунікаційних систем та додатків у єдиному транспортному середовищі, коли для передачі звичайного трафіку (даних), і трафіку іншої інформації (мови, відео) використовується єдина інфраструктура. МСМ відкриває багато можливостей для побудови різноманітних накладених сервісів поверх універсального транспортного середовища – від пакетної телефонії до інтерактивного телебачення й Web-сервісів [3].

Мультисервісна мережа нового покоління має наступні особливості: універсальний характер обслуговування різних додатків; незалежність від технологій послуг зв’язку і гнучкість одержання набору, обсягу і якості послуг; повна прозорість взаємозв’язку між постачальником послуг і користувачами. Інтеграція трафіка різнорідних даних і мови дозволяє якісно підвищити ефективність інформаційної підтримки керування глобальною інформаційно-телекомунікаційною структурою, при цьому використання інтегрованого транспортного середовища знижує витрати на створення й експлуатацію мережі. МСМ, використовуючи єдиний канал для передачі даних різних типів, дає можливість зменшити різноманітність типів устаткування, застосовувати єдині стандарти й технології, централізовано управляти комунікаційним середовищем. Треба відзначити, що МСМ – це скоріше технологічна доктрина

або новий підхід до усвідомлення сьогоднішньої ролі телекомунікацій, оснований на розумінні того, що комп'ютер і нова схема представлення даних сьогодні виходять на перше місце в порівнянні з мовним зв'язком. Модель бізнес-процесу, побудована на основі широкосмугових мереж зв'язку наступного покоління, дозволяє надавати широкий набір послуг і дає гнучкі можливості створювати їх, управляти і надавати персональні послуги [1-3].

Основні відмінності таких мереж полягають у наступному:

– можливість передачі великій кількості користувачів у реальному часі дуже великих обсягів інформації з необхідною синхронізацією та з використанням складних конфігурацій з'єднань;

– інтелектуальність (керування послугою, викликом і з'єднанням з боку користувача або постачальника сервісу, роздільна тарифікація й керування умовним доступом);

– інваріантність доступу (організація доступу до послуг незалежно від технології, що використовується);

– комплексність послуги (можливість участі декількох провайдерів у наданні послуги й поділ їхньої відповідальності й доходу згідно з видом діяльності кожного).

Основні проблеми, що обмежують сьогодні поширення широкосмугового доступу, а значить, і впровадження МСМ, полягають у тім, що це вимагає значних інвестицій у галузь. Коло потенційних користувачів МСМ досить широке. Це великі холдинги, що мають територіально вилучені філії й підрозділи, це компанії, що використовують віддалені автоматичні термінали (банкомати, торговельні автомати). Це системи телемедицини й компанії мобільного зв'язку, розподілені офіси, комутаційні центри й базові станції, які також можуть підключатися до єдиної МСМ. Базовими поняттями для МСМ виступають QoS (Quality of Service – якість надання послуг) і SLA (Service Level Agreement – угода про рівень надання послуги), тобто якість обслуговування та угода про рівень надання послуг мережі.

Перехід до нових мультисервісних технологій змінює саму концепцію надання послуг, коли якість гарантується не тільки на рівні договірних угод з постачальником послуг і вимог дотримання стандартів, але й на рівні технологій і операторських мереж. Архітектурно в структурі МСМ можна виділити кілька основних рівнів: магістральний, рівень розподілу й агрегування

та рівень доступу. Магістральний рівень представляє собою універсальну високошвидкісну і, по можливості, однорідну платформу передачі інформації, реалізовану на базі цифрових телекомунікаційних каналів. Рівень розподілу включає вузлове устаткування мережі оператора, а рівень агрегування виконує завдання агрегації трафіка з рівня доступу й підключення до магістральної (транспортної) мережі. Рівень доступу включає корпоративні або внутрішньобудинкові мережі, а також канали зв'язку, що забезпечують їхнє підключення до вузла (вузлів) розподілу мережі [3].

Мультисервісні мережі можна будувати на базі самих різних технологій, як на платформі IP, концепції мереж нового покоління NGN, так і на основі виділених каналів зв'язку. При великій кількості користувачів МСМ повинна мати складну й інтелектуальну систему керування. У мережі одночасно передається велика кількість різних видів трафіка, причому для кожного з них потрібне безумовне дотримання одних параметрів, але допускаються більш-менш серйозні поступки по інших, отже, не обійтися без спеціалізованих засобів, що не допускають перевантаження мережі й порушення необхідної якості. Мережа повинна самостійно усувати перевантаження, автоматично вирішуючи, чим можна пожертвувати в різних випадках – шириною смуги пропускання, часом доставки або цілісністю інформації.

В якості системи моніторингу й керування мультисервісною мережею використовуються засоби діагностики, що представляють собою потужні інструменти, а також програмні системи OSS/BSS (Operation Support Systems/Business Support Systems). МСМ є самостійним класом мереж, що будуються на основі концепції NGN, на базі яких може бути здійснене надання широкого набору як традиційних, так і нових послуг. Визначення МСМ як самостійного класу означає, що їх регламентація повинна здійснюватися на основі нормативно-технічної бази, що враховує особливості інтеграції різних послуг і системно-технічних рішень в рамках однієї мережі [3].

1.2 Визначення інформаційної інфраструктури готельного комплексу, як об'єкта розробки проекту

Сучасний готельний комплекс являє собою розгалужену ієрархічну структуру об'єктів сфери послуг з великою кількістю схем підпорядкованості та

взаємозв'язки. Організаційно така структура, звичайно, складається зі спальних корпусів готелю, ресторану, кафе-барів швидкого обслуговування, площадок для відпочинку, розважальних центрів та іншого. Група компактно розташованих площадок, будинків (корпусів) називається кампусом. Виходячи з такого визначення вважається, що об'єкти готельного комплексу розташовані на відособленій території утворюють кампус готельних послуг. Він може функціонувати автономно або входити в об'єднання готелів на різних умовах керування [4-5].

Комплексний характер та територіально-розподілена спрямованість надаваних послуг, змушує більшість готелів автоматизувати технологічні процеси, впроваджувати різноманітні системи планування, контролю й управління ресурсами. Зокрема, інтегрувати в інформаційний простір готелю наступні системи:

- система контролю й управління доступом, Інтернет та відеоконференції;
- системи відеоспостереження та охоронної сигналізації;
- системи озвучування і сповіщення;
- система внутрішнього та зовнішнього телефонного зв’язку;
- система відеозображення ефірного та кабельного телебачення;
- внутрішня силова мережа з гарантованим електроживленням;
- система інформаційної безпеки;
- аудіовізуальний комплекс конференц-залів та концерт-холів;
- структурована кабельна система.

Комплекс організаційних структур, систем, що забезпечують функціонування й розвиток інформаційного простору організації, та засобів інформаційної взаємодії утворюють інформаційну інфраструктуру готельного підприємства [4].

В узагальненому викладі [4-5] інформаційна інфраструктура розглядається як сукупність територіально-розподілених інформаційних систем, ліній зв'язку, мереж і каналів передачі даних, засобів комутації й управління інформаційними потоками, а також організаційних структур, правових і нормативних механізмів, що забезпечують їхнє ефективне функціонування [5].

Проведений аналіз дозволяє зробити висновок, що інформаційна інфраструктура готельного комплексу, як об'єкт проектування, містить у собі рішення з апаратно-програмного та організаційного забезпечення, а також методологію й механізми їхньої взаємодії, що цілком відповідає визначенню розподіленої інформаційної системи в сучасних стандартах типу ISO.

Формування інформаційної інфраструктури проходить у два етапи:

– на першому етапі інформаційна інфраструктура створюється за національними стандартами. Зокрема, нормативні документи ДСТУ 4269:2003 «Послуги туристичні: Класифікація готелів» і ДБН В.2.2-20:2008 «Будинки й споруди. Готелі» визначають принципи побудови готельних систем та їх об’єднання в комплекси на базі структурованих кабельних систем [4-5];

– на другому етапі відбувається модернізація інформаційна інфраструктура з використанням міжнародних стандартів та переведенням її з розряду внутрішньої до розряду міжнародної інформаційної структури як осередку глобальної інфраструктури.

Формування й розвиток інформаційної інфраструктури в сучасних готелів визначається цілями і задачами бізнесу. Для готельного комплексу, що має кампусну інфраструктуру, потрібна мережа з інтеграцією сервісів, яка виконує функцію об’єднання інформаційних систем в єдиний інформаційний простір. Управління МІС є невід’ємною частиною керування готельним бізнесом, а отже складає одну з основних задач інформаційного менеджменту.

1.3 Характеристика мультисервісної мережі готельного комплексу як предмету проектування

Основу інформаційної інфраструктури готельного комплексу становить мережна інфраструктура, для якої найбільш ефективні рішення забезпечують мультисервісні мережі. Сучасні мультисервісні мережі володіють можливостями передавати по одному каналу різнорідний трафік, включаючи дані, голос та відео. Для управління різнорідним трафіком у мережі розроблено декілька груп телекомунікаційних рішень, кожна з яких вирішує власну задачу, зокрема [4]:

– розмежування трафіку за типами для передачі по окремих каналах;

– побудова декількох незалежних локальних мереж;

– передача різних типів трафіку по одній фізичній лінії;

– управління процесом передачі: перетворення одного виду трафіку в інший з наступним транспортуванням та комутацією.

Мультисервісна мережа готелю, як предмет проектування, мало чим відрізняється від офісної мережі або мережі підприємства. Зокрема, як мережа з інтеграцією сервісів, вона забезпечує передачу різнорідних даних (рис. 1.1):

– трафіку Інтернет, телефонії та мобільного зв'язку, відеоконференцій, IP-телефонії, який виконується в реальному часі, а також трафіку корпоративних мереж з використанням технології комутації пакетів (IP);

– дозволяють організувати збір телеметричної інформації, багатоканальне ефірно-кабельне телебачення, канали відеоспостереження, оповіщення та сигналізації, мережі передачі даних Ethernet, управління системою бронювання білетів, автоматами автомобільного паркування та інше.

Особливість організації кампусної моделі МСМ полягає в тому, що [3]:

– локальні мультисервісні мережі розміщаються в декількох корпусах (будинках), точки доступу на площадках і для їх об'єднання використовуються власні виділені канали зв'язку з високою пропускною здатністю;

– за наявності в структурі територіально-віддалених вузлів, об'єднання їх здійснюється за допомогою інфраструктури операторів зв'язку.

Рисунок 1.1 – Узагальнена модель кампусної мультисервісної інфраструктури

Дана модель організації дозволяє підключати до кампусної інфраструктури нові корпуси та віддалені вузли без перебудови структури

мережі. В такому випадку кампусна мережа будується за багаторівневою архітектурою, яка, зокрема, містити у собі чотири рівня ієрархії (рис. 1.2):

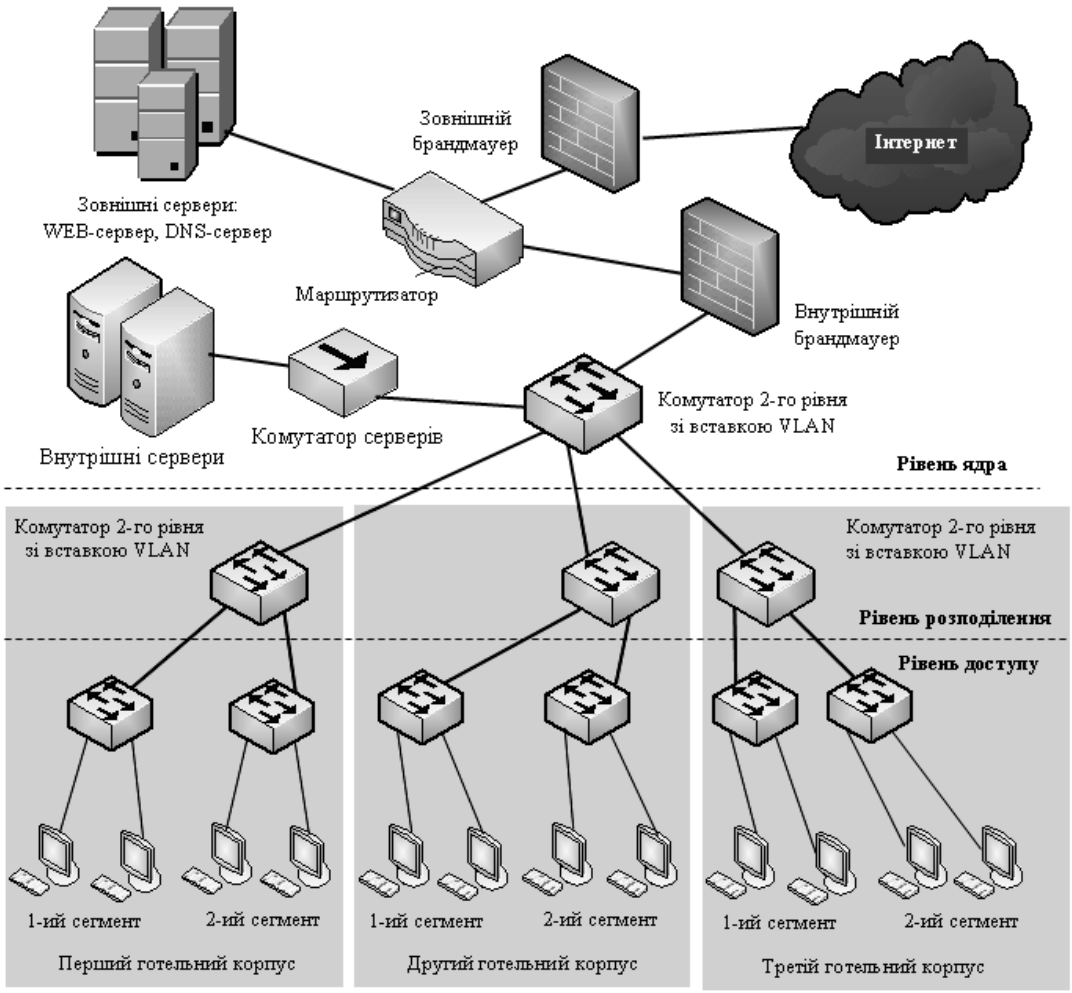

Рисунок 1.2 – Багаторівнева архітектура кампусної мультисервісної мережі

– магістральний рівень або рівень ядра мережі (Core Layer) – забезпечує максимально можливу швидкість передачі даних між частинами кампусної мультисервісної мережі, утворюючи систему магістральних каналів. Комутатори ядра працюють на другому й третьому рівнях згідно моделі взаємодії відкритих систем (OSI) [5]. З їхньою допомогою трафік з комутаторів рівня розподілення агрегується для підключення до транспортної мережі;

– рівень розподілу (Distribution Layer) – забезпечує агрегування характеристик трафіку, політику безпеки, політику доступу до інформаційних ресурсів, а також управління якістю надаваних послуг, маршрутизацію між логічними сегментами мережі, визначення мультимедійних доменів та інше.

Комутатори цього рівня працюють на третьому й четвертому рівнях моделі OSI та зв’язують комутатори рівня доступу з комутаторами рівня ядра;

– рівень доступу (Access Layer) – рівень кампусних і локальних мереж та каналів зв'язку забезпечує безпосереднє підключення користувачів до мережної інфраструктури завдяки комутаторам другого рівня моделі OSI. Дані комутатори надають користувачам порти 10/100Base-TX, утворюють віртуальні мережі (VLAN) у межах цих комутаторів. Вони можуть бути представлені як модульними пристроями, так і пристроями, що об'єднуються в стек;

– рівень серверів (Server Farm) – забезпечує підключення серверів (наприклад, серверів робочих груп) до мережної інфраструктури.

За такого підходу до опису кампусної МСМ існує можливість вибрати метод побудови мережі та устаткування, яке найбільш точно відповідає функціональним потребам мережевої структури готельного комплексу. Зокрема:

– вибрати стандартні рішення компаній-розроблювачів устаткування, Cisco, Alcatel, AVVID та інші. На стадії проектування мережі цей метод дає зниження часових і фінансових витрат, хоча загальний результат може бути дорогим, внаслідок функціональної надмірності устаткування;

– розробка власної МСМ на основі бізнес-моделі замовника. Цей метод забезпечує високу якість проекту. Часові й фінансові витрати на проектування МСМ окупаються за рахунок менших цін на устаткування. Продуктивність апаратних і програмних засобів та розподіл інформаційних потоків враховують специфіку задач мультисервісної мережі готельного комплексу.

Таким чином, перехід до класичного багаторівневого дизайну дозволяє раціонально використовувати функціональні можливості обладнання в вузлах мережі та мінімізувати витрати при її експлуатації. Зростання чисельності користувачів та необхідність одночасної передачі різних видів трафіку потребують інтелектуальної системи управління й моніторингу, яка дозволяє мережі самостійно усувати перевантаження та зберегти цілісність інформації.

1.4 Визначення мети та задачі на розробку мультисервісної мережі

Використовуючи весь потенціал сучасних інформаційних технологій, мультисервісна мережа дає можливість об’єднати територіально-рознесені

структури готельного комплексу в єдиний інфокомунікаційний простір та налагодити ефективне функціонування готельного підприємства в цілому.

Мета даної роботи – розглянути можливості побудови мультисервісної мережі з інтеграцією різнорідного трафіку на базі технології Ethernet та представити можливий варіант організації мережної інфраструктури готельного комплексу із забезпеченням захисту даних.

Загальна задача роботи полягає в реалізації зазначеної цільової установки шляхом розв’язування наступних задач:

– аналізу вихідних даних, умов існування мережної інфраструктури готельного комплексу та визначення вимог до основних параметрів МСМ;

– узагальнений огляд стандартів технології Ethernet та інтегрованих систем, аналіз логічних і фізичних ресурсів побудови мультисервісної мережі та вибір технічного рішення відносно операційної системи та якості обслуговування в мережах Ethernet;

– визначення функціонального обладнання та виконання ескізного проекту структурованої кабельної системи (СКС), як універсального фізичного середовища мультисервісної мережі готельного комплексу;

– формування пропозицій щодо безпечних умов роботи обслуговуючого персоналу, шляхом виконання вимог з електробезпеки та електромагнітного захисту, розрахунку захисного заземлення та організації робочого місця.

Таким чином, потреба в надійній передачі даних, звукової та відеоінформації призводить до розвитку МСМ, які дозволяють у рамках єдиної інформаційної інфраструктури готельного комплексу реалізувати ряд різних послуг. Вибір оптимального варіанта побудови МСМ в значній мірі визначається територіальною специфікою, пов'язаної з необхідністю об'єднати окремі структури готелю.

При організації інформаційної інфраструктури готельного комплексу важливо чітко розуміти, яких клієнтів готель обслуговує, тобто орієнтуватися на потенційного замовника. Крім того, дотримуватися операційної ефективності, тобто управляти всіма інформаційними системами готелю необхідно так, щоб вартість володіння інфраструктурою була мінімально можливою, а продуктивність – максимально ефективною.

2 АНАЛІЗ РЕСУРСІВ ПОБУДОВИ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ТА ВИБІР ТЕХНІЧНОГО РІШЕННЯ

Планування проекту гетерогенної мультисервісної мережі відбувається за умови, що структурно готельний комплекс складається з трьох типових корпусів (триповерхових будинків) та чотирьох розважальних площадок, котрі утворюють кампус з площею 1,5 гектарів. Відстань між корпусами не перевищує 70 метрів, а між розважальними площадками - 50 метрів. Всі об’єкти знаходяться у зоні прямого бачення. Характеристики кожної будівлі готельного комплексу наведені в табл. 2.1. Плани кожного поверху готельного корпусу та з розміщенням робочих місць представлені в додатку А-В.

Таблиця 2.1 – Параметри та характеристика готельних корпусів

Вихідні дані	Готельний корпус А	Готельний корпус Б	Готельний корпус В
1	2	3	4
Кількість поверхів	3	3	3
Загальна кількість номерів та на кожному поверсі	18 (9 номерів на 2 та 3 поверсі)	18 (9 номерів на 2 та 3 поверсі)	18 (9 номерів на 2 та 3 поверсі)
Кількість телевізорів у номерах	36	36	36
Приміщення адміністративні та загального доступу з розподілом номерів на першому, другому та третьому поверхах	26	26	26
	№ А1 - А20	№ Б1 - Б20	№ В1 - В20
	№ А24, А27, А29	№ Б24, Б27, Б29	№ В24, В27, В29
	№ А40, А36, А38	№ Б40, Б36, Б38	№ В40, В36, В38
Розподілення готельних номерів на другому та третьому поверхах	№ А21 - А23, А25, А26, А28, А30 - А32	№ Б21 - Б23, Б25, Б26, Б28, Б30 - Б32	№ В21 - В23, В25, В26, В28, В30 - В32
	№ А33 - А35, А37, А39, А41 - А44	№ Б33 - Б35, Б37, Б39, Б41 - Б44	№ В33 - В35, В37, В39, В41 - В44
Кількість адміністративних АРМ	14	14	14
Довжина поверху	40 метрів	40 метрів	40 метрів
Висота поверху в просвіті між перекриттями	3,5 метра	3,5 метра	3,5 метра
Загальна товщина міжповерхових перекриттів	0,20 метра	0,20 метра	0,20 метра
Товщина капітальних стін	0,60 метра	0,60 метра	0,60 метра

Продовження таблиці 2.1

Товщина внутрішніх некапітальних перегородок	0,20 метра	0,20 метра	0,20 метра
Підвісна стеля з гіпсокартону висотою вільного простору	0,30 метра	0,30 метра	0,30 метра
Матеріал внутрішньої обробки стін	гіпсокартон	гіпсокартон	гіпсокартон
В кожний будинок введено з встановленням розподільників:	50-парний кабель ТПП і 50-парний крос міської АТС	50-парний кабель ТПП і 50-парний крос міської АТС	50-парний кабель ТПП і 50-парний крос міської АТС
	кабель CATV	кабель CATV	кабель CATV
	-	багатомодовий ВОК з першого корпусу	
Зв'язок з Інтернет-провайдером	багатомодовий ВОК з пропускної здатністю 300 Мбіт/с	-	-

Окрім того, при проектуванні МСМ потрібно вибрати місця для розташування бездротових точок доступу таким чином, щоб у номерах розташовувалося не більше однієї точки доступу, а в ресторані або кафе-барі швидкого обслуговування не більше чотирьох точок доступу.

Мультисервісна мережа готельного комплексу проектується у відповідності до прийнятого в цьому підприємстві документообіг, який включає:

– програмний комплекс «1С: Підприємство 8.0. Бухгалтерський облік і Складський облік», а також 1С сумісні програми «Готель 3.30» та «1С-Рарус: Ресторан + Бар + Кафе 1.0» [2];

– авторизований, згідно з політикою інформаційної безпеки, мережний доступ до електронного документообігу та сумісна з ним 1С: Електронна пошта, доступ в Інтернет та представництво в Інтернеті, а також файловий сервіс, який забезпечує доступ до різних електронних документів.

Наряду з зазначеними сервісами потрібно організувати внутрішнє сховище мультимедійних даних та забезпечити до нього авторизований доступ співробітників готельного підприємства. Автоматизовані робочі місця (АРМ) персоналу готелю розподіляються наступним чином: директора (старший адміністратор) -1; секретаря - 1; бухгалтера - 1; адміністратора готелю - 1; касира готелю -1; портьє - 2 робочих місця; старшої покоївки -1; адміністратора

ресторану (кафе-бару) – 1; касира ресторану (кафе-бару) -1; бармена -1; офіціанта - 3 робочих місця.

Проживаючим у готелі необхідно надати можливість отримання в номерах мультисервісних послуг, що включають в себе кабельне телебачення, доступ до внутрішнього мультимедійного архіву, доступ в Інтернет. Для відображення медіа продукту застосувати телевізійні приймачі (можливо зі спеціальною приставкою) та встановити їх в номері, в холі готелю, залі ресторану та кафе-барі.

Необхідно передбачити можливість авторизованого бездротового доступу в Інтернет тим, що живуть у готелі і відвідувачам ресторану або кафе-бару. Доступ до мультимедійного сховищу для безпровідних клієнтів повинен бути закритий. Потрібно також передбачити можливість адміністрування якості надання послуг Інтернету для всіх, без винятку, користувачів.

Кабельна система готельного комплексу повинна володіти мультисервісністю, тобто забезпечувати функціонування локальної обчислювальної мережі, кабельного телебачення, телефонного мережі, системи охоронної сигналізації, охоронного відеоспостереження та системи озвучування та оповіщення будівлі.

2.1 Огляд стандартів та аналіз якості технологій передачі даних

2.1.1 Огляд стандартів і технології Ethernet (IEEE 802.3)

Технологія Ethernet в основному описується стандартами IEEE групи 802.3. Залежно від швидкості передачі даних і середовища передачі даних існує декілька варіантів технології. Разом з тим, незалежно від способу передачі стек мережного протоколу і програми працюють однаково практично у всіх варіантах. Більшість Ethernet-карт і пристроїв мають підтримку декількох швидкостей передачі даних, використовуючи авто визначення швидкості та дуплексності, для досягнення найкращого з'єднання між двома пристроями. Зокрема, наявність у пристрою порту Ethernet 10/100 свідчить про можливість працювати за технологіями 10BASE-T і 100BASE-TX, а порт Ethernet 10/100/1000 – підтримує стандарти 10BASE-T, 100BASE-TX і 1000BASE-T [6].

Таким чином, одним із самих привабливих рішень для побудови мультисервісної локальної мережі доцільно вибрати технологію гігабітного

Ethernet. Вибір технології Ethernet обумовлений її простотою, низькою вартістю, технічної зрілістю і заможністю рішень, перевірених часом.

Застосування комутації пакетів для передачі через IP-мережі різнорідного трафіка вимагає якості обслуговування (Quality of Service, QoS). Методи QoS покликані мінімізувати рівень затримок для чутливого до них трафіка; одночасно гарантувати середню швидкість і динамічну передачу пульсацій для трафіка даних. Для цього різнорідний трафік був розбитий на групи, залежно від вимог додатків його формують (табл. 2.2).

Таблиця 2.2 – Вимоги окремих додатків до якості обслуговування

Назва додатки	Надійність	Затримка	Флуктуації	Пропускна здатність
Електронна пошта	Висока	Низька	Слабкі	Низька
Передача файлів	Висока	Низька	Слабкі	Середня
WEB-доступ	Висока	Середня	Слабкі	Середня
Віддалений доступ	Висока	Середня	Середні	Низька
Аудіо за запитом	Низька	Низька	Сильні	Середня
Відео за запитом	Низька	Низька	Сильні	Висока
Телефонія	Низька	Висока	Сильні	Низька
Відеоконференції	Низька	Висока	Сильні	Висока

Як відомо, повнодуплексний Ethernet дозволяє управляти трафіком на мережному рівні. У кадр Ethernet було введено додаткове поле, що визначає класи пріоритетів. В результаті комутатори локальних мереж підтримують практично всі механізми QoS. Зокрема, комутатори локальних мереж другого рівня використовують специфікацію 802.1p, в якій є три біта додаткового заголовка CoS специфікації 802.1Q / p для зберігання пріоритету кадру [6].

Організація єдиної політики управління якістю в мережах Ethernet можлива за умови використання комутаторів третього рівня, тобто на рівні IP-протоколу.

2.1.2 Огляд стандартів і технології Wi-Fi (IEEE 802.11)

Бездротові технології дозволяють створювати локальні мережі не залежно від розташування всередині одного приміщення комутованих пристроїв. Бездротову локальну мережу, як і дротову, із зовнішньою мережею з'єднує комутатор Ethernet. Це стаціонарний пристрій підключається до бездротових точок доступу.

Організувати ж бездротову точку доступу допомагає маршрутизатор з функцією Wi-Fi доступу або безпосередньо сама точка доступу. Технологія Wi-Fi може використовуватися для мобільного розгортання локальної мережі. Різниця між точкою доступу і Wi-Fi роутером таке ж, як між роутером і комутатором [7]:

– точка доступу – аналог звичайного мережного комутатора, тобто вона просто об'єднує бездротові комп'ютери в один мережний сегмент;

– Wi-Fi роутер – це точка доступу, що включає програмно-апаратне рішення, яке дозволяє підключити вищеописаний мережний сегмент до Інтернету, налаштувати статичні і динамічні маршрути для різних сегментів підмережі, організувати фільтрацію трафіка і контроль дій користувача.

Враховуючи, що точку доступу організують на декілька каналів, то найдешевша точка доступу в 1.3 - 1.5 рази дорожче найдешевшого Wi-Fi роутера.

Комунікація в бездротовій локальній мережній зоні частотних діапазонів 2,4 ГГц; 3,6 ГГц та 5 ГГц організовується згідно набору стандарту IEEE 802.11 (відомий як Wi-Fi). До сімейства високошвидкісних стандартів бездротової технології IEEE 802.11, що опубліковані в 1999 … 2008 роках, відносяться [7]:

– IEEE 802.11a – визначає умови використання на фізичному рівні методу ортогонального частотного ущільнення (QFDM) в діапазоні частот 5 ГГц (ліцензованому в нашій країні) зі швидкістю передачі до 54 Мбіт/с;

– IEEE 802.11b – визначає умови використанням на фізичному рівні технології високошвидкісної передачі широкосмугового сигналу за методом прямої послідовності (HR-DSSS) у не ліцензованому діапазоні частот 2,402 ... 2,480 ГГц, зі швидкістю передачі до 11 Мбіт/с;

– IEEE 802.11g – визначає використання на фізичному рівні двох технологій: високошвидкісної передачі широкосмугового сигналу за методом прямої послідовності (HR-DSSS) і методу ортогонального частотного ущільнення (QFDM). Передача ведеться в не ліцензованому діапазоні частот 2,402 ... 2,480 ГГц, зі швидкостями передачі до 11 Мбіт/с і до 54 Мбіт/с відповідно;

– IEEE 802.11n – на фізичному рівні використовує метод ортогонального частотного ущільнення (QFDM), квадратурну амплітудну модуляцію (QAM) та

технологію множинного вводу/виводу (MIMO). Передача ведеться в діапазоні частот 2,402 ... 2,480 ГГц, зі швидкостями передачі до 300 Мбіт/с.

Порівняльний аналіз показує, що насьогодні стандарт IEEE 802.11n визначають найбільш прийнятну технологію для побудови бездротових мереж. Прийняте рішення відносно Wi-Fi добре підходить для організації точок доступу на території готельного комплексу, в готельних номерах та місцях загального доступу, наприклад, ресторані, кафе-барі та інших. Наявність бездротових сегментів визначають мультисервісну мережу, як мережу підвищеного комфорту.

Головні проблеми, які стоять перед механізмом реалізації заданої якості обслуговування в мережах стандарту 802.11, наступні [7]:

– напівдуплексне середовище. Стандарт 802.11 відноситься до напівдуплексного середовища, що використовується дротовими мережами Ethernet, що забезпечують високу якість обслуговування, є повнодуплексними;

– деякі канали BSS перекриваються - «перекриття по сумісним каналам». У випадках, коли два сусідніх BSS стандарту 802.11 працюють на одному і тому ж каналі, може статися інтерференція сигналів і їх згасання;

– прихований вузол. Вузли, що знаходяться в зоні дії точки доступу, але «не бачать» один одного, можуть викликати колізії і гостру конкуренцію за доступ до середовища в BSS.

2.2 Характеристика систем, що інтегровані в мультисервісну мережу

Згідно з технічним завданням кабельна система готельного комплексу повинна забезпечити розгортання мультисервісної мережі та інтеграцію системи охоронної сигналізації; системи відеоспостереження; системи озвучування та оповіщення; кабельного телебачення, телефонного зв'язку та інші додатки. Розподіл зазначених додатків по класах відбувається за табл. 2.3.

Системи охоронної сигналізації (СОС) призначені для виявлення несанкціонованого доступу на об'єкт, що охороняється. Звичайно здійснюється контроль відкриття дверей, вікон, розбиття скла, руху всередині та вздовж периметру зони, що охороняється [6].

У загальному випадку СОС складається з контролера і датчиків. Територія, що знаходиться під охороною, розбивається на окремі, не зв'язані

між собою зони. Підключення датчиків всередині зони здійснюється за технологією кільце. Спрацювання датчика здійснюється по постійному струму, незалежно від їх призначення і конструктивних особливостей, тобто їх спрацьовування полягає в замиканні (розмиканні) механічного або електронного реле. Живлення датчиків здійснюється постійним струмом напруги 12 В … 24 В.

Таблиця 2.3 – Розподіл систем, що інтегруються по класах

Найменування додатків	Клас додатків	Максимальна частота
Система охоронної сигналізації	A	100 кГц
Система відеоспостереження	C	16 МГц
Система озвучування та оповіщення	B	1 МГц
Кабельне телебачення	Fa	862 МГц
Телефонний зв'язок	A	100 кГц
Високошвидкісні мережеві додатки	E	250 МГц

Системи охоронного відеоспостереження (СОВ) є невід'ємною частиною загальної системи охорони будь-якого підприємства. Це пов'язано з їх високою інформативністю і використання людини для аналізу і прийняття рішення, що знижує ризик помилкової тривоги пов'язаної з помилковим спрацьовуванням датчика. Крім того, СОВ дозволяють вести відеозапис стану зони, що охороняється і використовувати її для подальшого аналізу. Типова система відеоспостереження (рис. 2.8) складається з монітора, чорно-білих або кольорових аналогових відеокамер і цифрового контролера відеозапису (DVR, Digital Video Recorder) [6].

Система озвучування та оповіщення складається з контролера, станції виклику, джерела фонової музики і гучномовців. Потужність та акустичні характеристики системи відповідають міжнародному стандарту IEC-60849.

2.3 Технологія шифрування даних VPN

Перед адміністраторами мережі при використанні VPN стоїть складне завдання – підготувати та розгорнути таке рішення, яке дасть можливість одночасно задовольняти потребам різних користувачів мережі підприємства. В даний час на ринку засобів організації віртуальних приватних мереж є безліч готових рішень і технологій, що частково дублюють один одного за функціональними можливостями.

Всі продукти для створення VPN можна умовно поділити на дві категорії – програмні та апаратні. Програмне рішення для VPN - як правило, готова програма, яка встановлюється на підключеному до мережі комп'ютері зі стандартною операційною системою. З міркувань захисту та продуктивності для встановлення VPN-застосунків найкраще виділяти окремі машини, які повинні встановлюватися на всіх кінцях з'єднань. Ряд виробників, таких як компанії Axent Technologies, Check Point Software Technologies та NetGuard, постачають VPN-пакети, які легко інтегруються з програмними міжмережевими екранами та працюють на різних операційних системах, включаючи Windows, Sun Solaris та Linux [16].

Для розгортання програмні рішення зазвичай складніші, ніж апаратні. Створення такої системи передбачає конфігурування сервера для розпізнавання комп'ютера та його операційної системи, VPN-пакету, мережевих плат для кожного з'єднання та спеціальних плат для прискорення операцій шифрування. Така робота складна навіть досвідчених фахівців. З іншого боку, вартість програмних рішень відносно нижча: залежно від розміру мережі можна придбати VPN-пакет за 2-25 тис. дол. (без вартості обладнання, встановлення та обслуговування).

Апаратні VPN-рішення включають все, що необхідно для з'єднання: комп'ютер, приватну (як правило) операційну систему і спеціальне програмне забезпечення. Ряд компаній, у тому числі Cisco Systems, NetScreen і Sonic, пропонують цілий спектр рішень, які можуть масштабуватися залежно від кількості одночасних VPN-з'єднань, з якими планується працювати, та очікуваного обсягу трафіку. Розгортати апаратні рішення значно простіше, на їх запуск потрібно лише кілька годин. Ще однією серйозною перевагою апаратних VPN-рішень є вища продуктивність. У них використовуються спеціальні друковані плати та операційні системи, оптимізовані під дане завдання та звільнені від необхідності підтримувати інші функції. До мінусів апаратних рішень належить їхня висока вартість. Діапазон цін – від 10 тис. дол. за пристрій для віддаленого офісу до сотень тисяч доларів за VPN для підприємства [16].

Вибір рішення залежить від розміру мережі та обсягу трафіку. Не слід забувати, що шифрування вимагає істотних обчислювальних ресурсів і може перевантажувати комп'ютер, коли кілька VPN-з'єднань одночасно беруть участь

у передачі даних. Для реалізації функції VPN у готельному комплексі оберемо варіант програмної реалізації, що буде встановлено на окремий сервер. Тож розглянемо варіанти програмних засобів VPN

2.4 Програмне VPN

Програмні засоби побудови захищених каналів VPN включають наступні варіанти:

1. Використання вільної реалізації IPSec (Internet Protocol Security). Як така можуть виступати FreeSWAN або FreeBSD IPSec.
2. Впровадження комерційного рішення. Наприклад, Cisco VPN або Securepoint VPN Server, які також базуються на IPSec.
3. Використання вільних розробок, що використовують криптографічні алгоритми власного виготовлення. Список таких програм досить великий. Тому перерахуємо тільки найвідоміші – cipe, vpnd, tinc.
4. Самостійне написання програмного забезпечення.
5. Використоання PPTP (Point to Point Tunneling Protocol).
6. Впровадження програмного пакету OpenVPN.

Розглянемо докладніше переваги та недоліки кожного з наведених вище програмних засобів VPN.

Останні кілька років при створенні VPN стандартом де-факто вважається IPSec. Така поширеність допомагає не надто перейматися сумісністю VPN-серверів і клієнтів. Єдиний стандарт – дуже зручний. Подібний спосіб хороший тим, що не вимагатиме великих матеріальних витрат і в той же час пропонує стійкий криптографічний захист даних, що передаються. Але на цьому його переваги закінчуються. Основним недоліком IPSec є те, що він некоректно працює з міжмережевими екранами, особливо якщо використовується технологія NAT. Екрани з контролем стану з'єднання (statefull firewall), що знаходяться між двома точками віртуального тунелю та керовані провайдером, можуть не пропускати ті чи інші IPSec-пакети. Про кросплатформність різних реалізацій IPSec поки що залишається тільки мріяти у зв'язку з тим, що для реалізації функцій IPSec доводиться вносити в ядро операційної системи та IP-стек досить багато змін. Як говорить старовинне прислів'я: «Надійність закінчується там, де починається складна механіка», це означає, що одна-єдина

помилка в коді, що реалізує IPSec, призведе до зниження безпеки. До того ж, на даний момент, не існує вільного клієнта, що легко настроюється. Також варто звернути увагу на велику складність встановлення та налаштування такого комплексу в порівнянні з іншими типами VPN. Ще одним із мінусів є відсутність технічної підтримки. Якщо виникнуть труднощі, то на кваліфіковану допомогу від виробника розраховувати не можна [17].

Другий спосіб підходить для тих, хто готовий вкласти більші гроші (хоча значно менші, ніж в апаратні засоби). Перевагою такого рішення є те, що буде отримано якісну технічну підтримку. Також зазвичай надається безкоштовна допомога фахівців, які самостійно або за вашими вказівками вирішать, як саме з'єднати мережі для досягнення найкращого результату. Але, вибравши рішення від одного виробника, ви будете дуже прив'язані до нього. Відповідно, якщо вибраний постачальник не реалізує ті чи інші можливості у своїй продуктовій лінійці, швидше за все, ви не зможете ними скористатися.

Третій варіант найбільше підходить для тих, кому потрібно розгорнути VPN без великих витрат часу, сил і капіталовкладень. У той же час потрібно усвідомлювати, що зазвичай подібні програми пишуть для власного використання ті, хто не зміг або не захотів розібратися з принципами роботи та методикою налаштування IPSec. Відповідно основною ідеєю розробки є зручність використання та невибагливість до ресурсів. Згодом такі програми потроху вдосконалюються, але все ж не варто очікувати від них позамежної надійності та безпеки. Відбувається це тому, що кожен автор використовує власні реалізації крипто алгоритмів. Звичайно, вони забезпечують певний ступінь захищеності, але без проведення сторонньої експертизи точно сказати, наскільки надійно працюють досить важко. Відповідно цей клас програм більше підходить для захисту каналів, якими передається інформація з малим часом життя, призначена для обмеженого поширення.

Четвертий шлях виглядає привабливим лише для фахівців у галузі криптографії, які мають велику кількість вільного часу.

Варіант рішення, заснований на PPT, переважно використовується прихильниками Microsoft. Цей стандарт реалізує досить стійке шифрування та аутентифікацію з'єднань. Створений у надрах великої Редмондської корпорації, не отримав особливого поширення у світі UNIX. Хоча вільне програмне забезпечення для роботи з ним існує і користується деяким попитом, все ж таки

рішення на основі IPSec практикують набагато частіше. Це відбувається тому, що IPSec має більш надійні процедури шифрування.

І останній варіант OpenVPN, по ціні та рівню захищеності займає золоту середину. Розглянемо більш детально можливості OpenVPN:

- офіційно OpenVPN успішно працює під управлінням таких операційних систем: Linux, Solaris, OpenBSD, FreeBSD, NetBSD, MacOS X, Windows. Це дозволяє створювати складні кросплатформні тунелі. Втім, не важко експортувати OpenVPN в будь-яку іншу систему, для якої існує драйвер tun/tap-пристроїв. До того ж ця технологія незалежна від розміру та старшинства байтів у машинному слові, що полегшує перенесення на нові операційні системи;

- компресія потоку даних і управління смугою пропускання проводяться за допомогою бібліотеки LZO. Процес стиснення є адаптивним, тобто спроби стиснути дані, що передаються, будуть здійснені, тільки якщо є сенс їх упаковувати. Ця можливість може бути легко відключена за бажанням користувача, як і будь-які інші компоненти;

- підтримуються два типи тунелів: IP та Ethernet, називаються відповідно routed і bridged. Таким чином з'являється можливість тунелювати як IP-підмережі, так і віртуальні Ethernet-адаптери;

- добре працює в мережах, де адреси розподіляються за допомогою DHCP;

- дозволяє створити тунелі поверх NAT, незважаючи на те, що NAT змінює вміст заголовків пакетів, що передаються;

- дає можливість працювати з будь-якими механізмами шифрування, вбудованими в OpenSSL для захисту трафіку, що передається. А це, у свою чергу, дозволяє кожному клієнту вибрати тип, режим роботи (CBC, CFB, OFB) та розмір ключа шифру відповідно до індивідуальних уподобань;

- у разі якщо в переданих даних є послідовності, що повторюються, для їх приховування буде використаний алгоритм explicit IV;

- кожна датаграма позначається за допомогою спеціальних ID, що створюються на основі часу відправлення та номера послідовності. Таким чином, запобігається можливість повторного відтворення зловмисником послідовності записаних пакетів;

- як додатковий захід безпеки може бути використаний протокол TLS, що дозволяє аутентифікувати сесію за допомогою динамічного обміну сертифікатами. Досить великої оптимізації швидкодії при динамічному обміні SSL/TLS-ключами дозволяє досягти використання мультипотокової бібліотеки pthread. Таким чином, навіть частий обмін між сервером і клієнтом ключами розміром більш ніж 2048 байт практично не впливає на швидкість передачі даних, що тунелюються;

- для збільшення безпеки OpenVPN дозволяє перемістити себе в chroot-оточення і знижує свої привілеї після старту так, щоб відмінно працювати від імені самого бездоганного користувача системи;

- ще однією корисною, з погляду безпеки, властивістю є наявність ключа -mlock. Він дозволяє заборонити OpenVPN записувати в процесі роботи на жорсткий диск будь-яку інформацію, пов'язану із секретними ключами та даними, що передаються тунелем;

- у зв'язку з тим, що дана програма є всього лише звичайним додатком користувача, а не частиною ядра, вона може цілком мирно співіснувати з іншими додатками, що використовують tun/tap-тунелі;

- OpenVPN створювався для тісної інтеграції з скриптами користувача та іншими високорівневими додатками, що в свою чергу дає можливість на першу вимогу легко створювати і знищувати тунелі;

- дозволяє зручно працювати через міжмережеві екрани з контролем стану з'єднання. У випадку, якщо по тунелю не передаються дані, OpenVPN дозволяє через певні проміжки часу посилати ping, щоб не дати міжмережевим екранам розірвати з'єднання через неактивність [18].

Найбільш економічним і надійним варіантом на сьогоднішній день для створення Virtual Private Networks між Windows і Unix системами оптимальним рішенням є використання OpenVPN. Тому для реалізації захищеного каналу у мережі готельного комплексу будемо використовувати OpenVPN.

3 РОЗРОБКА КАМПУСНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ГОТЕЛЬНОГО КОМПЛЕКСУ

3.1 Визначення логічної інфраструктури мультисервісної мережі

Логічна структуризація мультисервісної мережі дозволяє розбити інтегроване інформаційне середовище готельного комплексу на логічні сегменти, які представляють самостійні колективні середовища з меншою кількістю вузлів. Інструментом для такого розбиття, тобто створення логічної топології сучасних МСМ служить технологія VLAN (Virtual Local Area Network) [8].

Віртуальна локальна комп'ютерна мережа, представляє собою групу хостів з загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широкомовному домену, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. Така реорганізація здійснюється на основі програмного забезпечення замість фізичного переміщення пристроїв.

Технологія VLAN забезпечує [9]:

– гнучке розподілення пристроїв на групи. Одному VLAN відповідає одна підмережа. Пристрої, що знаходяться в різних VLAN, знаходяться в різних підмережах. Разом з тим, VLAN не прив'язана до місця розташування пристроїв і тому пристрої, що знаходяться на відстані один від одного, все одно можуть бути в одному VLAN незалежно від місця розташування;

– зменшення кількості широкомовного трафіка в мережі. Кожен VLAN представляє окремий широкомовний домен, то створення VLAN на пристрої (комутатор 2 рівня) означає розбиття комутатора на кілька широкомовних доменів. За умови знаходження одного і того же VLAN на різних комутаторах порти різних комутаторів утворюють один широкомовний домен;

– збільшення безпеки та керованості мережі. Якщо мережа розбита на VLAN, то спрощується задача застосування політик і правил безпеки. За технологією VLAN політики можна застосовувати до цілих підмереж, а не до окремого пристрою. Перехід з однієї VLAN в іншої передбачає проходження

через пристрій 3 рівня, на якому, як правило, застосовуються політики, що дозволяють або забороняють доступ з однієї VLAN до іншої VLAN.

Таким чином, розподіл мережі на логічні сегменти засобами технології VLAN підвищує продуктивність та надійність мультисервісної мережі.

Формування логічної інфраструктури МСМ відбувається на основі чинного документообігу, який існує в готельному комплексі. Аналіз заданих умов для планування мультисервісної мережі показує, що клієнтську частину МСМ, залежно від затребуваних додатків, та політики інформаційної безпеки, доцільно розбити на три логічних сегмента (рис. 3.1):

– синій сегмент – включає до себе автоматизовані робочі місця адміністрації та персоналу готельного комплексу: директора (старший адміністратор); секретаря; бухгалтера; адміністратора; касира; портьє; старшої покоївки; адміністратора ресторану (кафе-бару); касира ресторану (кафе-бару); бармена; офіціанта. Автоматизовані робочі місця, відповідно до вказівок їх виробників (компанії 1С, БІТ та АБІ-Україна) працюють під управлінням ОС Windows. Окрім функцій «АРМ» робочі станції адміністрації повинні мати доступ до сервісів мультимедіа;

– сірий сегмент – включає в себе мультимедійні робочі станції, що встановлюються в номерах, вестибюлі готелю та ресторані (кафе-барі). Вони призначені для відтворення потокового мультимедіа та виходу в Інтернет. Мультимедійні робочі станції працюють під управлінням ОС Linux Ubuntu;

– загальний сегмент – включає в себе гостьові станції безпровідного доступу, яким дозволяється вихід в Інтернет. Вони можуть працювати під управлінням будь-якої операційної системи, що використовує IP-адресацію та має в своєму складі Інтернет-браузер.

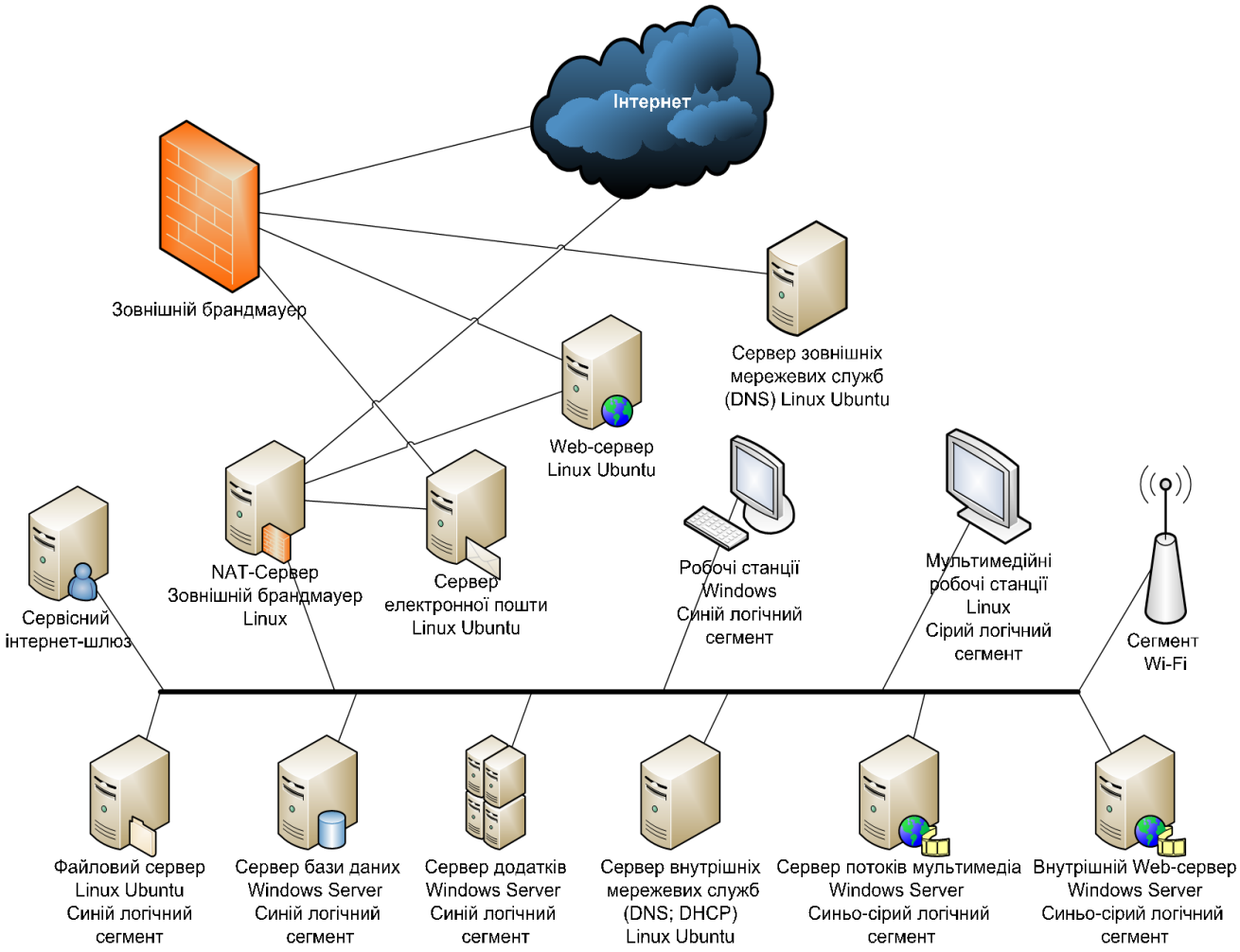

Рисунок 3.1 – Логічна інфраструктура мультисервісної мережі готельного комплексу

Розбиття інфраструктури мультисервісної кампусної мережі готельного комплексу на логічні сегменти, як показано на рис. 3.1, сприяє запобіганню можливості доступу мультимедійних та гостьових робочих станцій до мережних ресурсів, які призначені для адміністрації готельного комплексу [8].

Сервіси необхідні для забезпечення документообігу, відповідно до вказівок виробників програмного забезпечення, що використовується на готельному підприємстві, зокрема: 1С:Підприємство, БІТ: Готель та 1С-Рарус: Ресторан, реалізуються з використанням трирівневої моделі клієнт-сервер. При цьому сервер бази даних (SQL-сервер) та сервер додатків повинні працювати під управлінням ОС Windows. Зокрема, використовується ОС Windows Small Business Server 2008 Premium, яка включає до себе стандартну версію Windows Small Business Server 2008 з сервером додатків і Microsoft SQL Server. Резервна копія бази даних зберігається на файловому сервері, тут же розташовуються

файли даних готельного комплексу. Операційна система файлового сервера окремо не обговорюється, тому, з економічних міркувань вибирається ОС Linux Ubuntu з встановленим Samba-сервером. Всі перераховані вище сервери належать до синього логічного сегмента.

Сервіси потокового мультимедіа реалізовані на сервері під управлінням ОС Windows Small Business Server 2008. Доступ до мультимедійних ресурсів здійснюється через внутрішній Web-портал, який також працює на сервері під управлінням ОС Windows. Обидва сервера належать до синьо-сірому логічного сегмента.

Загальний логічний сегмент включає сервери, які забезпечують сервіси внутрішніх мережних служб – DNS і DHCP, працюють під управлінням ОС Linux Ubuntu. Сервери під управлінням ОС Linux Ubuntu реалізують функції трансляції адрес (NAT), зовнішнього брандмауера і сервісного інтернет-шлюзу, забезпечуючи аутентифікацію, авторизацію та облік доступу в Інтернет. До загального сегменту належать гостьові робочі станції, але не мають доступу до мультимедійних серверів готельного комплексу. Завдяки цьому унеможливлюється несанкціоноване завантаження файлів.

Зовнішня частина мультисервісної мережі представлена серверами електронної пошти та Web-сервером готельного комплексу та захищає їх зовнішнім брандмауером. Зазначені сервери працюють під управлінням ОС Linux Ubuntu.

У відповідності до завдання на проектування у мультисервісній мережі готельного комплексу організується одна підмережа з логічними сегментами, для адресації якої достатньо виділити групу приватних IP-адрес класу С зі стандартною маскою (наприклад, 192.168.0.0 - 192.168.0.255). Робочим станціям адреси призначаються динамічно DHCP-сервером, з призначеного діапазону всередині підмережі. Серверам призначаються фіксовані адреси з адресного діапазону підмережі, але тільки ті, що не входять в діапазон динамічного розподілу.

Організація внутрішньої доменної структури здійснюється з використанням DNS-сервера. Ім'я домену може бути будь-яке, оскільки це внутрішній домен, область дозволу адрес якої обмежена локальною (кампусною) мережею.

Зовнішні IP-адреси призначаються Інтернет-провайдером. Оскільки готельне підприємство використовує власні сервери електронної пошти та Web, адреси повинні бути фіксовані. Для організації спільного доступу в Інтернет, достатньо отримати зовнішній динамічний IP-адрес, однак на практиці підприємства користуються фіксованою адресою. Таким чином, у провайдера необхідно отримати три фіксовані Інтернет-адреси.

3.2 Визначення фізичної інфраструктури та обладнання мультисервісної мережі готельного комплексу

На основі логічної структури мультисервісної мережі формується фізична інфраструктура локальної комп'ютерної мережі. Аналіз мережних технологій, показує, що для організації кампусної мультисервісної мережі найкраще застосувати технологію Ethernet з повнодуплексним режимом обміну та зіркоподібною мережною топологією.

Для реалізації розробленої логічної структури, кампусна мультисервісна мережа розбивається на три фізичних сегмента, які функціонально збігаються з логічними сегментами (рис. 3.2), зокрема:

– сегмент «Адміністрація» – включає в себе АРМ адміністрації та персоналу готельного комплексу, що відповідає синьому логічному сегменту;

– сегмент «Телевізори» – включає в себе мультимедійні робочі станції, що встановлюються в готельних номерах, вестибюлі готелю та ресторані (кафе-барі), відповідає сірому логічному сегменту;

– сегмент Wi-Fi – включає в себе гостьові станції бездротового доступу, що відповідає загальному логічному сегменту

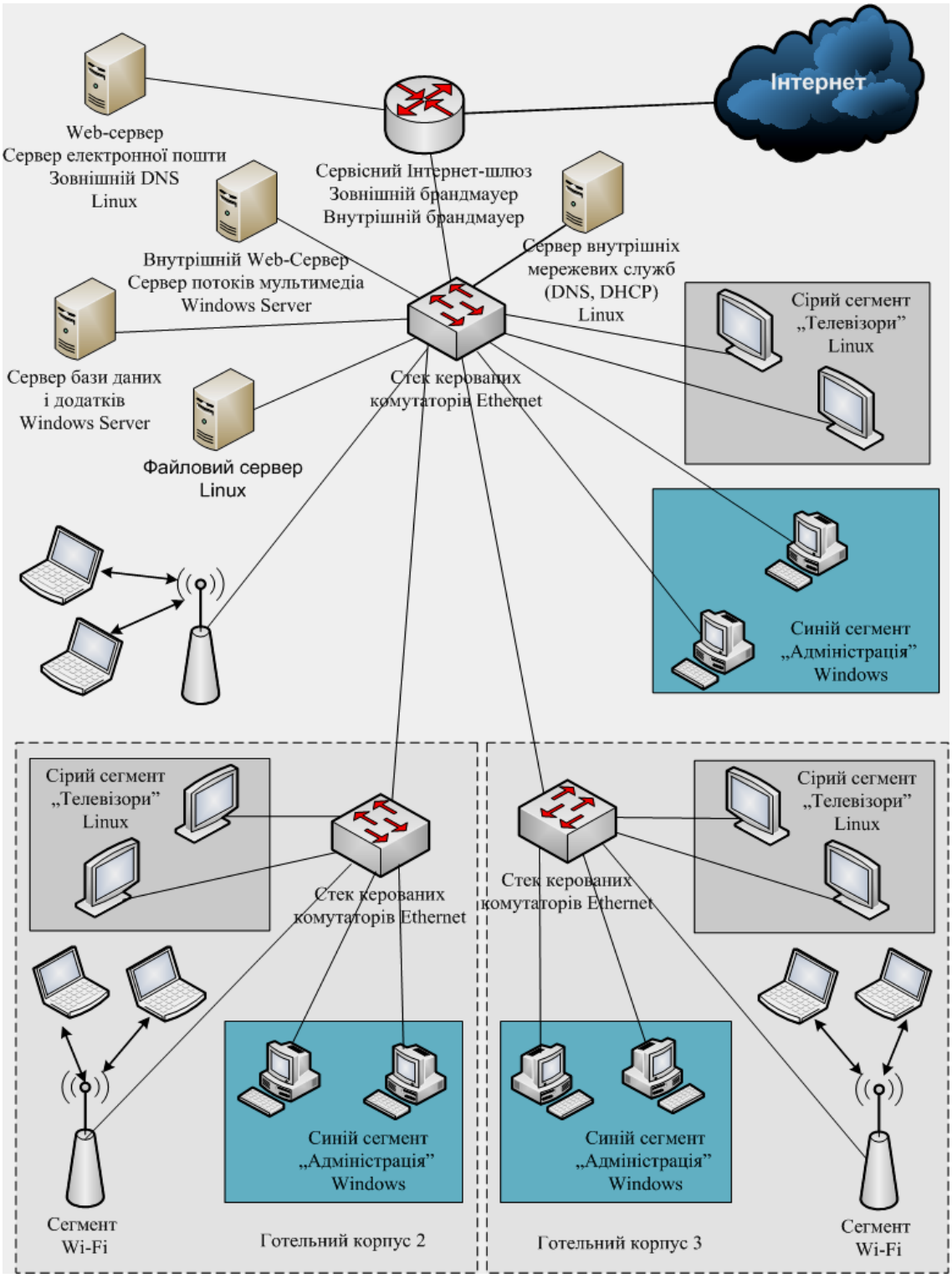

Рисунок 3.2 – Фізична інфраструктура мультисервісної мережі першого корпусу

Взаємодія між фізичними сегментами усередині кожного готельного корпусу та віддаленими сегментами другого та третього корпусів організовується за допомогою стека комутаторів 2-го рівня (рис. 3.2).

Кінцеві вузли сегмента «Адміністрація» складають робочі станції адміністрації готелю та ресторану (кафе-бара) працюють під управлінням ОС Windows, а також автоматизовані робочі місця програмного комплексу «1С: Підприємство». Оскільки робота МСМ готельного комплексу заснована на трирівневій моделі технології клієнт-сервер, то особливих вимог до продуктивності робочих станцій не пред'являється. Зокрема, можна застосувати стандартні комп'ютери на базі процесорів Intel Celeron або Pentium с інтегрованою відеокартою і мережним адаптером

Fast Ethernet. Такої конфігурації достатньо для відтворення на комп'ютерах мультимедійних файлів з файлового архіву готелю.

Робочі станції сегмента «Телевізори» встановлюються в готельних номерах холі готелю і в ресторані (кафе-барі). Станції складаються з двох компонентів:

– пристро\ відображення – телевізора з одним високочастотний вхід для підключення до мережі кабельного телебачення та декількома стандартних низькочастотних рознімань для підключення до телевізійної приставки;

– спеціальної телевізійної приставки, функція якої полягає в підключенні пристрою відображення до комп'ютерної мережі для забезпечення його роботи в інтерактивному режимі.

На вітчизняний ринок такі пристрої поставляються двома компаніями ZyXEL та D-Link. Оскільки пропозиції компанії D-Link більш переконливіші і в технічному відношенні, і ціновому плані [10-12], то вибирається цифрова телевізійна IP-приставка високого розділення DIB-120 [12]. Вона дозволяє переглядати на підключеному до неї телевізорі цифровий контент зверху будь-якої широкосмугової IP-мережі. Приставка DIB-120 підтримує відео високої роздільної здатності та відповідні кодеки (MPEG2 MP @ HL/H.264 MPEG-4 part10 MP @ L4). Це дозволяє клієнтам переглядати онлайн медіа-контент з потокового мультимедіа сервера в режимі високого розділення (HDTV) або стандартної чіткості (SDTV). Сполучення приставки з телевізором здійснюється через один зі стандартних рознімань: HDMI (відео високої роздільної здатності до 1080i та 720p); компонентне відео; S-Video та композитне відео [12].

До мультисервісної мережі приставка підключається за технологією Fast Ethernet, що забезпечує швидкість передачі даних до 100 Мбіт/с. Працює DIB-

120 під управлінням ОС Linux. Пристрій має вбудований телевізійний браузер та інтерактивне меню, що дозволяє отримати доступ, як до локальних медіа-ресурсів, так і до мережі Інтернет. Управління здійснюється за допомогою інфрачервоного пульта, що дозволяє вводити буквено-цифрові знаки.

Сегмент Wi-Fi утворюється за допомогою бездротових точок доступу і має топологію розширеної зони. Точки доступу встановлюються в готельних номерах і ресторані (кафе-барі). Результати аналізу показують, що практично усіма ноутбуками, як потенційними робочими станціями даного сегмента, підтримується стандарт IEEE 802.11g. Цей стандарт забезпечує швидкість передачі даних до 54 Мбіт/с у неліцензованому діапазоні частот 2,402 - 2,480 ГГц, а також сумісний зі стандартом IEEE 802.11b.

На вітчизняному ринку точки доступу представлені компаніями: Cisco, ZyXEL, D-Link, Planet та інші. Всі вони мають приблизно однакові технічні характеристики, але різняться за ціною, якістю продукції та рівнем сервісної підтримки [10-12]. Виходячи з критерію ціна/якість вибираються точки доступу DAP-1150 компанії D-Link [10]. Внутрішнє живлення точки бездротового доступу здійснюватися дистанційно за технологією Power over Ethernet.

В якості проміжного вузла, що з'єднує вищевказані сегменти мережі, використовується комутатор Ethernet. До такого комутатора пред'являються досить жорсткі вимоги, зокрема:

– висока пропускна здатність для забезпечення потокового трафіку HDTV до 25 Мбіт/с на один порт;

– підтримка багатоадресної розсилки та масштабованість;

– управління якістю обслуговування QoS;

– підтримка віртуальних локальних мереж (VLAN) для забезпечення логічної сегментації;

– передачу живлення за технологією Power over Ethernet (PoE);

– функції управління на основі Web-інтерфейсу.

Результати аналізу вітчизняного ринку [10-14] показали, що за критерієм ціна/якість найкращим співвідношенням володіють гігабітні комутатори серії DGS-3000, що входять в лінійку керованих комутаторів D-Link 2-го рівня. Зазначеним вимогам повністю відповідає комутатор DGS-3000-26TC, який містить: 20 портів 10/100/1000Base-T; 4 комбо-порта 10/100/1000Base-T/SFP; 2 порти 10G SFP +, що гарантує високу продуктивність при агрегації великої

кількості гігабітних з'єднань (продуктивність внутрішньої шини становить 88 Гбіт/с) [12].

Для роботи з потоковим медіа-контентом комутатор DGS-3000-26TC дозволяє використовувати Jumbo-фрейми розміром 12Кб, це означає, що накладні витрати на службові поля кадру Ethernet складуть приблизно 0,38%. Дійсно, враховуючи, що розмір службових полів кадру Ethernet 64 байта, то добуток даного параметра і параметра Jumbo-фрейму становить 0,000384. Очевидно, що для забезпечення одного потокового трафіку HDTV в 25 Мбіт/с необхідно передавати Ethernet-кадри зі швидкістю 26,75 Мбіт/с. Для передачі потокового відео 96 клієнтам потрібно, щоб продуктивність внутрішньої шини комутатора складала 2568Мбіт/с, тобто завантаженість її 0,35 % від можливої.

Підключення мультимедійного сервера до комутатора здійснюється через один з портів 10G. Необхідна швидкість на цьому порту, як було показано вище, становить 2568Мбіт/с або приблизно 4 % від його продуктивності. При критичному значенні (70 – 80) % цілком допустимий параметр, оскільки існує більш ніж 76% запас. Це найгірший прогноз, оскільки і комутатор, і мультимедійний сервер підтримують QoS/CoS, тобто забезпечують протокол 802.11p на канальному рівні, а багатоадресну розсилку та QoS на мережному. Таким чином, комутатори при обміні даними між собою та з клієнтами мережі будуть підтримувати систему управління якістю обслуговування.

Значна увага до потокового мультимедіа пов’язана з високими вимогами до швидкості передачі даних додатком, оскільки швидкість роботи мобільних абонентів обмежена технічним завданням і становить не більше 1 Мбіт/с, а АРМ 1С: Підприємства працюють як «тонкі клієнти» не споживають мережевих ресурсів. Вибраний тип комутатора DGS-3000-26TC підтримує протокол 802.1Q (VLAN) і дозволяє організувати до 4094 логічних сегментів.

Проведені розрахунки дозволяють визначити необхідну кількісті комутаторів 2-го рівня фізичної інфраструктури мультисервісної мережі. Згідно завдання на кваліфікаційну роботу фізичні сегменти кожного готельного корпусу об’єднують 74 робочих станцій або точок доступу (табл.3.1). Враховуючи, що комутатор DGS-3000-26TC містять 20 портів 10/100/1000Base-T та 2 порти SFP, нескладно підрахувати, що 4 комутатори (82 порти) дозволяють підключити 82 робочих станцій. Для забезпечення високої

керованості та масштабування 4 комутатори DGS-3000-26TC об'єднуються в стек за допомогою портів 10G SFP+.

Таблиця 3.1 – Кількість робочих станцій та розподілення їх по комутаторам

Найменування сегмента	Перший поверх		Другий поверх		Третій поверх		Кіл-сть робочих станцій (точок доступу)
	Кіль-кість	Номер комутатора в стеку	Кіль-кість	Номер комута-тора в стеку	Кіль-кість	Номер комута-тора в стеку	
Адміністрація	12	2	1	2	1	2	14
Телевізори	2	3	18	3	18	4	38
Wi-Fi	2	1	9	1	9	1	22
Віддалені сегменти							2
Усього:							74

Відповідно з територіальним та функціональним призначенням робочих станцій відбувається розподіл їх за комутаторами. Функціональна схема підключень для одного готельного корпусу представлена на рис. 3.3. За такої схеми для забезпечення необхідної швидкості потоку, підключення мультимедійного сервера здійснюється мережною картою 10G.

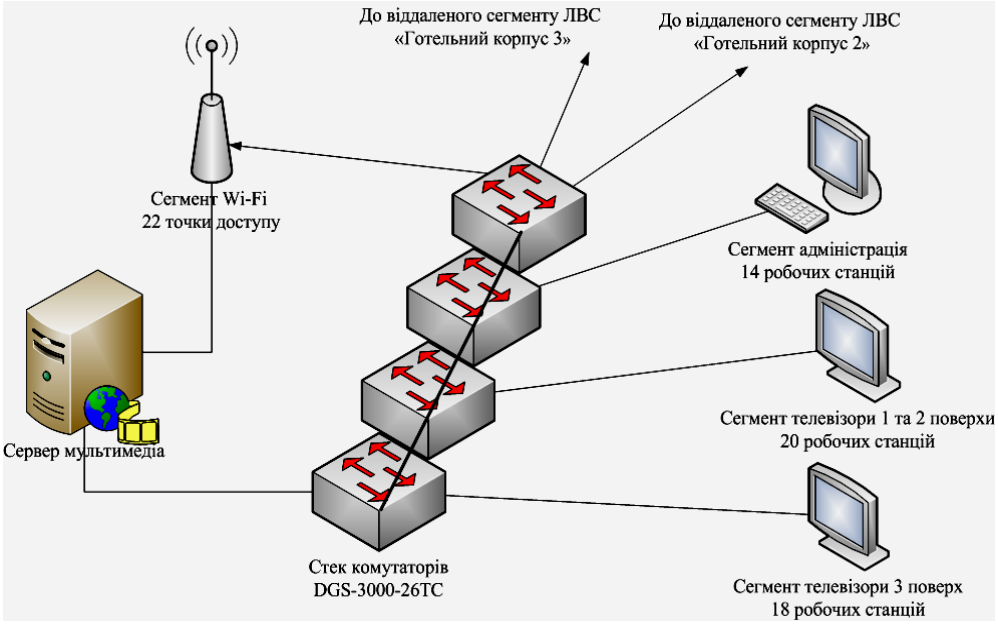

Рисунок 3.3 – Схема підключень робочих станцій та сервера до стека комутаторів

Підключення мережі готельного комплексу до Інтернет в тому числі і до її зовнішньої частини, яка реалізована на сервері під управлінням ОС Linux, здійснюється на базі модульного маршрутизатора Cisco 1721, який належить до серії Cisco 1700. Маршрутизатори серії Cisco 1700 забезпечують повне рішення для передачі мультимедійного трафіку в єдиній мережі, усуваючи необхідність установки декількох пристроїв [14].

Маршрутизатор Cisco 1721 володіє широкими можливостями WAN доступу, високоефективний роутинг, QoS, роутинг для віртуальних мереж, і доступ VPN з варіантами брандмауера. Базуючись на IOS Cisco, даний маршрутизатор пропонує високу надійність і гнучкість взаємозамінних WAN інтерфейсних карт, всебічну безпеку, яка включає апаратне шифрування VPN і брандмауер, а також DSL з розширеним QoS гарантує високу ефективність роботи.

Модульний маршрутизатори Cisco 1700 містить слоти WIC (WAN Interface Card) для установки різних модулів сполучення з територіально розподіленими мережами передачі даних в їх числі в оптичний модуль, слоти VIC (Voice Interface Card) для інтеграції з телефонними мережами і слоти WIC/VIC, що підтримують обидва види модулів. Потужний RISC-процесор, гнучка модульна конструкція і вбудований порт Fast Ethernet 10/100, визначають придатність пристрою Cisco 1721 в якості основи для побудови віртуальних приватних мультисервісних мереж, що дозволяє мінімізувати витрати на установку, настройку та підтримку мережі.

3.3 Вибір серверного обладнання

Багато інформаційні сервіси, що були описані при виборі логічної інфраструктури у вигляді окремих серверів, фізично реалізуються на комп'ютерах, що виконують комбіновані серверні функції:

– файловий сервер, сервер бази даних і додатків;

– сервер потоків мультимедіа та внутрішній Web-сервер;

– сервер внутрішніх мережевих служб (DNS-сервер і DHCP-сервер);

– Web-сервер, сервер електронної пошти, зовнішній DNS-сервер і зовнішній брандмауер.

Вибір сервера бази даних і додатків виконується за рекомендаціями

виробника програмного комплексу 1С: Підприємства, компанії 1С [15]:

– 32 розрядний сервер додатків – процесор не нижче Pentium III 866 МГц (доцільно Pentium IV або подібний процесор з частотою 2,0 ГГц та вище);

– сервер баз даних – будь-який комп'ютер, на якому може працювати Microsoft SQL Server.

Вимоги до решти серверів – файлового, внутрішніх мережних служб, зовнішнього «сумісного» – мінімальні. Оскільки, виходячи із кількості обслуговуваних ними станцій (для Web-сервера, це передбачувана кількість зовнішніх запитів), і даних виробників серверного програмного забезпечення сервери можуть мати мінімально допустиму конфігурацію [15].

Найбільш жорсткі вимоги пред'являються до продуктивності мультимедійного сервера, особливо до швидкості роботи його дискової підсистеми і розміру оперативної пам'яті. У найгіршому випадку, коли клієнти звертаються до різних мультимедійних файлів, швидкість передачі даних по мережі (за системних втрат) не повинна перевищувати 70% - 75% продуктивності дискової підсистеми .

У мультисервісній мережі максимально можлива кількість медіа-клієнтів (по числу портів комутаторів) дорівнює 82, отже, максимально можливий потік складе 2050 Мбіт/с, тобто 256 Мб/с. Для забезпечення безперебійності мережного потоку рекомендується на кожного клієнта виділяти обсяг буферної пам'яті не менше ніж на 5 секунд відтворення, що потребує приблизно 16 Мб оперативної пам'яті. Відповідно, загальний обсяг буферної пам'яті складе 1318 Мб

Ринок серверів досить різноманітний, однак лідируюче положення займає компанія Hewlett Packard Invent. Їх лінійку серверів HP ProLiant, що призначена для підприємств середнього розміру, зокрема, сервер ML115-G5 можна вибрати, як типовий сервер, що забезпечить всі необхідні сервіси [16].

У типовій конфігурації HP ProLiant ML115-G5 використовується як сервер внутрішніх мережних служб і зовнішній «суміщений» сервер. Для використання сервера в якості файлового сервера, в типову конфігурацію необхідно додати два жорсткі диски ємністю 500 Гб (вибір зроблено з міркувань ціни і надійності) і конфігурувати дискову підсистему як RAID 1 рівня. Використання сервера як мультимедійного, вимагає більш значної зміни конфігурації, зокрема [17]:

– виходячи з наведених розрахунків та враховуючи мінімальні системні вимоги, ємність оперативної пам'яті слід збільшити до 2 Гб модулями по 1Гб, виключивши встановлені у типовій конфігурації 2 модуля по 256 Мб;

– виключити зі складу сервера з жорсткими дисками ємністю 160 Мб і швидкістю обертання 7200 об/хв. Натомість встановити чотири жорсткі диски ємністю 1 Тб кожен, зі швидкістю обертання 15000 об/хв. Конфігурувати встановлені накопичувачі як RAID 10 рівня, що дає практично подвійне збільшення швидкості передачі даних (до 300 Мб/с) та збільшення надійності дискової підсистеми;

– додати, відповідно з функціональною схемою підключення сервера до стека комутаторів (рис. 3.3), одну серверну мережеву карту 10G.

Обладнання, що залишиться після доопрацювання мультимедійного сервера, доцільно використовувати для підвищення параметрів сервера бази даних. Зокрема: об'єм оперативної пам'яті збільшити до 1 Гб, додавши модулі по 256 Мб; встановити додатковий жорсткий диск ємністю 160 Гб; конфігурувати дискову підсистему, як RAID першого рівня.

3.4 Моделювання типових сегментів мультисервісної мережі

3.4.1 Моделювання зон покриття точок доступу Wi-Fi

Визначення необхідної кількості точок бездротового доступу Wi-Fi та місць розміщення їх в приміщеннях відповідного готельного комплексу вимагає попереднього моделювання зони покриття. Моделювання бездротових WLAN-мереж з застосуванням стандарту IEEE 802.11a/b/g проводиться у програмному середовищі InterpretAir виробництва компанії Fluke Networks (США). В ході дослідження програмне забезпечення InterpretAir забезпечує візуалізацію показників стану радіо ефіру, що значно спрощує аналіз бездротового середовища та дозволяє робити настроювання продуктивності мережі.

У інструментальному середовищі програми InterpretAir створюється план приміщення, і на ньому віртуально розміщуються точки доступу з необхідними характеристиками. Програмне забезпечення враховує потужність сигналу, наявність стін і перегородок, що дозволяє з досить високим відсотком точності уникнути інтерференції між каналами, які перекриваються. Крім того,

можливості програми InterpretAir дозволяють змоделювати технічні характеристики застосовуваних точок доступу та визначити оптимальні місця їх розміщення методом візуалізації зони дії. Нарешті потрібно відзначити, що планування мережі в середовищі програми може помітно знизитися кількість необхідного обладнання.

У процесі моделювання були обрані три типових приміщення: готельні номери на другому та третьому поверхах (рис. 3.4), зал ресторану (кафе-бар), в яких встановлюються точки безпровідного доступу. Вихідними даними для моделювання були вибрані: товщина стін, міжповерхових перекриттів, внутрішніх некапітальних перегородок, а також матеріал стін та вікон. Моделювання відбувається в середовищі безкоштовної пробної (demo) версії програми InterpretAir, що доступна для пробно-тимчасового використання [18].

Кількість точок доступу відповідає числу, заданому в завданні роботи, при цьому швидкість передачі даних в досліджуваних приміщеннях складає 54 Мбіт/с. Відповідність кольору на карті покриття відповідає рівню згасання сигналу та показано на рис. 3.5.

а) б)

Рисунок 3.4 – Результат моделювання точки доступу в номері на: а) 2-му та б) 3-му поверхах

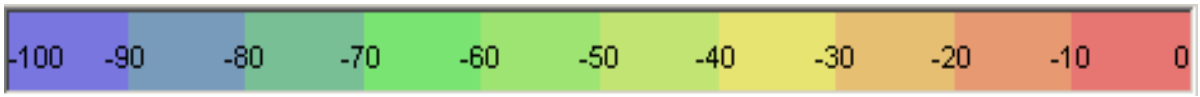

Рисунок 3.5 – Відповідність кольору на карті покриття рівню згасання сигналу

Таким чином, завдяки програмі InterpretAir здійснюється оцінка зон покриття безпровідних мереж та побудувати візуальну карту, яка дозволяє проаналізувати WLAN мережі та здійснити настройку обладнання. Після розгортання нової WLAN-мережі програма InterpretAir сканує всі канали стандартів IEEE 802.11a/b/g, записує їх основні характеристики та проводить кореляцію з планом приміщення. Рішення InterpretAir допомагає оптимізувати продуктивність бездротової мережі та прийняти своєчасні заходи для усунення проблем, які можуть вплинути на продуктивність мобільних додатків.

4 МОДЕЛЮВАННЯ, ПРОДУКТИВНІСТЬ ТА МАСШТАБОВАНІСТЬ ЗАХИЩЕНИХ КАНАЛІВ

Проблема вибору алгоритму шифрування та серверної ОС одна із найважливіших при створенні захищеного каналу мультисервісної мережі. Якби всі алгоритми були ідеальними (тобто не мали ніяких уразливостей), то криптостійкість його була б прямо пропорційна довжині ключа, оскільки єдиним способом для злому шифротексту був метод повного перебору. При використанні OpenVPN можливе використання алгоритмів шифрування RC5, DES, ECC, AES. Всі вищеописані алгоритми за весь час існування не були скомпрометовані жодного разу, отже, спиратимемося при оцінці стійкості алгоритму на довжину ключа. Збільшення довжини ключа позначається на продуктивності алгоритму через збільшення кількості раундів при шифруванні. Як приклад для тестування оберемо симетричний алгоритм блокового шифрування AES з розмірами блоку 128 і 256 біт. Цей вибір пояснюється тим, що, з одного боку, він є стандартом шифрування в багатьох країнах і, як наслідок, широко використовується для реалізації захищених каналів у корпоративних мережах. Тестування проводилося з двома серверними операційними системами Windows Server 2008 та Linux Ubuntu, що були обрані у якості основних для використання у мережі готельного комплексу.

4.1 Оцінка продуктивності захищеного каналу

Для основного тестування в реальних умовах були обрані сервером Intel Core 2 Du o E8200 (Wolfdale) з частотою 2667 МГц і об'ємом оперативної пам'яті в 2048 Мб. Як клієнти були обрані комп'ютери Intel Celeron з частотою 1800 МГц та оперативною пам'яттю у розмірі 790 Мб. Всі комп'ютери були об'єднані в загальну мережу за допомогою комутатора. Тестування

проводилося з двома серверними операційними системами Windows Server 2008 та Linux Ubuntu.

На клієнтах використовувалася операційна система Windows 8. Для реалізації зашифрованого каналу було обрано програму OpenVPN -2.0.

Як засіб вимірювання взято програмний продукт з графічною оболонкою Jpref версії 2.0.0. Jpref – кросплатформова клієнт-серверна програма – генератор TCP та UDP трафіку для тестування пропускної спроможності мережі.

Приведемо налаштування OpenVPN із застосуванням сертифікатів X.509.

Файл конфігурації серверів:

```
dev tap
server 192.168.0.0 255.255.255.0
cipher AES-128-CBC
tls-auth key.txt 0
tls-server
dh dh1024.pem
ca ca.crt
cert swat.crt
key swat.key
keepalive 10 60
```

Файл конфігурації клієнтів:

```
remote 192.160.1.111
dev tap
client
cipher AES-256-CBC
tls-auth key.txt 1
keepalive 10 60
tls-client
```

```
dh dh1024.pem
ca ca.crt
cert client.crt
key client.key
```

Для вибору мережевої ОС за умов роботи безлічі віддалених клієнтів із сервером по захищеному каналу необхідно отримати кількісну оцінку залежності пропускної спроможності цього каналу від типу використовуваної мережевої ОС, бітності ключа шифрування, кількості віддалених клієнтів. Під пропускною спроможністю захищеного каналу (його продуктивністю) розумітимемо кількість переданої інформації в одиницю часу [bits/sec].

Для вирішення поставленої задачі зробимо обчислювальний експеримент, використовуючи пакет Jpref для одного, двох і трьох клієнтів протягом 30 секунд для обраних варіантів мережевих ОС.

Результати тестування для варіанта ОС: сервер - Windows Server 2008, клієнт - Windows 8, представлені в таблиці 4.1

Таблиця 4.1 - Результати тестування захищеного каналу для варіанта: Windows Server 2008 із клієнтами Windows 8

Кількість клієнтів	Тип алгоритму шифрування							
	AES-128-CBC				AES-256-CBC			
	вих	вхід	сума	cpu	вих	вхід	сума	cpu
1	21	33,3	54,38	22,7	13,2	30,3	43,52	23
2	18,5	28,3	48,89	28,1	10,7	10,5	21,13	27,3
3	16	40,7	57,69	31,5	17,4	35,2	47,6	31,7

У таблиці 4.1 використані такі умовні позначення:

- вих - вихідний трафік від сервера до клієнта переданої інформації в одиницю часу [bits/sec];
- вхід - вхідний трафік від клієнта до сервера переданої інформації в одиницю часу [bits/sec];

- сума – сумований вихідний та вхідний трафік переданої інформації в одиницю часу [bits/sec];
- cpu – завантаження центрального процесора сервера представлена як % від максимально допустимого.

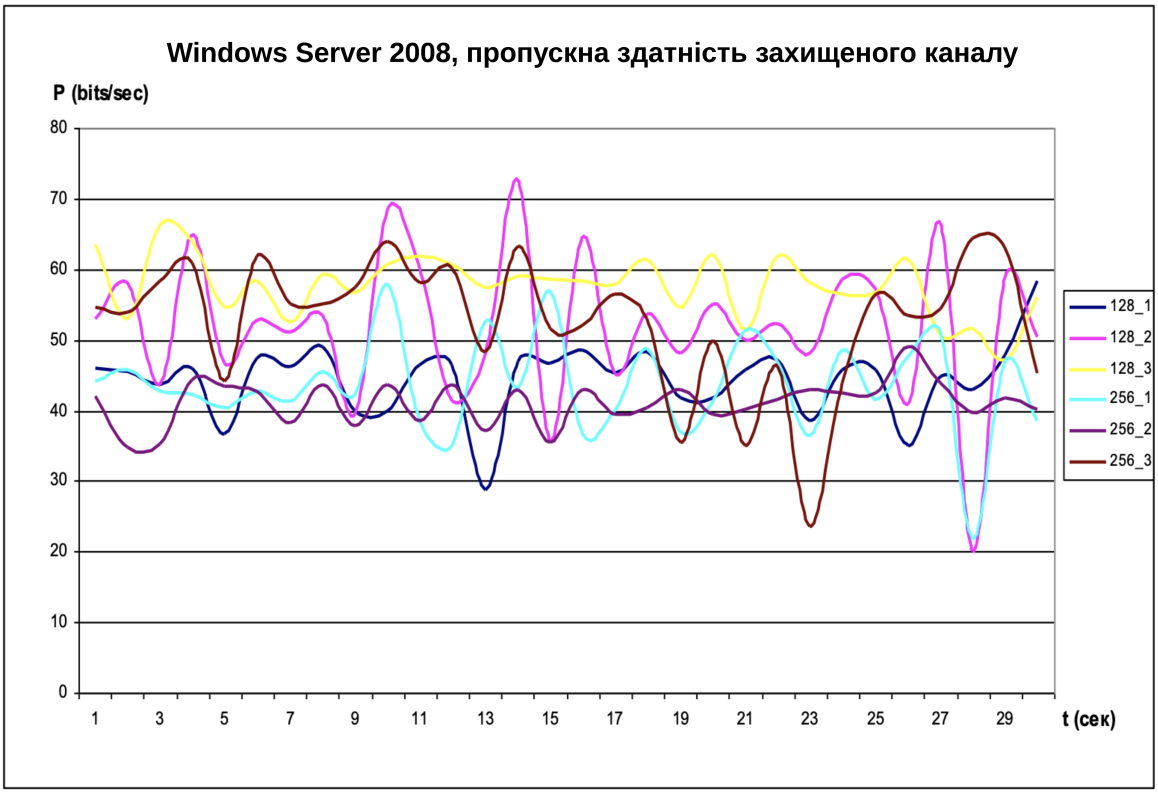

Рисунок 4.1 - Пропускна здатність каналу корпоративної мережі із захищеним каналом із серверною операційною системою Windows Server 2008

На рис. 4.1 використані такі умовні позначення:

128_1 – варіант досліду (128_1);

128 або 256 - розмір ключа шифрування у бітах 128, 256;

1, 2 чи 3 - кількість віддалених клієнтів під час тестування мережі;

P - пропускна здатність захищеного каналу, приймається значення за одиницю часу [bits/sec].

Результати тестування для варіанта ОС: сервер – Ubuntu, клієнт - Windows 8, представлені в таблиці 4.2

Таблиця 3.2 - Результати тестування захищеного каналу для варіанта: Ubuntu з клієнтами Windows 8

Кількість клієнтів	Алгоритм шифрування							
	AES-128-CBC				AES-256-CBC			
	вих	вхід	сума	cpu	вих	вхід	сума	cpu
1	22,5	33,6	55,04	23	22,5	31,7	54,21	22,4
2	20,3	32,2	51,47	27,7	22,3	30,8	53,16	26,6
3	27,9	41,8	68,68	29,6	24,5	39,2	63,78	30,5

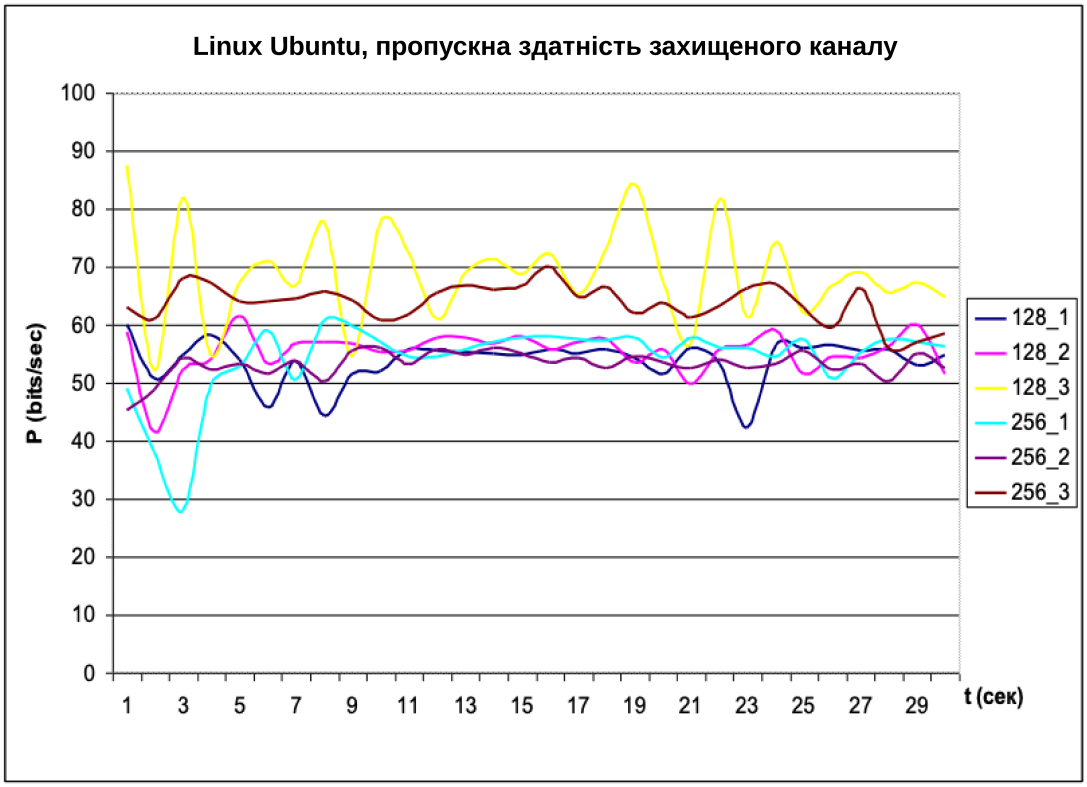

Рисунок 4.2 - Пропускна здатність каналу корпоративної мережі із захищеним каналом із серверною операційною системою Ubuntu

Усього було проведено 360 дослідів, і на їх основі побудовано узагальнений графік, що представляє загальну залежність пропускної спроможності захищеного каналу мережі. Ranал алгоритм шифрування регресійний

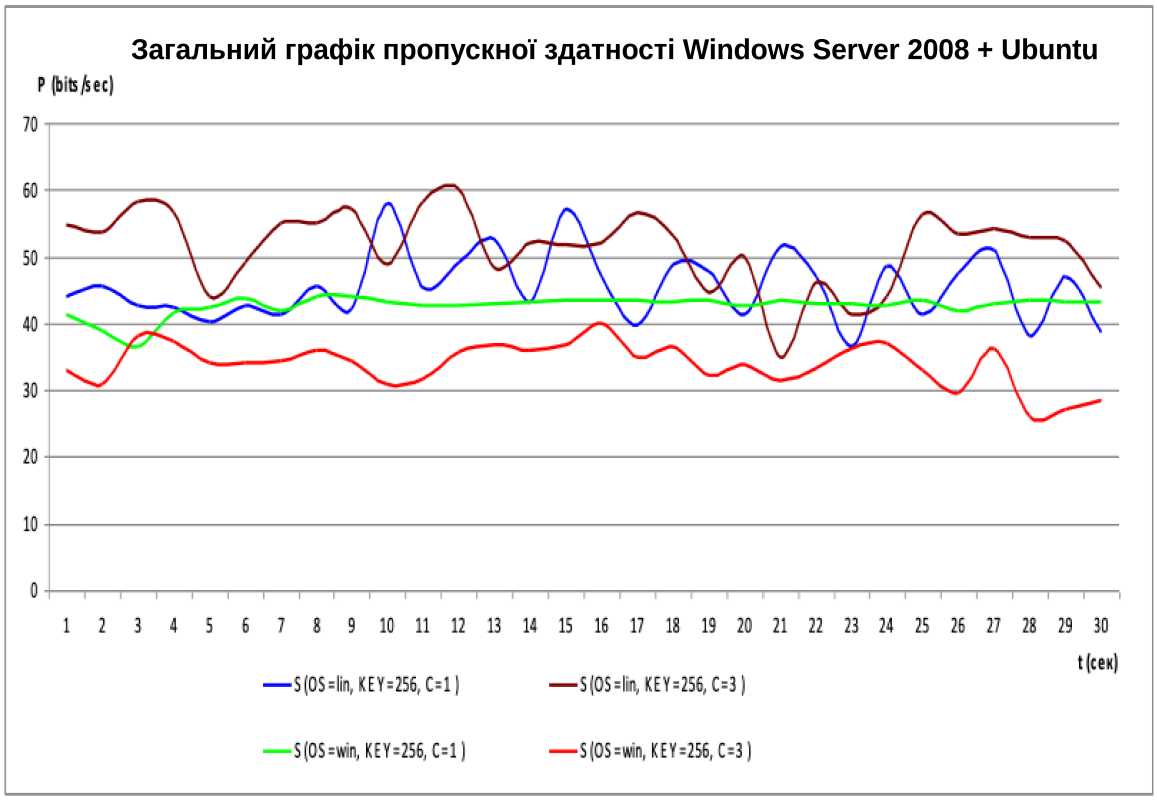

Рисунок 4.3 - Пропускна здатність каналу корпоративної мережі із захищеним каналом для альтернативних варіантів серверних ОС

На рис 4.3 використані такі умовні позначення:

- OS – тип мережевої операційної системи (MS Windows Server 2008 – win, Ubuntu – lin);
- KEY – y bit (біт) – довжина ключа, встановленого для використовуваного протоколу шифрування (використано групу протоколів AES-xxx-CBC, у назві якого замість xxx – вказується довжина ключа, використано значення 256 біт);
- C – кількість віддалених вузлів, які одночасно здійснюють обмін даними з сервером VPN;
- P - пропускна здатність захищеного каналу, приймається значення за одиницю часу [bits/sec].

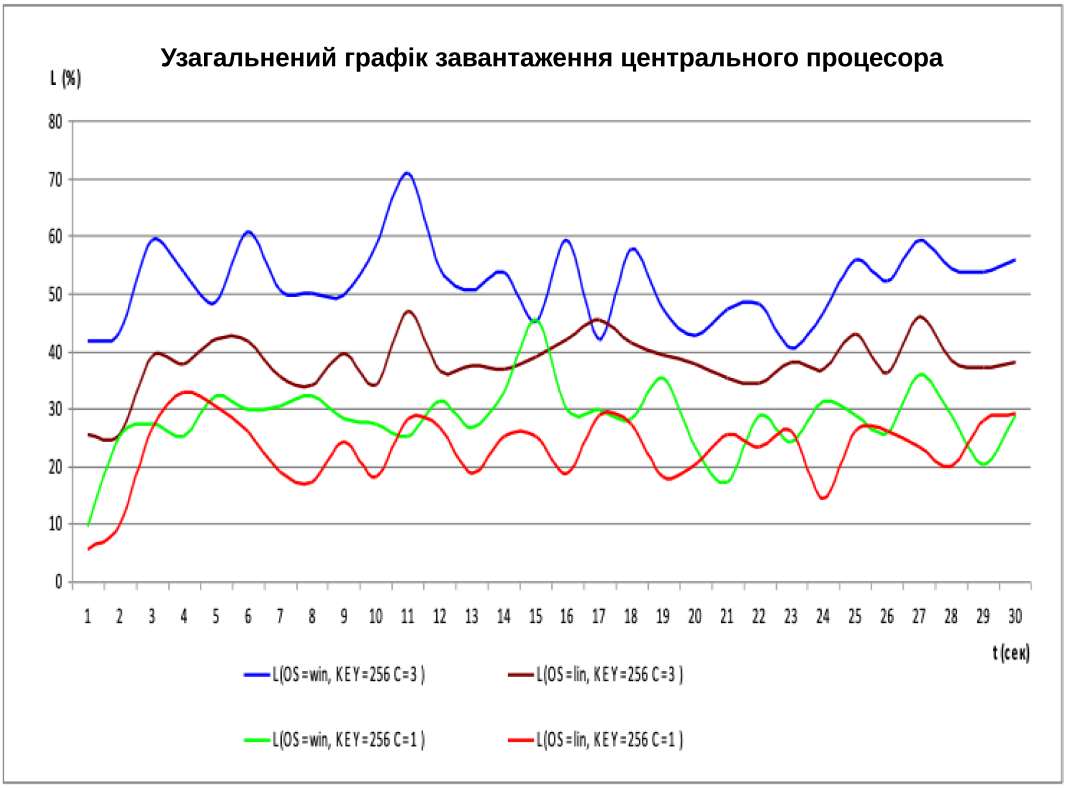

Рисунок 4.4 - Графік завантаження центрального процесора альтернативних варіантів серверних ОС

На рис 4.4 використані такі умовні позначення:

- OS – тип мережевої операційної системи (MS Windows Server 2008 – win, Ubuntu – lin);
- KEY – y bit (біт) – довжина ключа, встановленого для використовуваного протоколу шифрування (використано групу протоколів AES-xxx-CBC, у назві якого замість xxx – вказується довжина ключа, використано значення 256 біт);
- C – кількість віддалених вузлів, які одночасно здійснюють обмін даними з сервером VPN;
- L - завантаження центрального процесора сервера представлена у вигляді % від максимально допустимої.

Аналіз графіків, поданих на рис. 4.3 рис. 4.4, дозволяє зробити такі висновки:

1. За інших однакових умов збору статистики, ОС сімейства Ubuntu забезпечують більшу продуктивність порівняно з Windows 2008 в умовах захищеного каналу.
2. В умовах роботи ОС Ubuntu збільшення кількості віддалених клієнтів не позначається на пропускній здатності захищеного каналу, чого не можна сказати при використанні ОС сімейства MS Windows Server 2008, для неї характерні великі навантаження на продуктивність каналу;
3. Виходячи з проведених тестувань, можна зробити висновок, що для сучасних комп'ютерів серверного класу довжина ключа шифрування захищеного каналу незначно позначається на загальній продуктивності системи.
4. В умовах роботи Ubuntu навантаження на центральний процесор значно менше, особливо при збільшенні кількості вузлів мережі. Для ОС сімейства MS Windows Server 2008 характерні чималі навантаження на ЦП.

4.2 Розробка моделі функціонування мережі

З метою автоматизації вибору оптимальних параметрів у захищеному каналі корпоративної мережі, побудованої на базі OpenVPN, необхідно побудувати функцію відгуку, яка ідентифікуватиме пропускну здатність каналу в залежності від факторів, що впливають: операційної системи, довжини ключа, кількості вузлів корпоративної мережі. Математичним апаратом, який дозволяє вирішити це завдання, є Метод Групового Урахування Аргументів (Group Method of Data Handling). Він застосовується у найрізноманітніших галузях для аналізу даних та відшукання знань, прогнозування та моделювання систем, оптимізації та розпізнавання образів. Індуктивні алгоритми МГУА дають унікальну можливість автоматично знаходити взаємозалежність даних, вибрати оптимальну структуру моделі чи мережі та збільшити точність існуючих алгоритмів [19].

Цей підхід самоорганізації моделей принципово відрізняється від дедуктивних методів, що зазвичай використовуються. Він заснований на індуктивних принципах - знаходження кращого рішення ґрунтується на переборі різноманітних варіантів. За допомогою перебору різних рішень підхід індуктивного моделювання намагається мінімізувати роль передумов автора про результати моделювання. Комп'ютер сам знаходить структуру моделі та закони, що діють в об'єкті. Він може бути використаний при створенні штучного інтелекту, як порадник для вирішення спорів та прийняття рішень [20].

Іншим достоїнством МГУА є те, що він гарантує стійкість до перешкод одержуваних моделей. Чим більший ступінь неточності даних, що характеризується відношенням потужності перешкоди до потужності точних даних, тим простіше модель оптимальної складності, тому МГУА зі збільшенням перешкод вибирає дедалі вужчі кордони області моделювання і прості структури моделей. Таким чином, при самоорганізації моделі на ЕОМ вибирається структура, найближча до оптимальної для кожного рівня відношення завада/сигнал.

Виходячи з вищевикладеного, МГУА - найбільш зручний засіб для вирішення задачі кількісної ідентифікації системи, яка дозволяє отримати об'єктивну, стійку до перешкод, несуперечливу модель оптимальної структури.

Для підготовки елементів вибірки до використання в МГУА потрібно провести її цензурування, тобто, приведення до відрізка [0,1].

Для нормальної випадкової величини 99,7% значень перебувають усередині інтервалу

$$\left[\vec{X} - 3\sigma, \vec{X} + 3\sigma\right]$$

де $\vec{X}$ - середнє значення,

σ-дисперсія цієї величини, тому значення, що знаходяться поза цим інтервалом, як правило, породжені різними похибками і є викидами, а, отже, такі спостереження повинні бути видалені з вибірки.

Після цензурування вибірки усі її значення призводять до відрізка [0,1] за формулою

$$X_{ij} = \frac{X_{ij} - X_{jmin}}{X_{jmax} - X_{jmin}}. \tag{4.1}$$

Необхідність такого приведення викликана великою кількістю арифметичних операцій на елементах вибірки в МГУА, що при різних порядках чисел веде до накопичення великих похибок та поганої збіжності методу.

Для відновлення залежності використовується поліноміальний ітераційний алгоритм МГУА [20], в результаті роботи якого має бути отримана залежність

$$f(x,\alpha) = \sum_{k=1}^{m} \alpha_k \prod_{j=1}^{l} x_j^{\beta_{kj}} \quad , \tag{3.2}$$

де l - число елементів у вихідному базисі факторів;

m - число доданків моделі з ненульовими значеннями коефіцієнтів, зване складністю моделі.

Перед початком роботи алгоритму вибірка поділяється на дві частини: робочу, за якою модель будується, та екзаменаційну – на ній вона перевіряється.

Одне з основних труднощів при застосуванні методів перехресного обґрунтування, окремим випадком яких є МГУА, пов'язана з розбиттям вибірки на дві підмножини - робочу та екзаменаційну. Оскільки модель значною мірою визначається робочою частиною вибірки, необхідно, щоб обсяг робочої частини був більшим, і щоб і в робочу, і в екзаменаційну частину потрапляли

спостереження з усього інтервалу безлічі значень, тому перед запуском алгоритму МГУА, корисно впорядкувати спостереження у вибірці по зростанню відгуку, а, потім, вибирати дані для екзаменаційної частини через деяку однакову кількість спостережень [20].

Розглянемо докладніше процедуру МГУА.

Як нульове наближення береться безліч моделей складності 1, це самі значення факторів. Таким чином, початкова модель має вигляд $t = \alpha_k x_k$, де коефіцієнт α_k визначається ітераційним методом найменших квадратів (МНК) по робочій частині вибірки, після цього по екзаменаційній частині вибірки визначається F найкращих моделей за допомогою зовнішнього критерію регулярності - мінімуму евклідової норми вектора нев'язки між реальним значенням відгуку та значенням, отриманим по моделі, що перевіряється

$$R = \sum_{k=1}^{N_э} |t_k - f(x_k, \alpha_k)|, \qquad (4.3)$$

де $N_э$ - число елементів в екзаменаційній частині вибірки.

Для формування базису змінних подальших кроків ітераційної процедури використовується функція $g = (v_1, v_2, ..., v_m)$, яка з кращих моделей F попереднього кроку і l вихідних змінних формує базисні змінні наступного кроку, наприклад,

$$g(w_1, w_2, w_3, \eta) = \eta_1 w_1 + \eta_2 w_2 w_3. \qquad (4.4)$$

Число F переданих від кроку до кроку найкращих моделей називається свободою вибору методу.

При формуванні базису r-го кроку враховується той факт, що на r-му кроці складність моделі не повинна перевищувати r. Паралельно з процесом

побудови базису йде побудова набору коефіцієнтів для цього базису ітераційним МНК з робочої частини вибірки та обчислення критерію регулярності з екзаменаційної частини. У пам'яті ЕОМ у кожен момент часу зберігаються лише F кращих моделей. При вичерпанні безлічі базисів r-го кроку здійснюється перехід до наступного (r+1) кроку [20].

Процес зупиняється при виконанні наступної нерівності:

$$\min_k R_k^{r-1} \le \min_k R_k^r \le \min_k R_k^{r+1} \ , \tag{4.5}$$

і за результат приймається найкраща модель (r-1) кроку.

Тепер розглянемо докладніше процедуру підбору коефіцієнтів моделі за заданою структурою моделі ітераційним МНК.

Нехай задана структура моделі складності $m : f_1, f_2, ..., f_m$, необхідно підібрати коефіцієнти $\alpha_1, \alpha_2, ..., \alpha_m$, щоб наблизити значення відгуку з робочої частини вибірки:

$$t = \sum_{k=1}^{N_p} \alpha_k f_k = \varphi(\alpha, f) \tag{4.6}$$

з точністю до заданого ε, щоб мінімізувати виважену суму квадратів відхилень:

$$S = \sum_{l=1}^{N_p} \beta_i (t_i - \sum_{k=1}^{m} \alpha_k f_{ki})^2 \to min \ , \tag{4.7}$$

де Np – число спостережень у робочій частині вибірки.

Спочатку вагові коефіцієнти β_i спостережень передбачаються однаковими та рівними 1, з цими вагами будується система коефіцієнтів α_k, k =1,2,..., m моделі у вигляді розв'язання системи лінійних рівнянь

$$\begin{cases} \alpha_1 \sum_{l=1}^{N_p} \beta_i f_{1i}^2 + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{1i} f_{2i} + \ldots + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{1i} f_{ki} = \sum_{i=1}^{N_p} \beta_i t_i f_{1i} \\ \alpha_1 \sum_{i=1}^{N_p} \beta_i f_{2i} f_{1i} + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{2i}^2 + \ldots + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{2i} f_{ki} = \sum_{i=1}^{N_p} \beta_i t_i f_{2i} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_1 \sum_{i=1}^{N_p} \beta_i f_{ki} f_{1i} + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{ki} f_{2i} + \ldots + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{ki}^2 = \sum_{i=1}^{N_p} \beta_i t_i f_{ki} . \end{cases} \qquad (3.8)$$

Потім вибираються ваги $\beta_i \;, i = 1,2,\ldots,N_p$ таким чином, щоб вага і-го спостереження залежала від відношення і-го залишку в попередній ітерації до загальної міри залишків у цій ітерації:

$$\beta_i = \frac{1}{S}\left| t_i - \sum_{k=1}^{m} \alpha_k f_{ki} \right| \qquad (4.9)$$

і за цими вагами будується нова система коефіцієнтів моделі $\alpha_i \;, i = 1,2,\ldots,m$ і т.д. Процес зупиняється, коли досягається заданий рівень точності ε, тобто. коли виконається нерівність

$$\frac{1}{S_k}\left| S_k - S_{k-1} \right| \prec \varepsilon \;. \qquad (4.10)$$

Для використання отриманої залежності в імітаційній моделі необхідно провести перерахунок коефіцієнтів моделі з урахуванням коефіцієнтів лінійного перетворення, яке здійснювалося при центруванні та нормуванні [6].

Для побудови функції відгуку скористаємося спеціалізованим пакетом для моделювання нейронних мереж NeuroShell 2 (Ward Systems Group, Inc.), в якому реалізовано комбінаторний алгоритм МГУА. Для побудови функції потрібна серія дослідів з різним станом мережі, використовуватимемо дані, отримані під час тестування з додатка А.

В результаті розрахунку з пакетом NeuroShell було отримано функцію відгуку:

$$Y=-0.42-0.14*X1-8.8E-002*X2+0.4*X3+0.36*X3^2+6.7E-002*X1*X2+0.26*X1*X3-2.6E-002*X2*X3, \quad (4.11)$$

де: X1 = 2 * (win/lin-1) -1 операційна система;

X2 = 2 * (key-128)/128 довжина ключа в бітах;

X3=(Kol-1)/2 кількість клієнтів що у тестування;

Y = 2* S <-> C - 6.54/87 (розрахункова продуктивність у тисячах bit/sec).

В результаті роботи пакету NeuroShell побудуємо графіки:

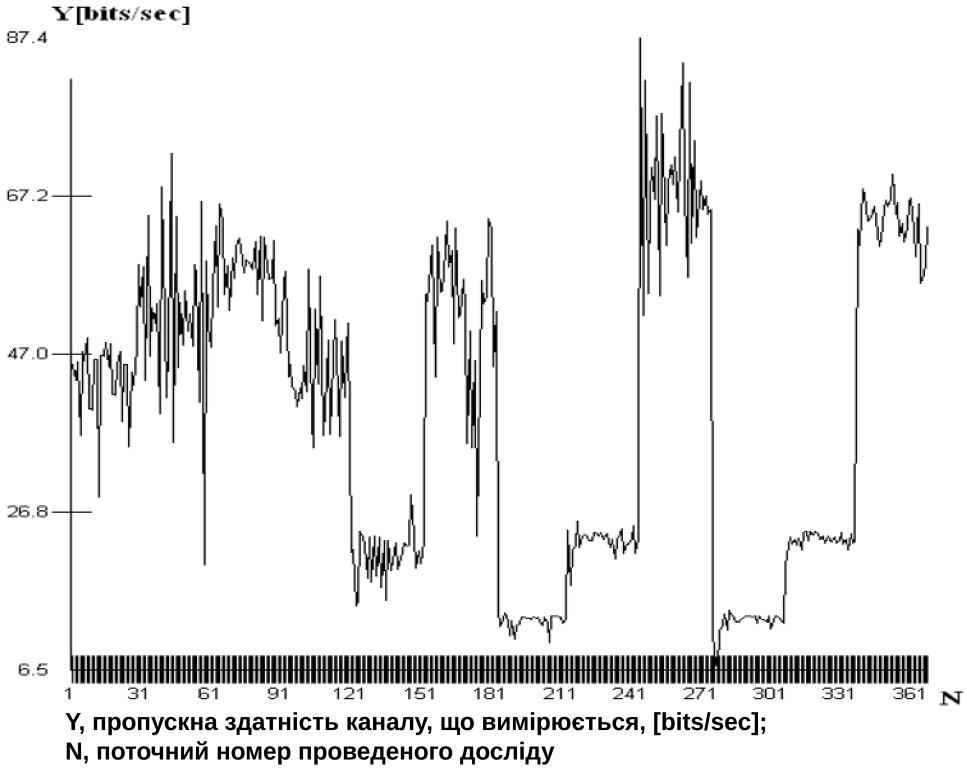

Рисунок 4.5 - Графік продуктивності захищеного каналу побудований на основі даних, отриманих дослідним шляхом

Значення параметра N визначає умови проведення досліду в частині операційної системи сервера, що використовується, кількості віддалених клієнтів мережі і довжини ключа шифрування. Вся необхідна інформація для побудови графіків на рис. 4.5-4.8, наведена у додатку А.

Для порівняння з вихідними даними, отриманими при прорахунку програмою, побудуємо графік пропускної спроможності мережі, отриманий дослідним шляхом при тестуванні (рис. 4.7).

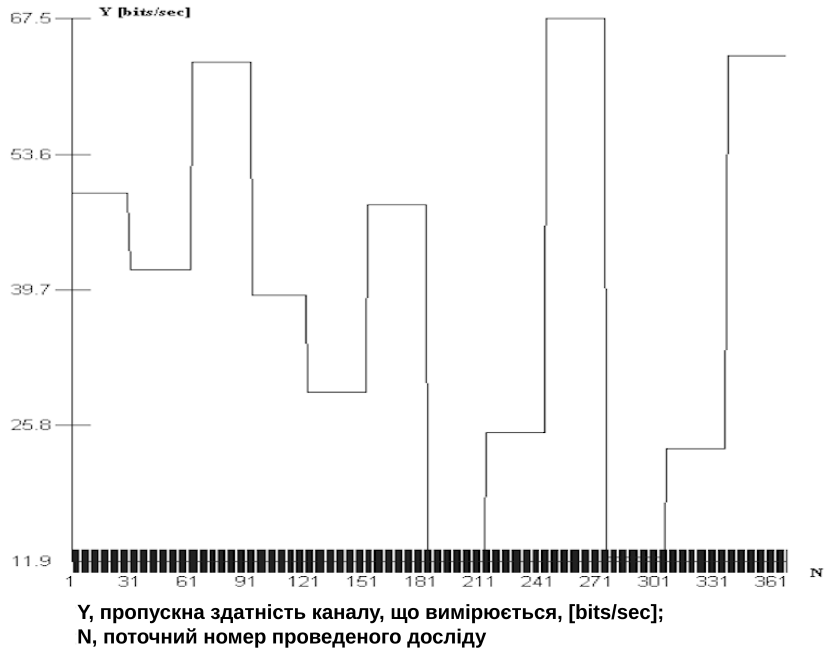

Рисунок 4.6 - Графік функції Y(N) продуктивності захищеного каналу корпоративної мережі

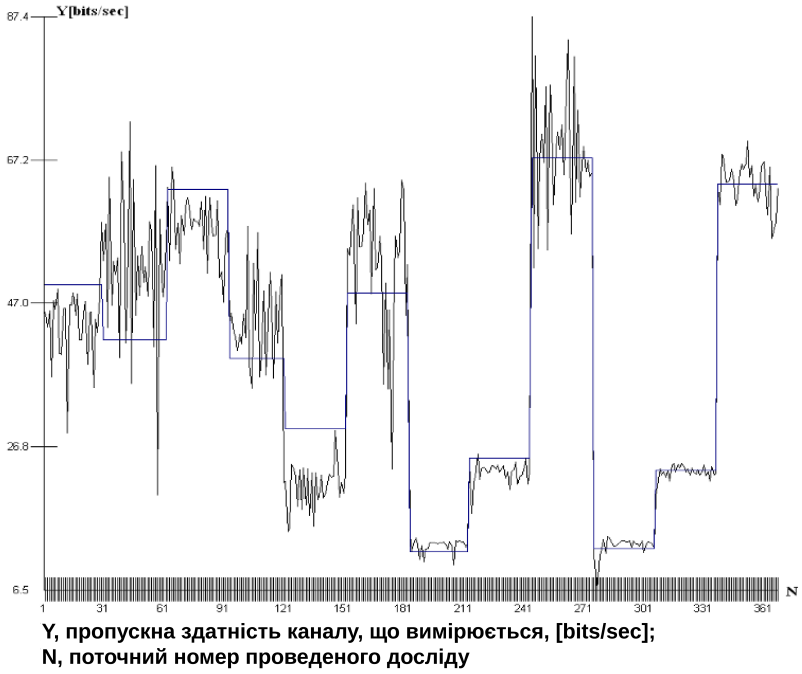

Рисунок 4.7 - Поєднаний графік функції відгуку Y(N) та емпіричних даних

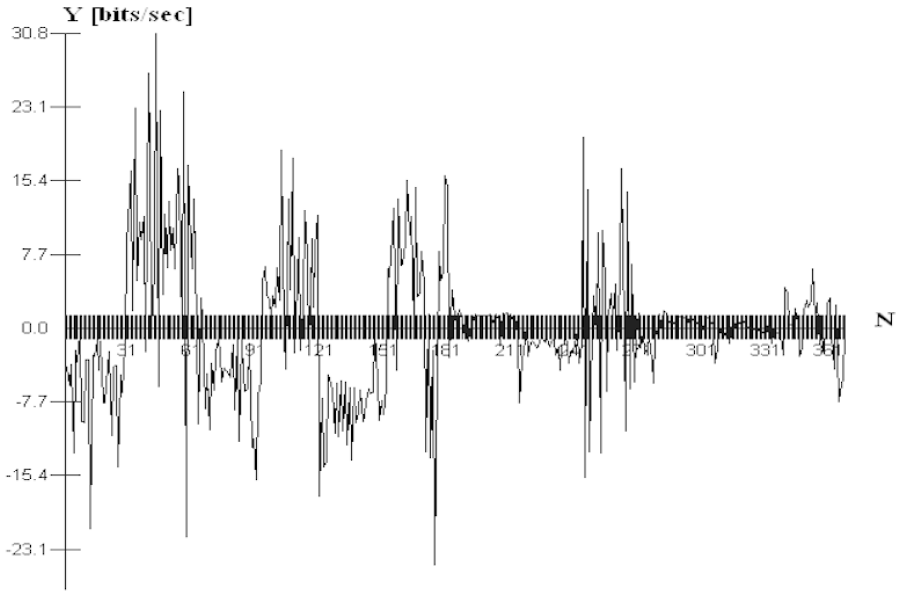

Рисунок 4.8 - Графік середньоквадратичного відхилення помилки та кореляцією Y(N) та вихідних даних

З графіка рис 4.7 видно, що функція відгуку, отримана за допомогою пакета МГУА рис 4.6, схожа на графік рис 4.5, що побудовано на основі даних отриманих дослідним шляхом. Виходячи з цього, можна судити про адекватність даної моделі в реальних умовах.

Отримана функція відгуку (4.11) дозволяє проводити періодичну адаптацію моделі до змін корпоративної мережі залежно від навантаження. Дозволяє розрахувати продуктивність захищеного каналу при зміні ситуації в корпоративній мережі (зростання трафіку, зміна алгоритмів шифрування, зміна кількості віддалених робочих станцій, що входять до корпоративної мережі). Ця функція може бути використана у програмному забезпеченні для керування захищеним каналом. Наприклад, така програма може виконувати динамічну зміну алгоритму шифрування на основі передбаченої моделі поведінки системи. Варто відзначити і те, що функцію можна автоматично адаптувати до середовища в міру розширення даних про стан каналу, оскільки МГУА дозволяє динамічно «навчати» нові вибірки.

4.3 Багатомірний регресійний аналіз

Щоб визначити значимість залежних змінних на отриману функцію відгуку (4.11) проведемо багатомірний регресійний аналіз.

Очевидно, що просте поверхове вивчення даних не дозволяє виявити, які фактори, розглянуті на стадії статистичного аналізу вихідної інформації, є суттєвими, а які – ні.

Необхідно знайти оптимальний варіант моделі, що відображає основні закономірності досліджуваного явища з достатньою мірою статистичної надійності.

У модель повинні бути включені всі фактори, що впливають на залежну змінну (у нашому випадку – кількість вузлів, операційна система, розмір ключа шифрування). При невиконанні цієї вимоги модель може виявитися неадекватною внаслідок неврахування істотних факторів.

З іншого боку, кількість факторів, що включаються до моделі, не повинна бути занадто великою. Невиконання цієї вимоги призводить до необхідності збільшення числа спостережень, неможливості використання досить складних залежностей, зниження точності оцінок, складності інтерпретації моделі і труднощі її практичного використання [21].

Отже, виникає завдання зменшення кількості змінних, які включаються до моделі, без порушення вихідних передумов, тобто, завдання зниження розмірності моделі.

Виділяють два суттєві підходи до вирішення проблеми скорочення кількості вихідних змінних:

- відсіювання менш істотних факторів у процесі побудови регресійної моделі;

- заміна вихідного набору змінних меншим числом еквівалентних факторів, отриманих в результаті перетворення вихідного набору.

Процедура відсіву несуттєвих факторів у процесі побудови регресійної моделі та отримала назву багатокрокового регресійного аналізу. Цей метод заснований на обчисленні кількох проміжних рівнянь регресії, в результаті аналізу яких отримують кінцеву модель, що включає лише фактори, що надають статистично значний вплив на залежну досліджувану змінну. Різні поєднання тих самих чинників надають різний вплив на залежну змінну. Внаслідок цього виникає необхідність вибору найкращої моделі, так як перебирати всі можливі варіанти поєднання факторів і будувати безліч рівнянь регресії (кількість яких може бути дуже великою) просто не має сенсу [21].

Таким чином, методи покрокового регресійного аналізу дозволяють уникнути настільки громіздких розрахунків і отримати досить надійну і повну модель залежності досліджуваної ознаки від ряду пояснюючих змінних.

Як було зазначено вище, основою багатокрокового регресійного аналізу є побудова рівняння регресії. Розглянемо докладніше його систему та основні поняття.

У загальному вигляді багатовимірна лінійна регресійна модель залежності у від змінних, що пояснюють x_1, x_2,…, x_k має вигляд:

$$\tilde{y} = M(y/x_i) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_k x_k + \varepsilon \qquad (4.12)$$

Для оцінки невідомих параметрів β_j взято випадкову вибірку обсягу n з (k+1)–вимірної випадкової величини (у, x_1, x_2,…, x_k).

У матричній формі модель має вигляд:

$$Y = X\beta + \varepsilon \qquad (4.13)$$

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ ... \\ ... \\ y_n \end{pmatrix}, \quad X = \begin{pmatrix} 1\,x_{11}\,x_{12}...x_{1k} \\ 1\,x_{21}\,x_{22}...x_{2k} \\ ..... \\ 1\,x_{n1}\,x_{n2}...x_{nk} \end{pmatrix}, \quad \beta = \begin{pmatrix} \beta_0 \\ \beta_1 \\ ... \\ \beta_k \end{pmatrix}, \varepsilon = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ ... \\ \varepsilon_n \end{pmatrix} \quad (4.14)$$

де

- вектор-стовпець фактичних значень залежної змінної розмірності n;

- матриця значень пояснюючих змінних розмірності n*(k+1);

- вектор-стовпець невідомих параметрів, що підлягають оцінці, розмірності (k+1);

- вектор-стовпець випадкових помилок розмірності n з математичним очікуванням ME = 0 і коваріаційної матриці

$$V(\varepsilon) = M(\varepsilon\,\varepsilon^T) = \sigma^2 E_n \quad (4.15)$$

при цьому

$E_n = \begin{pmatrix} 1\,0\,0...0 \\ 0\,1\,0...0 \\ ..... \\ 0\,0\,0...1 \end{pmatrix}$ - поодинока матриця розмірності (nxn)

Оцінки невідомих параметрів β_j є методом найменших квадратів, що мінімізує скалярну суму квадратів $Q = (Y - X\beta)^T (Y - X\beta)$ за компонентами вектора β.

Далі підставивши вираз

$$(Y - X\beta) = \begin{pmatrix} y_1 \\ y_2 \\ ... \\ y_n \end{pmatrix} - \begin{pmatrix} \beta_0 + \sum_{j=1}^{k} x_{1j}\beta_j \\ \beta_0 + \sum_{j=1}^{k} x_{2j}\beta_j \\ ..... \\ \beta_0 + \sum_{j=1}^{k} x_{nj}\beta_j \end{pmatrix} = \begin{pmatrix} y_1 - \beta_0 - \sum_{j=1}^{k} x_{1j}\beta_j \\ y_2 - \beta_0 - \sum_{j=1}^{k} x_{2j}\beta_j \\ ..... \\ y_n - \beta_0 - \sum_{j=1}^{k} x_{2j}\beta_j \end{pmatrix} \quad (4.16)$$

у $Q = (Y - X\beta)^T (Y - X\beta)$

отримуємо скалярну суму квадратів

$$Q = \sum_{i=1}^{n} (y_i - \beta_0 - \sum_{j=1}^{k} x_{ij}\beta_j)^2$$

Умовою обігу отриманої суми в мінімум є система нормальних рівнянь:

$$\frac{\partial Q}{\partial \beta_j} = 0$$, (J = 0,1,2, ..., k).

В результаті диференціювання виходить:

$$2X^T(Y - X\beta) = 0.$$

При заміні вектора невідомих параметрів на оцінки, отримані методом найменших квадратів, отримуємо наступний вираз:

$$X^T Y = X^T X b. \quad (4.17)$$

Далі помноживши обидві частини рівняння зліва на матрицю $(X^T X)^{-1}$, отримаємо

$$(X^T X)^{-1} \cdot (X^T Y) = (X^T X)^{-1} \cdot (X^T X) b \quad (4.18)$$

З урахуванням що $(X^T X)^{-1}(X^T X) = E$, то $b = (X^T X)^{-1}(X^T Y)$.

Отримані оцінки вектора b є не зміщеними та ефективними.

Коварійна матриця вектора b має вигляд:

$$V(b) = \sigma^2 (X^T X)^{-1}$$

де σ^2 - залишкова дисперсія.

Елементи головної діагоналі цієї матриці є дисперсією вектора оцінок b. Інші елементи є значеннями коефіцієнтів коваріації:

$$\text{cov}(b_i b_j) = M(b_i - \beta_i)(b_j - \beta_j), \tag{4.19}$$

де $i = 1 \div n$, $j = 0 \div k$.

Таким чином, оцінка b_j – це лінійна функція від залежної змінної. Вона має нормальний розподіл з математичним очікуванням β_j та дисперсією

$$D_{b_j} = \sigma^2 \,\&\, *[(X^T X)^{-1}]_{jj}. \tag{4.20}$$

Незміщена оцінка залишкової дисперсії визначається за такою формулою:

$$\hat{S}^2_{ост} = \frac{1}{n-k-1}(Y - Xb)^T (Y - Xb) \tag{4.21}$$

де n – обсяг вибіркової сукупності;

k - число пояснюючих змінних.

Для перевірки значущості рівняння регресії використовують F-критерій дисперсійного аналізу, що ґрунтується на розкладанні загальної суми квадратів відхилень на складові частини:

$$Q_{общ} = Q_R + Q_{ост}$$

де $Q_R = (Xb)^T (Xb) = \sum_{i=1}^{n} \hat{y}_i^2$ (4.22)

- сума квадратів відхилень (від нуля), обумовлена регресією;

$$Q_{ост} = (Y - Xb)^T (Y - Xb) = \sum_{i=1}^{n} e_i^2 \tag{4.23}$$

- сума квадратів відхилень фактичних значень залежної змінної від розрахункових $\hat{y} = Xb$, тобто. сума квадратів відхилень щодо площини регресії, обумовлене впливом випадкових та неврахованих у моделі факторів.

Для перевірки гіпотези $H_0 : \beta = 0$ використовується величина

$$F_H = \frac{\frac{1}{k+1} Q_R}{\frac{1}{n-k-1} Q_{ост}} \tag{4.24}$$

яка має F-розподіл Фішера-Снедекору з числом ступенів свободи $\nu_1 = k+1$ та $\nu_2 = n-k-1$. Якщо $F_H > F_{кр}$, то рівняння регресії значиме, тобто, у рівнянні є хоча б один коефіцієнт регресії, відмінний від нуля.

У разі значимого рівняння регресії перевіряється значимість окремих коефіцієнтів регресії. Для перевірки нульової гіпотези $H_0 : \beta_j = 0$ використовується величина

$$F_H = \frac{b_j^2}{\hat{S}^2 [(X^T X)^{-1}]_{jj}} \tag{4.25}$$

яка має F-розподіл Фішера-Снедекору з числом ступенів свободи $\nu_1 = 1$ та $\nu_2 = n-k-1$; $[(X^T X)^{-1}]_{jj}$ - відповідний елемент головної діагоналі коваріаційної матриці.

Коефіцієнт регресії β_j вважається значимим, якщо $F_H > F_{кр}$. Для значимих коефіцієнтів регресії можна побудувати довірчі інтервали, використовуючи формулу

$$\beta_j \in \{b_j \pm t_\gamma \hat{S}[(X^T X)^{-1}]_{jj}\} \quad (4.26)$$

де t_γ знаходиться за таблицею розподілу Стьюдента для рівня значущості $\alpha = 1 - \gamma$ та числа ступенів свободи $\nu = n - k - 1$.

Проводитимемо регресійний аналіз за допомогою програми Statistica 6.0

Як дані для проведення множинної регресії використовуватимемо табличні дані з додатка А.

Statistica 6.0 - система для статистичного аналізу даних, що включає широкий набір аналітичних процедур і методів: більше 10 000 різних типів графіків, описові та внутрішньогрупові статистики, розвідувальний аналіз даних, кореляції, швидкі основні статистики та блокові статистики, інтерактивний імовірнісний калькулятор, Т- критерії (та інші критерії групових відмінностей), таблиці частот, сполученості, прапорів та заголовків, аналіз багатовимірних відгуків, множинна регресія, непараметричні статистики, загальна модель дисперсійного та підступного розподілу [22]. (Наведено опис лише базового блоку. Також існують додаткові блоки: Лінійні/нелінійні моделі, Багатовимірні розвідувальні технології, Аналіз потужності, Нейронні мережі, Data Mining, Карти контролю якості, Аналіз Процесів, Планування експериментів та ін.)

Результати, отримані з програми Statistica 6.0 в результаті розрахунку за вихідними даними із додатка А:

Таблиця 4.3 Матриця парних коефіцієнтів кореляції

	X1	X2	X3	Y
X1	1,000 00	0,01094	-0,01016	-0,268308
X2	0,01094	1,000 00	0,00355	-0,180454
X3	-0,01016	0,00355	1,000 00	0,663083
Y	-0,26831	-0,18045	0,66308	1,00000

У таблиці 4.3 переставлені такі умовні позначення:

- X1 – тип мережевої операційної системи (MS Windows Server 2008 – win, Ubuntu 8 – lin);
- X2 – у bit (бітах) – довжина ключа, встановленого для використовуваного протоколу шифрування (використано групу протоколів AES-xxx-CBC, у назву якого замість xxx – вказано довжини ключа, використано значення 128 та 256);
- X3 – кількість віддалених вузлів, які одночасно здійснюють обмін даними з сервером VPN;
- Y – отримана функція відгуку.

Аналіз матриці таблиці 4.3 парних коефіцієнтів кореляції показує, що результативний показник найтісніше пов'язані з показником X3 – кількістю клієнтів, оскільки цей показник має найбільше значення.

Звідси можна зробити висновок, що найбільш значущим параметром функції відгуку (4.11), отриманої раніше, є параметр X3, тобто саме кількість клієнтів більшою мірою вплинула на функцію при її прорахуванні пакетом NeuroShell.

4.4 Механізми оптимізації мережі

Масштабованість — це здатність системи адаптуватися до розширення вимог і зростання обсягів розв'язуваних завдань. Система «1С: Підприємство 8.0» має гарні можливості масштабування. Вона дозволяє працювати як у файловому варіанті, так і з використанням технології клієнт-сервер. У разі застосовується сучасна трирівнева архітектура, коли між клієнтом і сервером баз даних Microsoft SQL Server розташовується сервер 1С: Підприємства 8.0.

Важливо, що одні й ті самі прикладні рішення (конфігурації) можна використовувати як і файловому, і у клієнт-серверному варіанті роботи. При переході від файлового варіанта до технології клієнт-сервер не потрібно вносити зміни в прикладне рішення. Тому вибір варіанта роботи повністю залежить від потреб замовника та його фінансових можливостей. На початковій

стадії можна працювати у файловому варіанті, а потім зі збільшенням кількості користувачів та обсягу бази даних можна легко перейти на клієнт-серверний варіант [8].

Платформа «1С: Підприємство 8.0» дозволяє створювати як прості рішення для автоматизації завдань невеликих підприємств та домашніх користувачів, так і досить складні автоматизовані системи з великою кількістю об'єктів та взаємозв'язків між ними, що реалізують комплекс завдань з обліку та управління підприємством [8].

Трирівнева архітектура «клієнт-сервер»

Одним із найбільш суттєвих нововведень 1С: Підприємства 8.0 є реалізація трирівневої архітектури «клієнт-сервер». У 1С: Підприємстві 7.7 у клієнт-серверному варіанті роботи з інформаційною базою програма, що працює на комп'ютері користувача, зверталася безпосередньо до бази даних у середовищі MS SQL Server. У новій версії одному з комп'ютерів працює сервер 1С: Підприємства 8.0. Програма, що працює у користувача, взаємодіє із сервером 1С: Підприємства 8.0, а сервер за потреби звертається до бази даних MS SQL Server. При цьому фізично сервер 1С: Підприємства 8.0 та MS SQL Server можуть розташовуватися як на одному комп'ютері, так і на різних. Це дозволяє адміністратору за необхідності розподіляти навантаження між серверами [8].

Використання сервера 1С: Підприємства 8.0 дає змогу зосередити на ньому виконання найбільш об'ємних операцій з обробки даних. Наприклад, при виконанні навіть дуже складних запитів програма, що працює у користувача, отримуватиме лише необхідну їй вибірку, а вся проміжна обробка виконуватиметься на сервері. Зазвичай збільшити потужність сервера набагато простіше, ніж оновити парк клієнтських машин [8].

Іншим важливим аспектом використання 3-х рівневої архітектури є зручність адміністрування та впорядкування доступу користувачів до інформаційної бази. У цьому варіанті користувач не повинен знати про фізичне розташування конфігурації або бази даних. Весь доступ здійснюється через

сервер 1С: Підприємства 8.0. При зверненні до тієї чи іншої інформаційної бази користувач повинен вказати лише ім'я сервера та ім'я інформаційної бази, а система запитує відповідно ім'я та пароль користувача.

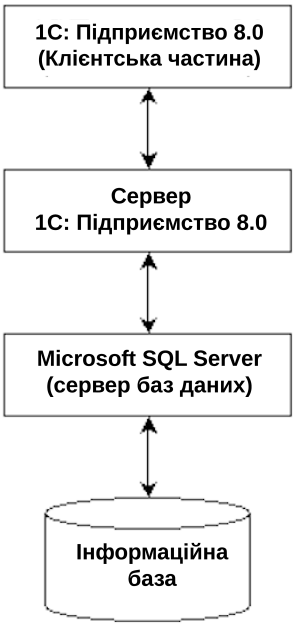

Рисунок 4.9 - Трирівнева архітектура «клієнт-сервер» 1С

Технологічна платформа 1С:Підприємства 8 містить ряд механізмів, що оптимізують швидкість роботи прикладних рішень.

1. Виконання на сервері

У варіанті клієнт-сервер використання сервера 1С:Підприємства 8 дозволяє зосередити на ньому виконання найбільш об'ємних операцій з обробки даних. Наприклад, при виконанні навіть дуже складних запитів програма, що працює у користувача, отримуватиме лише необхідну їй вибірку, а вся проміжна обробка виконуватиметься на сервері. Зазвичай збільшити потужність сервера набагато простіше, ніж оновити парк клієнтських машин [8].

2. Кешування даних

Система 1С:Підприємство 8 використовує механізм кешування даних, зчитаних з бази даних при використанні об'єктної техніки. Під час звернення до

реквізиту об'єкта виконується читання всіх даних об'єкта в кеш, що у оперативної пам'яті. Наступні звернення до реквізитів того ж об'єкта будуть направлятися вже в кеш, а не в базу даних, що значно скорочує час, що витрачається на отримання потрібних даних [8].

3. Робота вбудованої мови на сервері

При роботі в клієнт-серверному варіанті розробник може організувати виконання різних процедур та функцій загальних модулів та модулів об'єктів на сервері програми або клієнтському місці. Розподілене виконання процедур та функцій дозволяє винести на сервер виконання "важких" алгоритмів і тим самим забезпечити однакову продуктивність на різних клієнтських машинах [8].

4.5 Продуктивність 1С: Підприємства 8.1

Для оцінки продуктивності та масштабованості клієнт-серверної версії 1С:Підприємства 8 було проведено ряд тестів, що дозволяють:

- оцінити працездатність та продуктивність 1С:Підприємства 8 при роботі з серверними операційними системами: Windows Server 2008 та Ubuntu;
- оцінити працездатність та продуктивність 1С:Підприємства 8 при роботі з різними СУБД PostgresSQL, MSSQLserver.

Під час проведення тесту застосовувалися загальноприйняті підходи до оцінки продуктивності корпоративних інформаційних систем:

- використання для тестування типового прикладного рішення;
- тестування операцій, найбільш критичних з погляду роботи типової організації;
- тестування операцій при фіксованих параметрах, типових більшості організацій;
- програмна імітація типових сценаріїв роботи користувачів системи, що створюють навантаження, яке істотно перевищує навантаження, що створюється реальними користувачами;

- використання як основні показники обсягу бізнес-операцій, що відображаються в системі в одиницю часу, та середнього часу виконання операції.

4.6 Тестування 1С Підприємства

Тестування проводилося на двох серверних операційних системах Windows Server 2008 (Ms SQL Server 2008) та Linux Ubuntu (PostgreSQL). Використовувалося спеціалізоване програмне забезпечення для тестування: 1С:Корпоративний інструментальний пакет та TPC-1C-GILV безкоштовна утиліта для тестування.

Корпоративний інструментальний пакет

1С: Корпоративний інструментальний пакет - призначений для підвищення продуктивності, масштабованості та надійності інформаційних систем на платформі 1С: Підприємство 8 за рахунок:

- виявлення та автоматичного аналізу можливих технічних проблем на будь-яких стадіях впровадження (у тому числі на стадії проектування);

- отримання об'єктивної інформації про продуктивність системи;

- отримання повної технічної інформації про проблеми продуктивності, що є в системі, з метою подальшої оптимізації її коду [22].

Корпоративний інструментальний пакет може використовуватися як самостійно (наприклад, для оцінки застосування будь-якої типової конфігурації для вирішення завдань клієнта) так і як додатковий інструмент, що дозволяє провести аналіз «вузьких місць» і підвищити продуктивність і масштабованість впроваджуваної або вже впровадженої системи [22].

Основні завдання, які вирішуються за допомогою Корпоративного інструментального пакету:

- проведення розрахованих на велику кількість користувачів навантажувальних випробувань без участі реальних користувачів:

- оцінка застосовності системи в заданих умовах;

- оцінка масштабованості системи;

- вибір обладнання;

- отримання об'єктивних (числових) показників продуктивності системи під час її навантажувальних випробувань або робочої експлуатації;

- збір та зберігання інформації про динаміку продуктивності системи в часі;

- пошук та аналіз «вузьких місць» та оптимізація коду системи;

- збір повної інформації про всі проблеми продуктивності, що є в розрахованій на багато користувачів системі:

- ранжування проблем за рівнем їх впливу на продуктивність системи в цілому;

- надання наскрізної інформації про контекст кожної проблеми всіх рівнях функціонування системи (дії користувача, стек викликів вихідного коду, запити до СУБД).

Загальна схема роботи представлена на рис. 4.10.

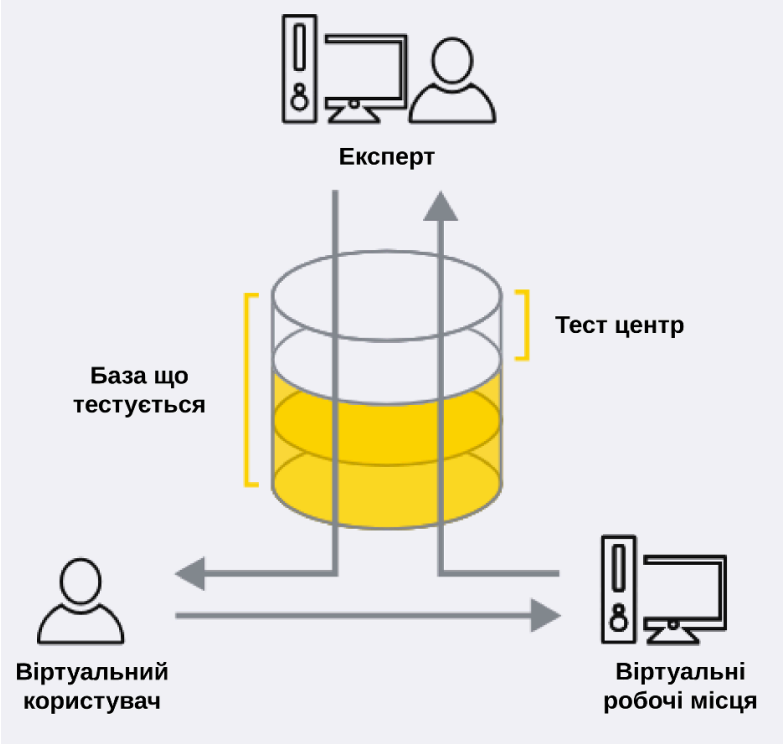

Рисунок 4.10 – Схема роботи 1С: Корпоративного інструментального пакету

Досліджувана інформаційна база – це прикладна система на платформі 1С:Підприємство 8, в якій необхідно провести аналіз продуктивності, а також пошук можливих проблем та вузьких місць з метою подальшої оптимізації.

Навантаження в досліджуваній основі може створюватися Тест-центром (з допомогою сценаріїв тестування) чи справжніми користувачами системи. Експерт за допомогою Тест-центру та «Центру управління продуктивністю» здійснює збір показників продуктивності системи. З отриманих значень він оцінює поточну працездатність системи та наявність у ній проблем продуктивності [22].

Якщо виявлено проблеми продуктивності, то експерт за допомогою ЦУП збирає додаткову (аналітичну) інформацію про «вузькі місця» системи. На підставі цієї інформації та рекомендацій, даних у посібнику з використання "Корпоративного інструментального паркету", експерт може зробити оптимізацію системи, змінивши код конфігурації та/або структуру метаданих [22].

Тест-центр – інструмент автоматизації розрахованих на багато користувачів навантажувальних випробувань інформаційних систем на платформі 1С:Підприємство 8. З його допомогою можна моделювати роботу підприємства без участі реальних користувачів [22].

«Центр управління продуктивністю» (ЦУП) – інструмент моніторингу та аналізу продуктивності інформаційних систем на платформі 1С:Підприємство 8.ЦУП призначений для оцінки продуктивності системи, збору детальної технічної інформації про наявні «вузькі місця» та аналізу цієї інформації з метою подальшої оптимізації [22].

За допомогою тест-центру проводилося навантаження на сервер 1С: Підприємства з 10 віртуальними користувачами, статистика збиралася за допомогою Центру управління продуктивністю.

4.7 Результати тестування платформи 1С Підприємство 8.1

Для вибору мережної ОС та СУБД в умовах роботи безлічі клієнтів з сервером «1С Підприємство 8.1» необхідно отримати як кількісну оцінку продуктивності від типу використовуваної мережної ОС, кількості віддалених клієнтів, так і оцінку масштабованості платформи 1С Підприємство 8.1.

Для вирішення поставленої задачі зробимо обчислювальний експеримент, використовуючи пакет 1С Корпоративний інструментальний пакет і тест TCP-1 C-GILV-A для 10 віддалених віртуальних користувачів і альтернативних варіантів мережевих ОС.

Результати тестування для варіанта використовуваних ОС представлені:

- для Windows Server 2008+Ms SQLserver 2008 на рис.4.11 та таблиця 4.4;
- для Ubuntu + PostgreSQL на рис.4.12 та таблиця 4.5.

Результати другого тесту для варіанту використовуваних ОС представлені:

- для Windows Server 2008+Ms SQLserver 2008 рис.4.13 ;
- для Ubuntu + PostgreSQL на рис.4.14.

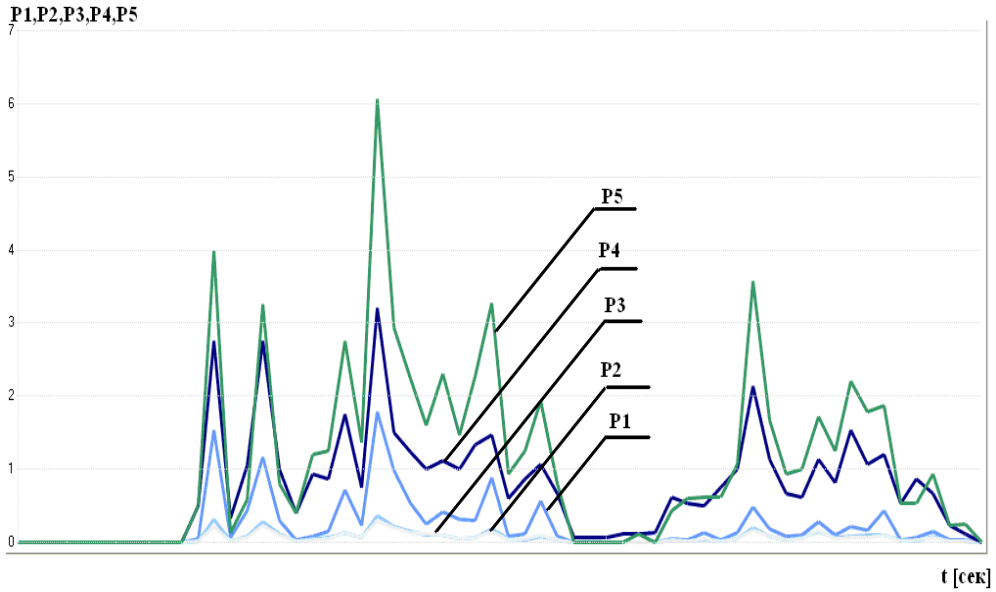

Рисунок 4.11 - Продуктивність технологічної платформи для Windows Server 2008+Ms SQLserver 2008

1С Підприємство на сервері Windows 2008

Прив'язка позначень функцій P1, P2, P3, P4, P5 до їхньої смислової назви представлені в таблиці 3.4.

Таблиця 4.4 - Зведена таблиця значень для сервера Windows 2008, отриманих при тестуванні ЦУП

Показник продуктивності	Одиниця	Середнє	Максимум	Сума
Сумарний час виконання запиту, P1	Сік.	0.231	1.791	13.879
Максимальний час виконання запиту, P2	Сік.	0.063	0.359	3.772
Середній час виконання запиту, P3	Сік.	0.057	0.294	3.430
Кількість запитів, що виконуються, P4	Шт.	0.748	3.200	44.903
Сумарний час очікування на блокування СУБД та 1С, P5	Сік	1.088	6.067	65.268

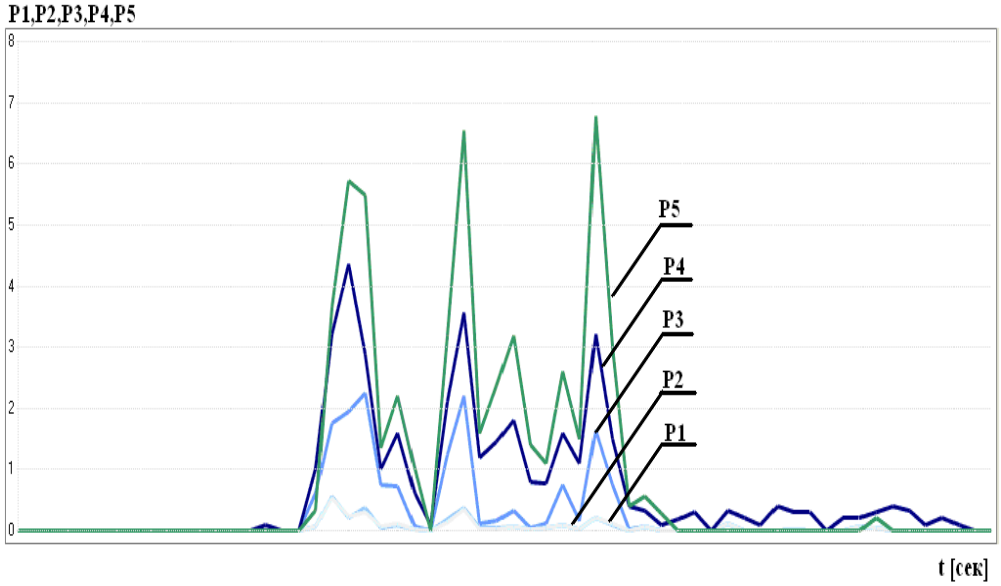

Рисунок 4.12 - Продуктивність технологічної платформи для Ubuntu + PostgreSQL

1С Підприємство на сервері Ubuntu

Прив'язка позначень функцій P1, P2, P3, P4, P5 до їхньої смислової назви представлені в таблиці 4.5.

Таблиця 4.5 - Зведена таблиця значень для сервера Ubuntu, отриманих при тестуванні ЦУП

Показник продуктивності	Одиниця	Середнє	Максимум	Сума
Сумарний час виконання запиту, Р 1	Сік.	0.267	2.251	17.879
Максимальний час виконання запиту, Р 2	Сік.	0.0 50	0. 564	3.943
Середній час виконання запиту, Р 3	Сік.	0.0 71	0. 539	3.542
Кількість запитів, що виконуються, Р 4	Шт.	0. 6 48	4 . 364	50.012
Сумарний час очікування на блокуваннях СУБД та 1, Р 5С	Сік	1. 304	6. 778	67.328

Тестування за допомогою TPC-1C-GILV-A

Тест відноситься до розділу універсальних інтегральних кроссплатформенних тестів. Навіть більше того, він застосовується для файлового та клієнт-серверного варіантів експлуатації 1С:Підприємство. Тест працює всім СУБД, підтримуваних 1С. Як результат, отримуємо певний індекс продуктивності (швидкості). Не важливо, добрий чи поганий результат – це результат роботи платформи на нашому сервері. Даний тест, виконаний на конкретному сервері, дає результат із сукупності налаштувань hardware, операційної системи, СУБД і т.д. Проте високий результат на конкретному серверному обладнанні означає, що за дотримання нормальних умов такий самий результат буде на ідентичному серверному обладнанні [22].

Результати тестування представлено на рис. 4.13, 4.14.

На підставі отриманих тестових результатів можна з упевненістю сказати, що для використання платформи 1С Підприємства 8.1 і для реалізації клієнт-серверної технології, найкраще використовувати її у зв'язці з сервером Windows Server 2008 і СУБД MSSQLserver 2008. Так як за результатами двох тестів ця ОС показала найкращу продуктивність і масштабованість в умовах нашої мультисервісної корпоративної мережі.

Для використання сервера Ubuntu і СУБД PostgreSQL для клієнт-серверної технологій 1С Підприємство 8.1 сервер потребує професійного налаштування як самої операційної системи, так і СУБД PostgreSQL.Це пов’язано з тим, що технологічна платформа 1С Підприємство 8.1 спочатку

розроблялася, і було оптимізовано до роботи з Windows Server 2003 і СУБД MS SQLServer.

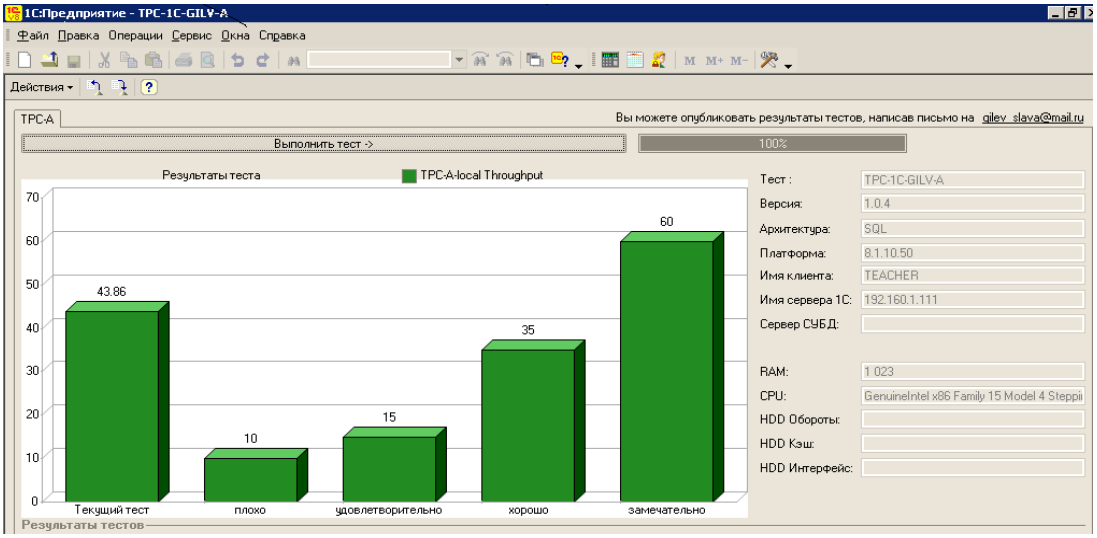

Рисунок 4.13 - Показник продуктивності технологічної платформи 1С Підприємство 8.1 на сервері Windows 2008 в результаті застосування тесту TPC -1C-GILV-A

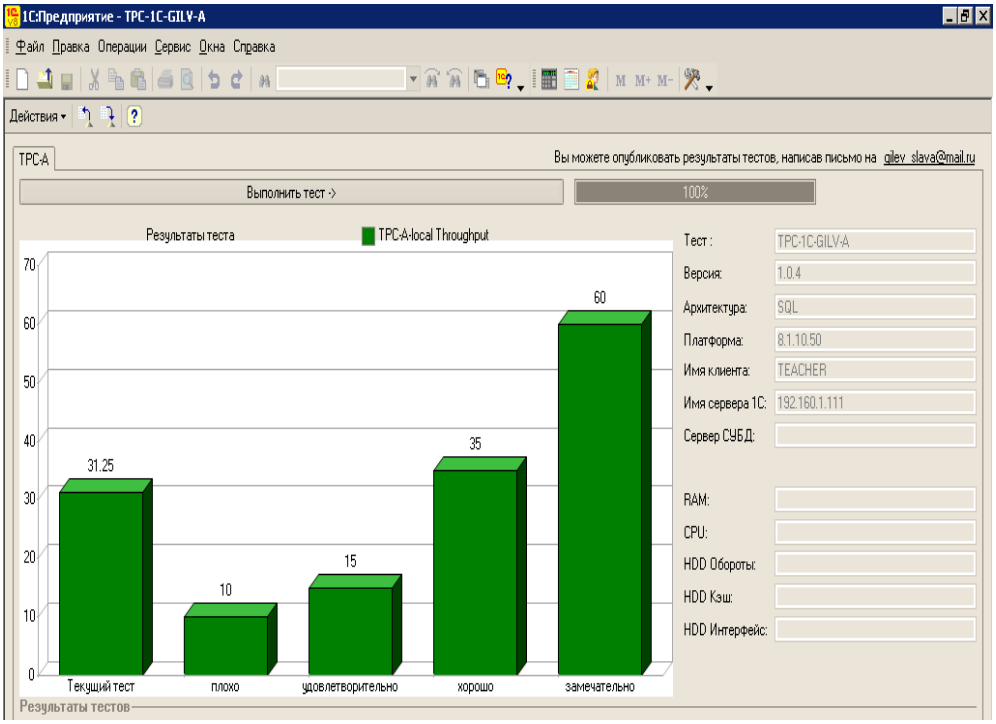

Рисунок 4.14 - Показник продуктивності технологічної платформи 1С Підприємство 8.1 на сервері Ubuntu в результаті застосування тесту TPC-1C-GILV-A

ВИСНОВКИ

На основі чинного для готельного комплексу документообігу та у відповідності до вимог щодо надання клієнтам мультисервісних послуг, була виконана задача: організувати на базі IP-технології кампусну мультисервісну мережу.

Проаналізовано сучасні стандарти технології Ethernet, операційні системи, що використовуються при організації мультисервісних мереж, та загальні принципи побудови логічної й фізичної інфраструктури мультисервісної мережі готельного комплексу. За результатами аналізу:

– вибрана конфігурація зв'язків між комп’ютерами «ієрархічна зірка»;

– запропонована трирівнева модель клієнт-серверної архітектури для організації взаємодії між робочими станціями;

– вибрані операційні системи Microsoft Windows Server та Linux Ubuntu для забезпечення інформаційних сервісів та мультисервісних послуг, які характерні сучасному готельному комплексу;

– показано, що технології Ethernet і Wi-Fi задовольняють вимогам політики управління якістю, які пред'являються мультисервісними мережами при їх реалізації на базі локальних обчислювальних мереж.

Спроектовані логічна та фізична інфраструктури МСМ готелю. Проведена логічна сегментація мережі на основі технології VLAN, а фізична сегментація за функціональною ознакою. Зроблено вибір необхідного обладнання. У відповідності до вимог, що висуваються до серверів з заданими інформаційними сервісами, розрахована необхідна продуктивність і об'єм оперативної і дискової пам'яті серверів. Проведено вибір серверного обладнання та визначена його остаточна конфігурація.

Використовуючи середовище програми Interpret Air, змодельована карта зон покриття точок бездротового доступу в типових приміщеннях готельного корпусу. Проведено моделювання та визначено місця встановлення точок доступу та їх кількість, яка співпала з вимогами чинного завдання.

Проаналізовано протоколи технології VPN для захисту даних при передачі у мережі. В результаті проведеного дослідження було побудовано аналітичну функцію відгуку для моделювання та оцінки продуктивності

пропускної спроможності корпоративної мережі із захищеним каналом. Протестовано один із найпопулярніших алгоритмів шифрування з різними параметрами та з двома різними операційними системами та проведено оцінку їхньої продуктивності. Отримано набори оптимальних конфігурацій для побудови захищених каналів корпоративних мереж. За підсумками тестування можна зробити висновок що найбільш продуктивною та модельованою серверною операційною системою є Windows Server 2008 і СУБД MSSQLserver 2008.

Проведено тестування технологічної платформи 1С Підприємство з двома різними серверними операційними системами та СУБД. За результатами тестування можна дійти висновку про найбільш продуктивну серверну операційну систему, що найкраще підходить для реалізації клієнт–серверної технології з урахуванням технологічної платформи 1С Підприємство 8.1.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Бобылева М. П. Корпоративные информационные системы и технологии электронного документооборота: новый потенциал управленческой интеграции. // Деньги и кредит. – 2007. – № 12. – С. 60 – 67.

2. Волков С.Л. Мультисервисные сети AMP Netconnect: Учебное пособие к дипломному проектированию - Одесса: МГУ, 2007. – 36 с.

3. Козленко В. ИТ-инфраструктура гостиниц. Телеком. Коммуникации и Сети, 2008, №10, [Електронний ресурс] – Режим доступу: http://www.dynamix.ua/news/press/ 2008/ telekom-10-08-1.htm

4. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. – СПб.: БХВ-Питербург, 2007. – 592 с.

5. Бакланов И.Г. NGN: принципы построения и организация / Под ред. Ю.Н. Чернышова. – М.: Эко-трендз, 2008 – 400 с.

6. Pathan A. S. K. (ed.). 2010. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 638.

7. Технология Wi-Fi. [Електронний ресурс] – Режим доступу: www.wifi.org.ua

8. Величко В.В. Телекоммуникационные системы и сети: Учебное пособие. В 3-х томах. Том 3. – Мультисервисные сети //В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев. – М.: Горячая линия-Телеком, 2005. – 592 с.

9. Intel. [Електронний ресурс] – Режим доступу: www.intel.com

10. Zyxel.[Електронний ресурс] – Режим доступу: www.zyxel.com

11. Dlink. [Електронний ресурс] – Режим доступу: www.dlink.com

12. Cisco. [Електронний ресурс] – Режим доступу: www.cisco.com

13. Itc. [Електронний ресурс] – Режим доступу: www.itc.ua

14. 1С: Предприятие. [Електронний ресурс] – Режим доступу: www.1C.ru

15. Novell. [Електронний ресурс] – Режим доступу: www.novell.com

16. HP. [Електронний ресурс] – Режим доступу: www.hp.com

17. A. InterpretAir. Программное обеспечение для исследования WLAN. [Електронний ресурс] – Режим доступу: www.flukenetworks.com/interpretair

18. Строгалев В. П. Толкачева И. О. Имитационное моделирование. - МГТУ им. Баумана, 2008. – С. 697-737.

19. W. Stallings Cryptography and Network Security: Principles and Practice (Second Edition). – Prentice Hall Upper Saddle River, New Jersey 07458 – 569 с.

20. А.В. Соколов, В.Ф.Шаньгин. Защита информации в распределенных корпоративных сетях и системах. – М.:ДМК Пресс, 2002. – 656с.

21. Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. Handbook of Applied Cryptography. — CRC Press, October 1996. ISBN 0-8493-8523-7

22. А. Г. Ивахненко, Ю. П. Юрачковский Моделирование сложных систем по экспериментальным данным. — М.: «Радио и связь», 1987. -120с.

23. Ананий В. Левитин Глава 3. Метод грубой силы: Задача о рюкзаке // Алгоритмы: введение в разработку и анализ = Introduction to The Design and Analysis of Aigorithms. — М.: «Вильямс», 2006. — С. 160-163. — ISBN 0-201-74395-7