МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Клівіцький Роман Ярославович

Програмний засіб планування трафіку комп'ютерної мережі / The software for computer network traffic planning

напрям підготовки: 6.050102 - Комп’ютерна інженерія
фахове спрямування - Комп’ютерні системи та мережі
Бакалаврська робота

Виконав: студент групи КСМзкп-41/2
фахового спрямування комп’ютерні системи та мережі
Клівіцький Роман Ярославович

Науковий керівник:
Мельник Г.М.

Тернопіль - 2018

РЕЗЮМЕ

Бакалаврська робота містить 69 сторінок пояснюючої записки, 8 рисунків, 4 таблиці, 2 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою дипломного проекту є розробка програмного засобу для планування трафіку комп'ютерної мережі.

Дослідження систем моніторингу трафіка показало, що існуючі підходи по плануванню трафіка комп'ютерної мережі не враховують вплив загроз.

Формалізовано методику розрахунку параметрів трафіку. В основі розрахунків трафіку комп'ютерної мережі лежать імовірнісні характеристики потоку даних, які генеруються різними мережними пристроями. Для виконання розрахунків необхідно мати інформацію про приблизну структуру мережі, кількість абонентів у кожному вузлі мережі, розподіл абонентів по різних класах обслуговування, перелік мережних послуг. Трафік розраховується окремо для кожного виду послуги на кожному мережному вузлі. Розроблене програмне забезпечення розраховує пропускну здатність каналів зв'язку та затримку передачі пакетів.

Розроблено програмне забезпечення розрахунку трафіку та аналізу існуючого трафіку. Розроблювальна система складається з таких компонентів: модуль розрахунку параметрів трафіку, модуль збору даних у мережному сегменті, база даних, модулі аналізу зібраних даних і виводу інформації.

В якості інструментальних засобів розроблення обрано мову C++ та бібліотеку розроблення графічних інтерфейсів Qt. Розроблено графічний інтерфейс програмного засобу. Система пройшла тестування й може виконувати поставлені їй задачі.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, ПЛАНУВАННЯ, OSI.

RESUME

Bachelor thesis contains 69 pages of text, 8 figures, 4 tables, 2 appendixes. The amount of graphic material is 2 sheets of A3 format.

The purpose of bachelor thesis is to develop a software tool for planning computer network traffic.

The research of traffic monitoring systems has shown that existing approaches to planning a computer network traffic do not take into account the impact of threats.

Formalized method of calculating traffic parameters. The basis of computer network traffic calculations are the probabilistic characteristics of the data flow generated by different network devices. To perform the calculations it is necessary to have information about the approximate structure of the network, the number of subscribers in each node of the network, the distribution of subscribers in different classes of service, a list of network services. The traffic is calculated separately for each type of service on each network node. The developed software calculates the bandwidth of the communication channels and delays in the transmission of packets.

Software for calculating traffic and analysis of existing traffic has been developed. The development system consists of the following components: a module for calculating traffic parameters, module for data collection in a network segment, a database, modules for analyzing collected data and output information.

As a development tool, the C ++ language and the Qt graphical interfaces development library are selected. The graphical interface of the software is developed. The system has been tested and can perform its tasks.

Keywords: COMPUTER NETWORK, PLANNING, OSI.

ЗМІСТ

					ДП.КСМ.111256/17.00.00.000 ПЗ		
Змн.	Лист	№ докум.	Підпис	Дата			
Розробив		Клівіцький Р.Я.			ПРОГРАМНИЙ ЗАСІБ ДЛЯ ПЛАНУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ	Літ.	Арк. 7 / Акрушів
Перевір.		Мельник Г.М.					
Консульт.		Паздрій І.Р.				ТНЕУ.ФКІТ. КСМзкп-41/2	
Н. Контр.		Мельник Г.М..					
Затвердив		Березький О.М.					

ВСТУП

Стрімкий розвиток телекомунікаційної галузі втягує в цей вид діяльності значні матеріальні й людські ресурси. Різко збільшується обсяг надаваних послуг, зростають вимоги до якості транспорту даних. Робота великих розподілених корпорацій, таких, наприклад, як банки, торговельні мережі, страхові компанії й інших неможлива без надійно працюючих мереж передачі й обробки даних.

У той же час у зв'язку зі збільшенням кількості й різноманітності надаваних послуг різко збільшуються вимоги до обсягу і якості транспорту даних, що найчастіше приводить до невиправдано високих витрат на побудову мереж. При побудові мереж великих корпорацій необхідно враховувати різноманітні джерела трафіка – такі, як трафік бази даних, файловий документообіг, IP-Телефонію й IP-відеозв'язок, і багато інших. Кожний вид трафіка висуває свої вимоги до якості транспорту й показникам пропускної здатності. Тому актуальним є розроблення засобів для проектування мереж з урахуванням показників якості обслуговування.

Метою дипломного проекту є розробка програмного засобу для планування трафіку комп'ютерної мережі. Для досягнення мети потрібно розв’язати наступні задачі:

- проаналізувати основні етапи планування трафіку;
- проаналізувати вплив мережевих загроз на трафік;
- формалізувати методику розрахунку параметрів трафіку;
- розробити та реалізувати програмне забезпечення для розрахунку параметрів трафіку;
- протестувати розроблене програмне забезпечення.

1 ЗАДАЧА ПЛАНУВАННЯ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Планування трафіку

Планування мережі – це процес визначення задач (аналіз вимог) які буде вирішувати КМ. Результат – логічна структура мережі з врахуванням майбутнього кількісного та якісного розширення.

При сучасних темпах розвитку мережних технологій корпоративні мережі постійно перебувають у стані трансформації, як через впровадження нових задач, так і у зв'язку з ростом розмірів мережі й кількості користувачів. У таких умовах стає проблематично визначити, як надалі вдосконалювати мережну інфраструктуру, і є чи в цьому необхідність.

Створення корпоративної мережі (або її модернізація) починається з етапу планування, на якому визначаються задачі, які буде вирішувати мережа, складається логічна структура мережі з урахуванням подальшого росту, як кількісного, так і якісного. Не можна побудувати (модернізувати) гарну корпоративну мережу без ясного розуміння всіх цілей підприємства, без чіткого плану досягнення цих цілей. Якщо модернізується існуюча мережна інфраструктура, то етапу планування повинно передувати проведення аудиту мережі. Це необхідно для раціонального використання наявних ресурсів і приведення мережної інфраструктури у відповідність поточним задачам бізнесу.

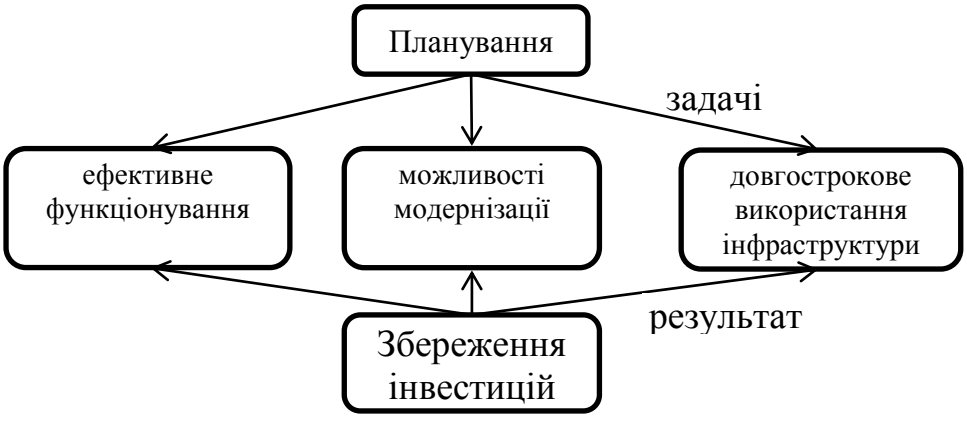

Рисунок 1.1 - Планування мережі

При проведенні аудита мережі необхідно:

– зібрати потрібну інформацію й проаналізувати поточний стан мережі і її компонентів, що дозволить виявити проблеми, що вимагають рішення;

– підготувати документацію, потрібну для експлуатації мережі;

– визначити можливості модернізації мережі й оцінити вигоди від її проведення.

Досвід проведення робіт з аудита мереж свідчить про те, що задача аудита носить не тільки технічний характер: результатом аудита є виявлення технічних і технологічних (експлуатаційних) проблем, що виявляють негативний вплив на бізнеси-процеси. Задачі бізнесу із часом можуть змінюватися, а мережна інфраструктура піддається змінам постійно. Тому доцільним є періодичне проведення аудита, незалежно від того, чи бідує мережа в модернізації.

На підставі робіт, проведених на етапі планування, виконується проектування корпоративної мережі: визначається її фізична конфігурація. Реалізація проекту полягає в побудові мережі й накладенні на фізичну інфраструктуру логічної схеми функціонування, визначеної при плануванні.

У процесі експлуатації мережі часто виникає необхідність робити які-небудь незначні зміни або впроваджувати прикладні системи. У міру нагромадження такого роду змін корпоративна мережа перестає відповідати тому, що було описано в документації, складеній при введенні мережі в експлуатацію. У результаті мережа перестає функціонувати в оптимальному режимі, часто можуть виникати які-небудь аварійні ситуації. Впровадження деяких прикладних задач або збільшення кількості користувачів мережі можуть зажадати архітектурних змін. Це визначає необхідність модернізації, яка починається із проведення аудита корпоративної мережі.

Таким чином, життєвий цикл корпоративної мережі, проілюстрований на рис. 2, складається з наступних етапів:

– планування корпоративної ЛОМ;

– проектування;

- реалізації проекту;
- періоду експлуатації мережі;
- модернізація.

Сучасні корпоративні мережі потребують періодичної модернізації як для розв'язку знову виникаючих задач, так і для підтримки інфраструктури в працездатному стані.

Традиційні вимоги, які пред'являють користувачі до сучасних корпоративних мереж наступні:

- висока продуктивність;
- висока доступність мережних ресурсів і служб;
- забезпечення необхідного рівня безпеки;
- можливість керування ресурсами.

1.2 Розрахунок швидкості передачі даних та кількості підмереж

Топологія інформаційної мережі – напрямок потоків між активними й пасивними вузлами (включаючи кінцеве обладнання), а також швидкість передачі інформації з них. Топологія фізичної мережі – схема розташування кінцевого встаткування, серверів, точок бездротового доступу, маршрути прокладки кабельних трас і структура бездротових мереж. Топологія інформаційної мережі створюється на основі інформації про три її складових:

- величина максимального потоку, створюваного всіма вузлами системи;
- величина максимального потоку, який здатна транслювати мережа (пропускна здатність);
- величина максимального потоку на один порт, який здатне забезпечити мережне встаткування.

Проектування мережі починають зі знаходження максимальних інформаційних потоків, створюваних усіма вузлами системи. Результуюче

значення потоку від кожного вузла залежить від величини трафіку, що створюється програмами та функції трафіку в часі.

Знаходження сумарного значення максимальних інформаційних потоків на початковому етапі проектування дозволяє:

– визначити кількість інформаційних підмереж, за допомогою яких можна передати весь об'єм інформації від вузлів до сервера (серверів) або через канал в інтернет;

– розробити структуру й склад інформаційної підмережі.

Основні етапи розрахунків.

1. Визначення загальної швидкості інформаційного потоку. Для визначення швидкості інформаційного потоку від кожного вузла можна використовувати калькулятори або програми симуляціх роботи мережі OPNEt IT Guru. Сумарна швидкість інформаційних потоків від усіх вузлів

$$B=\sum_{i=1}^{n}\sum_{j=1}^{k}V(i,j), \qquad (1.1)$$

де: B- сумарна швидкість потоків від усіх вузлів;

$V(i, j)$– швидкість j-го «потоку» від і-го вузла;

k - загальна кількість «потоків», переданих вузлами;

n – загальна кількість вузлів.

Термін «потоки», використовуваний у меню IP-камер для завдання характеристик додатковим потокам і вибору їх кількості, візьмемо в лапки. Пов’язано це з тим, що від камери йде всього один цифровий потік. При формуванні цього потоку інформація про основний і додаткові «потоки» буде перетворюватися в пакети зі своїми адресами доставки. І вже ці пакети в загальному інформаційному потоці передаються по мережі.

Для збільшення надійності роботи мережі, у частині запобігання непередбачених перевантажень від зміни інтенсивності руху перед вузлами, доцільно значення швидкості потоку збільшити на 25-30 %.

$$B_{max} = 1{,}3 \cdot B. \quad (1.2)$$

2. Вибір пропускної здатності мережі. Пропускна здатність мережі визначається обраним середовищем передачі сигналу. У якості середовища передачі сигналу використовуються різні види кабелів: коаксіальний кабель, кабель на основі екранованої й неекранованої витої пари й оптоволоконний кабель. Найбільш популярним видом середовища передачі даних на невеликі відстані (до 100 м) стає неекранована вита пари (UTP), яка включена практично в усі сучасні стандарти й технології локальних мереж і забезпечує пропускну здатність до 100 Мбіт/с. Екранована кручена пари (STP категорії 6) дозволяє побільшати пропускну здатність до 1000 Мбіт/с.

Оптоволоконний кабель широко застосовується як для побудови локальних зв'язків, так і для утвору магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох Тбіт/с) і передачу на значні відстані (до декількох десятків кілометрів без проміжного посилення сигналу).

3. Визначення кількості інформаційних підмереж. Виходячи із сумарної швидкості інформаційного потоку від усіх вузлів (B_{max}) обраної пропускної здатності мережі (W), можна визначити кількість інформаційних підмереж, які необхідно створити. Така кількість підмереж забезпечить доставку даних від вузлів до сервера без видимих затримок.

$$M = B_{max} /(0{,}8 \cdot W), \quad (1.3)$$

де M - кількість підмереж;

B_{max} – сумарна швидкість потоків від усіх вузлів;

W- пропускна здатність мережі;

0,8- коефіцієнт, що характеризує максимально припустиму завантаження мережі (80%).

Наприклад:

– мережа побудована на кабелі кручена пари UTP Cat.6 максимальну швидкістю, що забезпечує, передачі W = 1 Гбіт/с;

– сумарна швидкість потоку від усіх вузлів B_{max}=4 Гбіт/с;

– отже, для розв'язку задачі потрібно створювати 5 підмереж. 4 Гбіт/с / (0,8·1Гбіт/с) = 5

4. Визначення максимального потоку на один порт, який здатне забезпечити мережне встаткування. Розв'язок цієї задачі має дуже багато варіантів, але, разом з тим, існують основні принципи розподілу потоків і знаходження результуючих швидкостей на ділянках мережі, які ми розглянемо. При побудові мережі використовується активне встаткування, призначене для поділу/об'єднання потоків від вузлів до сервера (серверів). Поділ/об'єднання потоків здійснюють комутатори. Максимальне завантаження порту комутатора визначена в його технічних характеристиках. При завантаженні всіх портів комутатора загальний інформаційний потік не повинен перевищувати значення максимальної пропускної здатності комутатора. Для виконання цієї умови потрібно визначити максимально припустиму швидкість потоку на кожний порт. При використанні простого комутатора в мережі, коли до всіх портів крім одного підключені вузла, а порт, що залишився, підключений до іншого комутатора (комутатор № 2), максимальний припустимий потік на один порт визначається як:

$$V_2 = V_1 /[2(N – 1)]. \quad (1.4)$$

Якщо порт, що залишився, підключений до магістралі (комутатор № 1), то максимальний припустимий потік на порт визначається як:

$$V_1 = 0{,}8 \cdot W /[2(N – 1)], \quad (1.5)$$

де $V_{1(2)}$ – максимальна швидкість для одного порту комутатора №1;

N - загальна кількість портів;

W - пропускна здатність мережі (Мбіт/с);

0,8- коефіцієнт, що характеризує максимально припустиму завантаження мережі (80 %).

Якщо задіяти в комутаторі комбопорт, максимальна швидкість через кожний порт може бути визначена в такий спосіб:

$$V = 0,8 \cdot W/N, \quad (1.6)$$

де *V* - максимальна швидкість для одного порту (Мбіт/с);

W - пропускна здатність мережі (Мбіт/с);

N - загальна кількість портів.

Не слід забувати, що розрахункове значення швидкості потоку через порт не повинне перевищувати значення цього ж параметра в паспорті комутатора.

З вищесказаного випливає, що вузол повинен бути настроєний таким чином, щоб її потік не перевищував розрахункове значення швидкості потоку через порт комутатора, до якого вона буде підключена.

1.3 Вплив загроз на трафік та засоби аналізу трафіку

Розглянемо протокол IP версії 4 як найпоширеніший. Специфікація протоколу IP визначається документом RFC 791. Протокол IP обмежується доставкою бітових пакетів (дейтаграм) від відправника до одержувача через систему з'єднаних між собою мереж. Протокол не підтримує механізмів підвищення надійності наскрізної доставки, керування потоком даних, збереження порядку й інших функцій, загальноприйнятих для протоколів прямої взаємодії між хостами. Протокол IP використовує послуги підтримуючих цей протокол мереж для надання послуг різного типу й з різною якістю [4]. У багаторівневій моделі протокол TCP розташовується безпосередньо над базовим протоколом IP, який забезпечує для TCP

можливість приймання й передачі сегментів інформації змінної довжини, "вкладених" у дейтаграми. Дейтаграми забезпечують спосіб адресації відправника й одержувача TCP, розташованих у різних мережах. Згідно RFC 793 протокол TCP повинен відновлювати дані у випадку їх ушкодження, втрати, дублювання або доставки з порушенням порядку. Це забезпечується за допомогою порядкових номерів, що надаються кожному переданому октету й підтвердженням доставки даних (ACK - acknowledgment), переданим прийомною стороною TCP. Якщо підтвердження ACK не було отримано протягом заданого часу (тайм-аут), дані передаються заново.

Розглянемо основні види мережних атак. Прослуховування. Впровадження в інформаційну систему й перехоплення трафіка для подальшого аналізу, розшифрування й вичленовування корисної для зловмисника інформації. Найбільш уразливі для такого виду атаки відкриті Wi-Fi мережі, мережі Ethernet а також телефонні й комутовані лінії даній атаці піддаються менше через необхідність фізичного доступу до даних мереж.

Неправильні ARP-Відповіді. Різновид атаки «людей посередині». Застосовується в основному в мережах Ethernet. Атака можлива через уразливість у протоколі ARP, який не перевіряє дійсність ARP-Запитів і відповідей. Зловмисник відсилає два ARP відповіді до вузлів мережі, чий трафік він збирається перехопити, підмінюючи MAC адреса адресата на свій власний. Після одержання такого Arp-Відповіді жертви змінять свої ARP таблиці й тепер усі пакети між двома вузлами почнуть проходити через комп'ютер зловмисника.

Відмова в обслуговуванні DoS (Denial of Service) - хакерська атака на мережу, ціль якої довести систему до стану припинення обслуговування легальних користувачів. При поточному стані обчислювальних мереж одиночна DoS атака, як правило, не може нанести серйозного збитку й з високою часткою ймовірності буде відфільтрована обчислювальною системою, що служить предметом атаки.

Більш серйозну небезпеку представляють розподілені DoS атаки - DdoS (Distributed Denial of Service). Така атака проводиться одночасно з великої

кількості комп'ютерів. Для проведення такої атаки зловмисникові потрібно набрати достатню кількість комп'ютер-зомбі. Для цього зловмисник установлює спеціальне програмне забезпечення (троянські програми) на вразливі комп'ютери, що мають доступ у мережу. Як правило, дане програмне забезпечення працює у фоновому режимі й користувач зараженого комп'ютера навіть не підозрює, що є учасником атаки.

При ping флуді насичення смуги пропущення відбувається за рахунок звичайних ping-запитів. У загальному виді суть методу в тому, що ICMP exo запит, відправлений на адресу сервера, вимагає від пристрою прийняття, а також обробки запиту, а потім формування й відправлення відповіді на нього, обсяг дій у даній ситуації перевищує обсяг при маршрутизації звичайного пакета, у результаті при постійній необхідності обробляти луна-запити може виникнути перевантаження по кількості пакетів і віддалений сервер почне втрачати інші пакети, що й викличе відмову в обслуговуванні. Але такий вид атаки працює тільки в тому випадку, коли пропускна смуга атакуючого комп'ютера набагато ширше, чим канал, що атакується, що свідчить про практичну марність при атаці потужного сервера із широким каналом.

Атака HTTP-Флуд ефективний при атаці на сервер. Зміст атаки полягає в тому, що атакуючий комп'ютер відправляє маленький за обсягом пакет, але сформований таким чином, що сервер повинен відповісти на нього пакетом у сотні раз більше, атакуючи з величезного числа машин, шанс наситити пропускну смугу суттєво вище, чим при стандартному ping- флуді. Для того, щоб HTTP-пакети не викликали відмову в обслуговуванні в атакуючої машини - відбувається підміна своєї IP-адреси на IP-адресу вузлів у мережі, тим самим, пакети вертаються на інші пристрої [9].

Атака SYN-флуд базується на відправленні на протязі короткого проміжку часу великої кількості запитів на встановлення з'єднання по протоколу TCP - SYN-Запитів [10]. Згідно зі стандартом клієнт відправляє пакет із установленим прапором SYN, а у відповідь сервер відправляє комбінацію прапорців SYN+ACK, на який клієнтом повинен бути відправлений пакет із прапором ACK, після цього “троєкратного рукостискання” з'єднання

буде вважатися встановленим. Суть атаки в наступному: зловмисник відправляє жертві SYN запити й переповняє на сервері черга підключення, а відповідні SYN+ACK пакети будуть зігноровані або заголовок пакета підробляється так, що відповідний пакет відправляється на неіснуючу адресу, у черзі утворюються «напіввідчинені з'єднання», що очікують відповіді від клієнта адже за замовчуванням кожне «напіввідчинене» з'єднання скидається тільки по закінченню 3 хвилин [11]. SYN-Пакети відправляються постійно, що підтримує чергу з «напіввідчинених» з'єднань і не дає можливості добропорядним клієнтам здійснити підключення. Зараз даний вид атаки втратив свою актуальність тому що введене в повсюдне застосування SYN cookie.

Більшість із розглянутих загроз проявляються в аномаліях мережного трафіка, хоч і аномалії можуть бути зв'язані не тільки з діяльністю зловмисників, а мати зовсім інші причини, такі як: збій у роботі програмного забезпечення, дефект апаратури, невірні дії користувача системи, але в кожному разі, адміністратор інформаційної системи повинен обертати уваги на подібні події, які можуть бути індикатором порушення безпеки.

1.4 Постановка задач дипломного проекту

Метою дипломного проекту є розробка програмного засобу для планування трафіку комп'ютерної мережі. Для досягнення мети потрібно розв’язати наступні задачі:

– проаналізувати основні етапи планування трафіку та вплив мережевих загроз на трафік;

– формалізувати методику розрахунку параметрів трафіку;

– розробити та реалізувати програмне забезпечення для розрахунку параметрів трафіку;

– протестувати розроблене програмне забезпечення.

2 МЕТОДИКА ПЛАНУВАННЯ ТРАФІКУ КОМПЮТЕРНОЇ МЕРЕЖІ

2.1 Розрахунок параметрів трафіку комп’ютерної мережі

В основі розрахунків лежать імовірнісні характеристики потоку даних, які генеруються різними мережними пристроями. Для використання даної методики необхідно мати інформацію про:

- приблизну структуру мережі;
- кількість абонентів у кожному вузлі мережі;
- розподіл абонентів по різних класах обслуговування;
- перелік мережних послуг;
- характеристики послуг.

Трафік розраховується окремо для кожного виду послуги на кожному мережному вузлі. Формула для розрахунків має вигляд:

$$Y_i^{(k)} = B_{порівн}^{(k)} * N_{аб.\,i}^{(k)} * T_c^{(k)} * f_{викл.\,i}^{(k)},$$

де k - номер мережної послуги;

i - номер вузла;

$Y_i^{(k)}$ - математичне очікування трафіка, який генерується k-ою послугою на i-ому вузлі;

$B_{порівн}^{(k)}$ - швидкість передачі даних (у бітах на секунду);

$N_{аб.i}^{(k)}$ - кількість абонентів на i-ому вузлі, які використовують k-у послугу;

$T_c^{(k)}$ - середня тривалість сеансу зв’язку для k -ї послуги;

$f_{викл.\,i}^{(k)}$ - середня кількість викликів у ЧНН для користувачів і-го вузла, які використовують k-у послугу

У свою чергу швидкість передачі даних визначається по формулі:

$$B_{порівн}^{(k)} = (B_{\max}^{(k)}) / (P^{(k)}),$$

де $B_{\max}^{(k)}$ - максимальна пропускна здатність каналу зв’язку;

$P^{(k)}$ – пачковість (burstness) на одного абонента, відношення між максимальною й середньою пропускною здатністю, необхідної для забезпечення *k*-ої послуги.

Сумарний трафік є сумою $Y_i^{(k)}$ для всіх послуг, які генеруються на *i*-ом вузлі.

Навантаження розподіляється на 3 напрямки:

– усередині вузла;

– передається в сусідні вузли;

– передається в зовнішні мережі.

Існує 2 методики розрахунків внутрішнього навантаження й вихідного трафіка.

1. Перший полягає в завданні коефіцієнтів, які показують частку трафіка в кожному напрямку: k_1 - у внутрішню мережу, k_2 - у сусідні вузли, k_3 - в інші мережі. При цьому має місце співвідношення $k_1+k_2+k_3 = 1$.

2. На кожному етапі аналізу мережної послуги визначають які послуги є внутрішніми, які пов'язані із сусідніми вузлами, а які - із зовнішніми мережами. Необхідно врахувати частину службової інформації, яка передається по мережі (це буде відомо після вибору технології й протоколу передачі).

Якщо в мережі є послуги реального часу, то при виборі каналів необхідно, щоб пропускна здатність каналу зв'язку була не менше, ніж необхідна смуга пропущення.

2.2 Алгоритм розрахунків параметрів трафіку

Розглянемо задачу об'єднання декількох каналів в один на прикладі ділянки корпоративної мережі. Як приклад візьмемо регіональну мережу міста

й прилягаючих до нього районів, на основі топології транспортної оптоволоконної мережі оператора зв'язку.

Таблиця 2.1 – Параметри абонентського навантаження для кожного класу послуг

Послуга	Максимальна швидкість Кбіт/с	Тривалість сеансу зв'язку (с)	Кількість викликів у годину	Пачко-вість	Вхідне навантаження Ерланг
Voip	95,2	150	3	1	0,125
Відеоспостереження	1024	3600	1	1	1
Internet	1024	60	10	8	0,167
База даних	512	15	20	5	0,083
Файловий обмін	2048	30	3	10	0,025
Відеоспостереження (банкомат)	384	3600	1	1	1

На основі параметрів абонентського навантаження (таблиця 1), розраховується трафік, створюваний різними класами послуг, а також пропускна здатність отримана методом підсумовування. Варто відзначить що, показники абонентського навантаження загальнодоступні й отримані емпіричним шляхом. У більшість випадок трафік або пропускна здатність розраховується саме цим методом [1]. Результат розрахунків представлено в таблиці 2.2.

Трафік кожного відділення отриманий простим арифметичним підсумовування по всіх послугах, які надаються абонентам цього відділення. А сумарний трафік усього вузла розподілу отриманий простим арифметичним підсумовуванням необхідної пропускної здатності кожного з відділень. Такий спосіб обчислення пропускної здатності не враховує декількох важливих показників, що може привести до помилки в розрахунках як у більшу, так і в меншу сторону. По-перше, чим більше число абонентів створюють трафік, тим він більш рівномірний, тому що малоймовірно, щоб велика кількість абонентів одночасно зажадали обслуговування з максимальною швидкістю. По-друге, пакети від множини абонентів можуть накопичуватися в черзі на передачу, тим самим, трафік вирівнюється ще більше – особливо цей ефект проявляється, коли передається регулярний трафік, наприклад, голосові або відео пакети. З

іншого боку, стояння в черзі викликає затримку передачі пакетів, отже, погіршує показники якості транспорту.

Таблиця 2.2 – Трафік відділень і сумарний трафік

		Пропускна здатність для послуг, Кбіт/с					
Назва об'єкта	Число абонентів	VoIP	Інтернет	База даних	Файлів. обмін	Трафік філії (Кбіт/с)	Сумарн. Трафік (Кбіт/с)
Місто	27	329	576	236	138	1279	10423
Район 1	26	317	555	227	133	1232	
Район 2	24	292	512	210	123	1137	
Район 3	24	292	512	210	123	1137	
Район 4	23	280	491	201	118	1090	
Район 5	22	268	469	192	113	1042	
Район 6	22	268	469	192	113	1042	
Район 7	26	317	555	227	133	1232	
Район 8	26	317	555	227	133	1232	
	Навантаження створюваної групи абонентів, Ерл.						
Назва об'єкта		Voip	Інтернет	База даних	Файлів. обмін		
Місто		3,00	3,86	2,07	0,66		
Район 1		2,89	3,72	1,99	0,63		
Район 2		2,67	3,43	1,84	0,59		
Район 3		2,67	3,43	1,84	0,59		
Район 4		2,56	3,29	1,76	0,56		
Район 5		2,44	3,15	1,69	0,54		
Район 6		2,44	3,15	1,69	0,54		
Район 7		2,89	3,72	1,99	0,63		
Район 8		2,89	3,72	1,99	0,63		

Регулюючи співвідношення між сумарним трафіком усіх відділень і пропускною здатністю об'єднаного каналу від міста до ядра, можна впливати на показники якості. Таким чином, ставиться наступна задача: запропонувати методику розрахунків, що враховує довжину черги так, щоб час стояння пакетів не перевищував допустимий, а пропускна здатність була найменша.

2.3 Розрахунки показників якості транспорту пакетів

Наступним кроком необхідно розрахувати показники якості – а саме, затримку, обумовлену стоянням пакета в черзі й часом, витраченим на

передачу. Оскільки для обслуговування пакетів IP-Телефонії й інших послуг використовуються різні черги, то розрахунки будемо вести окремо, виходячи з типового розміру пакета для кожного виду послуг. Нижче наведений докладний розрахунки для міста, а для інших відділень результати розрахунків зведені в таблицю.

Для телефонії реальний розмір пакета визначений розрахунковим шляхом – 1904 біта. Пропускна здатність каналу – 0,857 Мбіт/с. Отже, час, необхідний для передачі 1 пакета, визначається так:

$$T_s = b_{реальн} / B_{каналу}; \quad T_s = 1904 / 0{,}857 = 2{,}22 \text{ мс}. \tag{2.1}$$

Оскільки розрахункове навантаження абонентської групи рівна $Y_{гр}$=3 Ерланг, а інтервал передачі пакетів кожним абонентом (час семпла) *ts*=20 мс, то інтенсивність передачі пакетів від усієї групи буде розраховано так:

$$\lambda = Y_{гр} / t_s; \quad \lambda = \frac{3}{20 \cdot 10^{-3}} = 150 \text{ пак/с}. \tag{2.2}$$

Звідки визначаємо коефіцієнт утилізації показник завантаженості каналу зв'язку, який впливає на час стояння в черзі:

$$\rho = \lambda \cdot T_s; \quad \rho = 150 \cdot 2{,}22 \cdot 10^{-3} = 0{,}333. \tag{2.3}$$

З нього, згідно [3], враховуючи той факт, що всі пакети телефонії мають однаковий розмір, визначаються наступні показники якості. Загальне число пакетів *r*, що перебувають у системі:

$$r = \frac{\rho^2}{2 \cdot (1 - \rho)} + \rho; \quad r = \frac{0{,}333^2}{2 \cdot (1 - 0{,}333)} + 0{,}333 = 0{,}417. \tag{2.4}$$

З них у черзі на обслуговування перебувають *w* пакетів:

$$w = \frac{\rho^2}{2 \cdot (1-\rho)}; \quad w = \frac{0{,}333^2}{2 \cdot (1-0{,}333)} = 0{,}0833. \qquad (2.5)$$

Ця цифра може бути корисною при настроюванні черг на устаткуванні – в апаратурі можна вказувати максимальний розмір черги пакетів. У цьому випадку в системі на обслуговуванні менше 1 пакета, значення достатнє умовне; воно свідчить про те, що система працює з більшим запасом по продуктивності. Але при подальшій оптимізації ця цифра буде вже набагато більш реальна.

Час стояння пакетів у черзі T_w:

$$T_w = \frac{\rho \cdot T_s}{2 \cdot (1-\rho)}; \quad T_w = \frac{0{,}333 \cdot 2{,}22}{2 \cdot (1-0{,}333)} = 0{,}556 \text{ мс}. \qquad (2.6)$$

Повний час знаходження пакета в системі T_r, включаючи час обслуговування й час стояння в черзі:

$$T_r = \frac{T_s \cdot (2-\rho)}{2 \cdot (1-\rho)}; \quad T_r = \frac{2{,}22 \cdot (2-0{,}333)}{2 \cdot (1-0{,}333)} = 2{,}778 \text{ мс}. \qquad (2.7)$$

Як видно, цей час значно менше, чим необхідний показник якості 50 мсек для телефонії. Виходить, можна зменшити пропускну здатність каналу зв’язку, і тим самим заощадити витрати.

Розрахунки показників якості для послуги обміну з інтернет розраховуються подібним чином. Середня пропускна здатність, необхідна для завантаження сторінок, визначена емпірично в 1024 Кбіт/сек, середній розмір пакета – теж емпірично, 750 байт. Із цих даних можна визначити середній інтервал передачі пакетів t_s від одного абонента – по формулі:

$$t_s = b_{реальн} / B_{абон}; \quad t_s = 6000/1024 = 5{,}859 \text{ мс}.$$

Для пропущення навантаження 3,86 Ерл потрібно 10 каналів (з таблиці 2.2), що дасть у сумі пропускну здатність по формулі 2.8:

$$B_{послуги} = B_{абонента} \cdot V;\ \ B_{послуги} = 1024 \cdot 10 = 10240 \text{ Кбіт/с.} \qquad (2.8)$$

Час обслуговування одного пакета – по формулі 2.1:

$$T_s = 6000 / 10240 = 0{,}586 \text{ мс.}$$

Інтенсивність передачі пакетів від усієї абон. Групи по формулі 2.2

$$\lambda = 3{,}86 / 5{,}859 \cdot 10^{-3} = 659 \text{ пак/с.}$$

Коефіцієнт утилізації ρ по формулі 2.3

$$\rho = 659 \cdot 0{,}586 \cdot 10^{-3} = 0{,}386.$$

Потім визначаються показники якості; але, на відміну від телефонії, пакети мають неоднакову довжину. У першому наближенні можна вважати, що розмір пакетів підкоряється експонентному розподілу, хоча це й не зовсім так. Для розрахунків показників якості при експонентному розподілі використовуються наступні формули [3, 4].

Число пакетів у системі:

$$r = \frac{\rho}{1-\rho};\ \ r = \frac{0{,}386}{1-0{,}386} = 0{,}6297. \qquad (2.9)$$

Число пакетів у черзі:

$$w = \frac{\rho^2}{1-\rho}; \quad w = \frac{0{,}386^2}{1-0{,}386} = 0{,}243. \tag{2.10}$$

Час стояння пакетів у черзі T_w:

$$T_w = \frac{\rho \cdot T_s}{1-\rho}; \quad T_w = \frac{0{,}386 \cdot 0{,}586}{1-0{,}386} = 0{,}369 \text{ мс}. \tag{2.11}$$

Повний час знаходження пакета в системі *Tr*, включаючи час обслуговування й час стояння в черзі:

$$T_r = \frac{T_s}{1-\rho}; \quad T_r = \frac{0{,}586}{1-0{,}386} = 0{,}955 \text{ мс}. \tag{2.12}$$

Звернемо увагу, що час знаходження пакета обміну з інтернет у системі набагато менше, чим те ж час для телефонних пакетів, хоча вимоги до якості транспорту телефонії набагато вище, ніж транспорту інтернет. Резервів для економії пропускної здатності тут набагато більше.

Аналогічно розраховуються показники для обміну з базою даних і файловим сервером. Результати розрахунків приводяться в таблиці 2.3.

2.4 Оптимізація пропускної здатності каналів зв’язку

Для більш ефективного використання оплаченої пропускної здатності каналу можна зменшити необхідну пропускну здатність до величини, при якій затримка знаходження пакета в системі буде збільшена до припустимого значенні [5]. Для телефонії це – 50 мсек, для послуг інтернет, бази даних і файлового обміну – 500 мсек. Розрахунки за наведеною методикою показує, що пропускну здатність можна зменшити до 306 Кбіт/с, при цьому затримка складе

не більш 50 мсек. А для послуги доступу до інтернет пропускну здатність можна зменшити до 3970 Кбіт/с, при цьому затримка складе не більш 444 мсек при вимозі не більш 500 мсек. Для послуг бази даних ці цифри складуть 1068 Кбіт/с при затримці не більш 468 мсек, а для файлового обміну – 1363 Кбіт/с при затримці 475 мсек. Таким чином, наведений розрахунки дозволяє зменшити оплачену пропускну здатність і поліпшити економічні показники роботи мережі. Результати розрахунків оптимальної пропускний для філії в місті показано в таблиці 2.4.

Таблиця 2.3 – Розрахунки показників якості

Вид показника	телефонія	інтернет	База даних	Файл. обмін	розмір-ність
1) середня пропускна здатність для послуги	321,3	4617,2	1147,4	1382,4	Кбіт/сек
2) загальне навантаження групи	3	3,86	2,07	0,66	Ерланга
3) середня інтенсивність передачі пакетів =	150	659,4	264,9	198,3	пак/сек
4) Число каналів по таблиці Башарина	9	10	7	4	шт
5) загальна пропускна здатність для групи Вгр=	856,8	10240	3584	8192	Кбіт/сек
6) час обслуговування пакета T_s	2,22	0,586	1,116	0,83	мсек
7) коефіцієнт утилізації p=	0,333	0,386	0,296	0,165	
8) кількість пакетів у системі r=	0,417	0,6297	0,42	0,197	шт
9) кількість пакетів у черзі w=	0,083	0,2433	0,124	0,032	шт
10) час надходження пакета в системі T_r =	2,778	0,955	1,584	0,994	мсек
11) час стояння в черзі T_w =	0,556	0,369	0,468	0,164	мсек

Таблиця 2.4 – Результати розрахунків для оптимізованої пропускної здатності філії

Вид показника	телефонія	інтернет	база даних	Файл. обмін	розмір-ність
1	2	3	4	5	6
оптимальна пропускна здатність =	306	3970	1068	1363	Кбіт/с
1) середня пропускна здатність для послуги	285,6	3956,5	1147,392	1382,4	Кбіт/с
2) загальне навантаження групи	3	3,86	2,07	0,66	Ерланга

Продовження таблиці 2.4

1	2	3	4	5	6
3) середня інтенсивність передачі пакетів =	150	659,4	264,9	198,3	пак/сек
5) загальна пропускна здатність для групи Вгр=	306	3970	1068	1363	Кбіт/сек
6) час обслуговування пакета Ts=	6,222	1,511	3,745	4,989	мс
7) коефіцієнт утилізації *p*=	0,933	0,997	0,992	0,989	
8) кількість пакетів у системі *r*=	7,467	292,7105	124,016	94,201	шт
9) кількість пакетів у черзі *w*=	6,533	291,7139	123,024	93,212	шт
10) час надходження пакета в системі *Tr*=	49,778	443,895	468,223	474,957	мсек
11) час стояння в черзі *Tw*=	43,556	442,384	464,478	469,968	мсек

Результати розрахунків для інших філій, що входять у регіональну філію Куляб, наведено в таблиці 2.5.

Таблиця 2.5 – Результати розрахунків для оптимізованої пропускної здатності районів регіональної філії міста

		пропускна здатність для послуг, Кбіт/с					
Назва об'єкта	Число абонентів	Телефонія	інтернет	База Даних	Файловий Обмін	Трафік філії (Кбіт/с)	Сумарн. трафік (Кбіт/с)
Місто	27	306	3970	1068	1363	6707	54692
Район 1	26	296	3822	1029	1313	6460	
Район 2	24	275	3529	950	1213	5967	
Район 3	24	275	3529	950	1213	5967	
Район 4	23	264	3383	911	1163	5721	
Район 5	22	254	3236	872	1113	5475	
Район 6	22	254	3236	872	1113	5475	
Район 7	26	296	3822	1029	1313	6460	
Район 8	26	296	3822	1029	1313	6460	

Для оцінки результатів розрахунків за пропонованою методикою цікаво зрівняти в одній таблиці підсумкові цифри необхідної пропускної здатності мережі, розраховані по різних методиках. Дані, просумовані й приведені до однакових одиниць, представлено в таблиці 2.6.

Як видно з порівняння, метод підсумовування дає показники приблизно в 5 раз більше ніж оптимізація. Виникає питання, які дані ближче до реальних

цифр, при якій пропускній здатності абоненти будуть одержувати послуги з гарантованою якістю? На підставі практичного досвіду користування цифровими послугами в мережі, розрахованої методом простого підсумовування, можна зробити вивід, що в годину найбільшого навантаження якість надаваних послуг буде незадовільним. Тому потрібно користуватися пропонованою методикою розрахунків.

Таблиця 2.6 – Зведена таблиця пропускної здатності, розрахованої по різних методиках

Назва об'єкта	Число абонентів	Пропускна здатність методом підсумовування (Кбіт/с)		Пропускна здатність методом оптимізації (Кбіт/с)	
Місто	27	1279	10423	6707	54692
Район 1	26	1232		6460	
Район 2	24	1137		5967	
Район 3	24	1137		5967	
Район 4	23	1090		5721	
Район 5	22	1042		5475	
Район 6	22	1042		5475	
Район 7	26	1232		6460	
Район 8	26	1232		6460	

Пропускна здатність каналів, розрахована методом підсумовування, значно менше тієї, яка розрахована по оптимізованому варіанту виходячи з максимально припустимих затримок. Якщо спробувати розрахувати затримки доставки пакетів при такій же пропускній здатності, то вийдуть негативні значення – це означає, що частина пакетів буде загублена. Задача розрахунків втрат пакетів не ставилася в даній роботі, але очевидно, що втрати пакетів значно погіршать якість надаваних послуг. Тому оптимізація проводилася тільки виходячи із затримок, і отримані цифри можна вважати цілком достовірними для проектування мережі.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ

3.1 Архітектура програмного засобу

У загальному виді принцип роботи розроблювальної системи полягає в тому, що в сегменті мережі запущене спеціальне програмне забезпечення, яке здатне аналізувати мережний трафік і зберігати інформацію про показники інформаційної безпеки й виводити дані показники на аналіз адміністраторові мережі, для того, щоб той зміг вчасно ухвалити рішення щодо необхідних заходів запобігання загроз.

Розробку розв'язку будемо робити під персональний комп'ютер, що працює на базі операційної системи сімейства Windows, що й має бездротове або провідне підключення до аналізованого сегмента мережі.

Реалізацію застосування будемо здійснювати використовуючи вільний інструмент розробки Qt, а в якості мови програмування виберемо C++. Даний підхід дозволить створити застосування. Що володіє графічним інтерфейсом користувача, яке при необхідності може бути перенесене на будь-яку іншу платформу з найменшими працезатратами, що скоротить витрати при подальшій модернізації системи.

Для розробки рішення нам необхідно продумати структуру для зберігання й обробки даних (модель даних). У цьому випадку, найбільш ефективним способом зберігання даних мені бачиться реляційна база даних. Даний підхід спрощує доступ до бази даних, забезпечує високий рівень цілісності й захисту даних, а також дозволить зробити обробку інформації ефективніше.

У якості, що походить реляційної СУБД була обрана вільна кросплатформенна база даних SQLite. До її перевагою ставиться те, що дана база є, що вбудовується, що дозволяє відійти від традиційного підходу клієнт-сервер і глибше інтегрувати нашу базу даних з розроблювальною системою.

Також даний підхід здатний скоротити час відгуку програми й спростити розроблювану систему за рахунок того, що движок бази не є окремо

працюючим процесом, а є складовою частиною програми, протоколом обміну в цьому випадку є виклики функцій бібліотеки SQLite, варто відзначити, що дана база даних підтримує динамічне типізування даних.

Створимо модель схеми даних у програмному комплексі SQLeditor (рисунок 3.1).

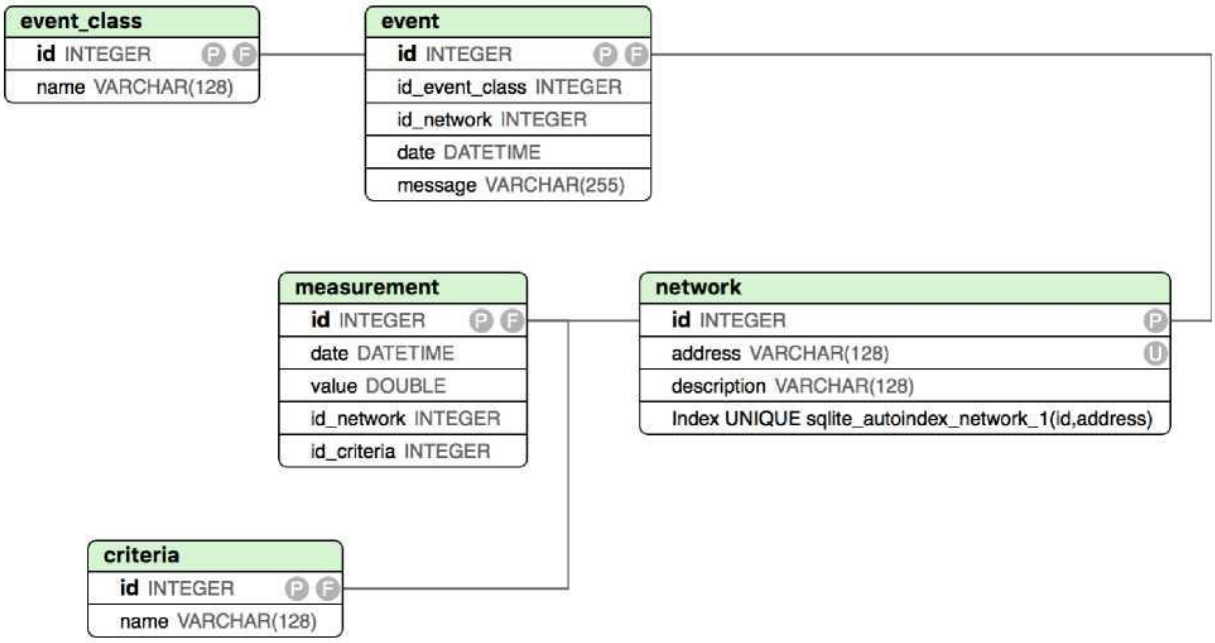

Рисунок 3.1 - Модель бази даних розроблювальної системи.

Опишемо використовувані типи даних:

– INTEGER - ціле;

– DOUBLE - дійсне;

– VARCHAR - текст;

– DATETIME - оцінка часу.

Приведемо опис сутностей, що входять у модель базу даних у таблиці 3.1.

На основі даної моделі бази даних буде створений програмний код ініціалізації таблиць, що створює всі необхідні таблиці враховуючий обмеження первинних і зовнішніх ключів.

Узагальнена схема аналізу мережного трафіка. Розглянемо цикл, що моделює процеси й етапи роботи розроблювальної програми і їх зв'язок з адміністратором комплексу.

Таблиця 3.1 - Опис сутностей, що входять у модель БД.

Сутність	Опис
Event	Подія інформаційної безпеки мережі
event_class	Тип події інформаційної безпеки
Network	Зберігання даних про сегмент мережі
Measurement	Зберігання показників для сегмента мережі в момент часу.
Criteria	Критерії інформаційної безпеки мережі

У загальному виді даний цикл буде виглядати як круговий зв'язок між інформаційно обчислювальною мережею, засобом захоплення й вимірювання параметрів мережі - засобів обробки отриманої інформації - засобів виводу обробленої інформації - адміністратора сегмента мережі й замикається на інформаційно обчислювальній мережі.

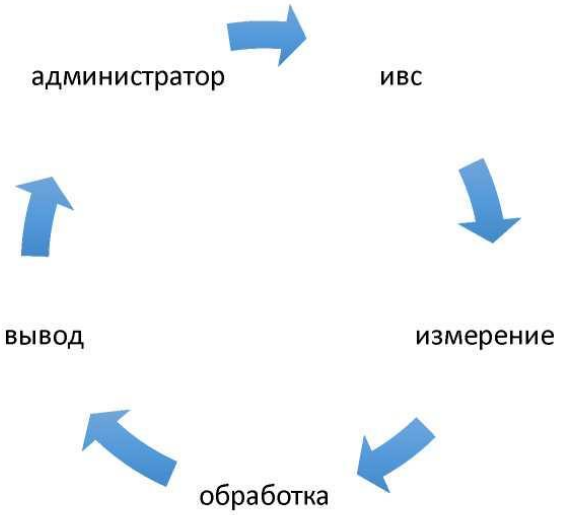

Рисунок 2.2 - Етапи роботи системи аналізу трафіка.

Розглянемо етапи даного циклу:

– програмний комплекс підключається до аналізованого сегмента мережі й робить зчитування трафіка.

– при обробці аналізованого трафіка ідентифікується його тип, визначаються характеристики зібраних пакетів, генеруються події й відбувається запис інформації в базу даних.

– компонент виводу зчитує інформацію з бази даних і формує

повідомлення, звіти й будує графіки для подальшого аналізу адміністратора мережі.

– адміністратор аналізує отримані графіки й звіти й приймає рішення щодо рівня захищеності мережі і якщо буде потреба впливає на мережу для усунення потенційних загроз.

Розглянемо характерні ознаки трафіка й визначимо показники, які ми можемо вважати з мережного інтерфейсу пристрою, що перебуває в аналізованому сегменті мережі.

Ознаки, на основі яких ми зробимо класифікацію пакетів:

– тип мережного протоколу;

– тип транспортного протоколу;

– напрямок передачі даних;

– значення полів заголовка, специфічних для протоколу.

На основі даної класифікації ми розраховуємо дані показники для подальшого аналізу:

– загальна кількість трафіка по протоколу (IP, TCP, ICMP і ін.);

– кількість TCP-Трафіка із прапорцями SYN, FIN, RST;

– кількість ICMP-Трафіка типів Echo Request, Destination Unreachable і подібних їх;

Для вимірювання показників і їх подальшої обробки нам необхідно виконати перехоплення пакетів з мережі, у нашому випадку доцільно виконати дану задачу за допомогою бібліотеки WinPcap. Потім, отримані після перехоплення пакети необхідно класифікувати й аналізувати показники за допомогою математичної статистики.

Спосіб розбору заголовка пакета заснований на його структурі, описуваної стандартом RFC. При обробці показників для виявлень потенційних загроз необхідно вибирати такі параметри трафіка, які будуть інваріантні до зміни величин легального трафіка, але будуть чутливі до появи атак. [14].

Зведемо в таблицю 2.2 такі показники.

Таблиця 2.2 - Приклади показників інформаційної безпеки

Показник	Пояснення	Застосування
$R_{IP}=V_{in}/V_{out}$	Відношення вхідного й вихідного трафіка	Підвищення обсягу вхідного трафіка без підвищення обсягу вихідного трафіка може говорити про потенційну атаку
$R_{PSH}=N_{PSH}/N_{TCP}$	Відносна частка прапорця PSH у вхідних пакетах	Даний показник відбиває ефективність передачі даних
$R_{EC3}=N_{PSH}/(N_{TCP}-N_{PSH})$	Відношення, що характеризує ступінь корисного завантаження каналу	Показник падає при SYN-flood і підвищується при TCP-flood
$d_{ACK}=N_{out}+N_{in}$	Різниця між кількістю вхідних і вихідних ACK-Прапорців у трафіку TCP	Виявлення атак, подібних SYN-flood і HTTP-flood
$R_{DU}=N_{ICMP,3}/N_{IP}$	Відношення, що показує відносну частку пакетів Destination Unreachable у трафіку.	Виявлення сканерів адрес і портів
$R_{ICMP}=N_{ICMP}/N_{IP}$	Відносна частка службових пакетів.	Визначення різних мережних аномалій, пов'язаних з використанням протоколу ICMP
$R_{SYN}=N_{TCP/SYN}/N_{TCP}$	Відносна частота TCP-Пакетів із прапором SYN	Визначення SYN flood.
$L=T_{IP}/N_{IP}$	Середня довжина IP-Пакета	Визначення різних атак класу DDoS.

У даному підрозділі був розроблений алгоритм до розробки системи засобу аналізу трафіка сегмента мережі й застосування інструмента для підвищення її надійності.

3.2 Програмна реалізація компонентів системи

Розроблювальна система аналізу трафіка в загальному виді складається з таких компонентів (креслення ДП.КСМ.111256/17.00.00.000 С1 .

1. Модуль збору даних у мережному сегменті. Його задача – збір даних у сегменті мережі, запис подій у базу. Для збору трафіка ми будемо

використовувати бібліотеку з відкритим вихідним кодом WinPcap. На базі даної бібліотеки створено багато відомі програмні продукти, наприклад Wireshark. Тому що трафік має великий обсяг, то нами був розроблений сніфер, що записує в базу даних лише необхідні числові характеристики з мережного інтерфейсу.

2. База даних. Задача компоненту зберігання даних. У якості підходящої бази даних була обрана вбудована реляційна база даних з відкритим вихідним кодом SQLite.

3. Модуль аналізу зібраних даних і виводу інформації. Його задача: аналіз зібраної інформації й вивід показників безпеки мережі в зручному для адміністратора виді. Для цих цілей був використаний фреймворк Qt і модуль для побудови графіків QCustomPlot.

Розроблювальний програмний продукт має наступні системні вимоги: 512Мб оперативної пам'яті, 10Гб вільного дискового простору, вихід у мережу із пристрою, що має підтримку бібліотеки WinPcap. Операційна система: Windows 7 і старше. Програмне забезпечення: установлений програмний продукт WinPcap.

Структура аналізатора трафіка. Розроблювальна програма працює у фоновому режимі й перехоплює трафік із заданого мережного інтерфейсу, використовуючи системну бібліотеку WinPcap. Далі відбувається класифікація пакетів по протоколах, виконується їхній кількісний підрахунок, а також підрахунок інших параметрів, таких як довжина пакета, наявність або відсутність прапорців. По вимірюваних величинах будуються часові ряди. Надалі програма затягає інформацію про аналізовані пакети в базу даних і розраховує показники мережної активності - допоміжні функції, чутливі до мережних аномалій.

Далі відбувається аналіз ряду критеріїв мережних аномалій, у випадку якщо критерій виконується неодноразово, те це сприймається як можлива загроза й відбувається повідомлення про це в інтерфейсі програми. Також відбувається побудова графіка мережної активності, піки якого також можуть бути сприйняті адміністратором мережі як потенційна загроза.

Збір і аналіз даних у мережному сегменті. Розглянемо роботу розробленого нами сніфера, його підключення до мережі відбувається завдяки бібліотеці WinPcap для виконання захвата пакета необхідно відкрити мережний пристрій за допомогою виклику функції

```
handleadapter = pcap_open_live(nameadapter, 65536, 1, 1000, errorbuffer);
```

де nameadapter - назва мережного інтерфейсу, далі зазначений розмір буфера, цифра 1 - указує на нерозбірливий режим, 1000 використання секунд як одиниці виміру й errorbuffer - буфер для повідомлень про помилку.

Потім перехоплення пакетів здійснюється за допомогою команди

```
pcap_loop(handlerAdapter, 0, callbackPacketHandler, NULL);
```

де handlerAdapter отриманий раніше дескриптор потоку, а callbackPacketHandler це функція, у яку пакети зроблять для подальшої обробки.

При подальшому зчитуванні пакетів їх уміст аналізується й визначається тип трафіка з використанням розбору структур заголовків згідно зі стандартами RFC, після чого проводиться перевірка за критеріями на відповідність потенційній загрозі.

Повний код мережного сніфера наведений у додатку А.

3.3 Робота з базою даних.

У даному розділі ми опишемо метод, що дозволяє встановити з'єднання з менеджером бази даних. Приведемо програмний код даного методу для подальшого аналізу.

```
Qsqldatabase Snifferdb::createconnection() {
```

```
static Qsqldatabase database = Qsqldatabase::adddatabase("QSQLITE");
Qdir
databasefile(Qstring::fromstdstring(Constants::PATH_SNIFFER_DATA
DASE));
database.setdatabasename(databasefile.absolutepath());
if (!database.open()) {
qdebug() << "Не можливо відкрити БД" << database.lasterror() << endl;
} else {
qdebug() << "БД підключена!" << endl;
}
return database;
}
```

Як ми бачимо, даний метод робить підключення до SQLite бази даних, яка зберігається в локальній папці програми, шлях до якої задається в конфігураційному файлі складання середовища Qt за назвою pcap_sniffer.pro. Даний файл зберігає також і інші змінні, необхідні для складання програми. У випадку помилки підключення бази даних виводиться помилка, що сповіщає адміністратора про збій у роботі програми, у випадку ж успішного підключення до бази даних виводиться повідомлення, що сповіщає про успішне підключення.

Створення таблиць у БД. Метод, що дозволяє встановити з'єднання з менеджером бази даних використовує клас qt QSQLdatabase, який представляє інтерфейс для підключення до БД через з'єднання й перебуває у файлі snifferdb.cpp .

Самі ж методи, що дозволяють створювати таблиці, зберігаються у файлах criteri- atable.cpp, eventtable.cpp, eventclasstable.cpp, measurementtable.cpp, networkta- ble.cpp і працюють аналогічним чином.

Розглянемо як приклад фрагмент методу, що дозволяє створити таблицю “Мережа”.

```
Qsqlquery* sqlquery = new Qsqlquery(database);
if (!sqlquery->exec("CREATE TABLE IF NOT EXISTS network (id INTEGER PRIMARY KEY, "
"address VARCHAR(128), "
"description VARCHAR(128),"
"UNIQUE(id, address));"))
```

Даний метод створює таблицю 'network' з полем id як первинний ключ, а також полями 'address', 'description' у які й заносяться дані про мережне з'єднання, UNIQUE є обмеженням унікальності тобто додатковий ключ, його відмінність від первинного ключа полягає в тому, що первинний ключ не може містити необов'язкові атрибути.

3.2 Перевірка мережі на можливі загрози

Розглянемо один з методів, що дозволяє виявити потенційну атаку на мережу. У цьому випадку будемо розглядати варіант атаки SYN- Flood, який був докладно розглянуто в розділі 1.

```
void PcapSniffer::storeAverageLengthInputPacket (u_int totalLengthInputPackets,
                    u_int countpackets) {
            if (numberPacket == countPackets) {
                    averagelegthinputpacket = totallengthinputpackets /
                                                countpackets;
qInfo(”AVERAGE TOTAL LEGTH PACKET: %u”, averageLegthInputPacket);
/* Одержати номер мережі в таблиці "Мережа" */
        this->idNetwork = networkTable- >getNetwork(ipAddress).getId();
/* Заносимо показник у таблицю "Показник" */
        Measurement measurement(1, getCurrentTime(), averageLegthInputPacket,
```

```
                    idnetwork, Constants::INPUT_IP_PACKET);
        measurementtable->addmeasurement(measurement);
/* Перевірка на загрози */
if (averageLegthInputPacket <= 65)                                    {
qDebug ("Пакети мають лише заголовок. Загроза DDoS-Атаки SYN-FLOOD!");
Event event(1, Constants::CRITERIA_EVENT_CLASS, idNetwork,
        getcurrenttime(), "N_IP_I/N_IP: Загроза DDoS-Атаки SYN-FLOOD!" );
                eventtable->addevent(event);
            }
}
```

Даний метод визначає середню довжину пакета, номер мережі, у якій відбувається вимірювання, а потім затягає інформацію в таблицю, у якій зберігаються вимірювані величини. Потім відбувається порівняння довжини прийнятого пакета, якщо довжина пакета перевищує задану величину, то виводиться повідомлення про можливу загрозу. Інформація про можливу атаку заноситься в таблицю разом з поточним часом і описом атаки.

Розглянемо користувацький інтерфейс системи.

Організація користувацького інтерфейсу проводилася стандартними засобами Qt використовуючи класи Qwidget і Qlabel, а для виводу графіків віджет Qcustomplot. На рисунку 3.1 представлений інтерфейс програми, що демонструє список мереж у якій здійснювався моніторинг.

У випадку недоступності мережі статус мережі зміниться на ‘error’. Технічні результати роботи, такі як запуск агента, початок зчитування пакетів, програма виводить в відладочну консоль Qt, що видно на рисунку 3.2.

Узагальнений основний цикл роботи графічного інтерфейсу програмного засобу зображено на кресленні ДП.КСМ.111256/17.00.00.001 А2. На основному вікні користувачу надається можливість переходу до одного з вікон котре відповідає за певну функцію програмного засобу. Основні гілки множинного вибору: ввід вхідної інформації, визначення мережевих ресурсів, аналіз поточного трафіку в мережі.

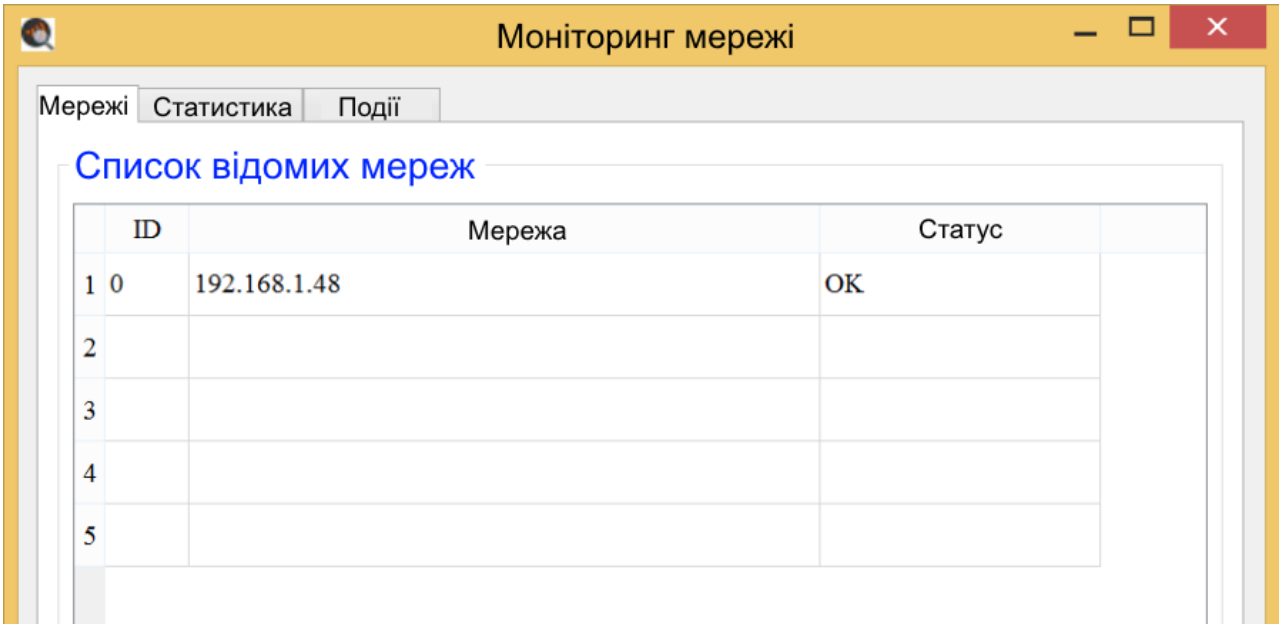

Рисунок 3.1 – Перегляд списку відомих мереж.

Рисунок 3.2 - Результат збору даних

Вкладка події представляє вивід як технічної інформації для адміністратора мережі (наприклад про запуск агента), так і інформацію, пов'язану з можливими загрозами, що ми бачимо на рисунку 3.3.

Вкладка статистика - відображає графіки, що будуються на базі накопиченої інформації про захоплені пакети. На рисунку 3.4 показана вкладка користувацького інтерфейсу програми, що відображає кількість вхідних IP пакетів.

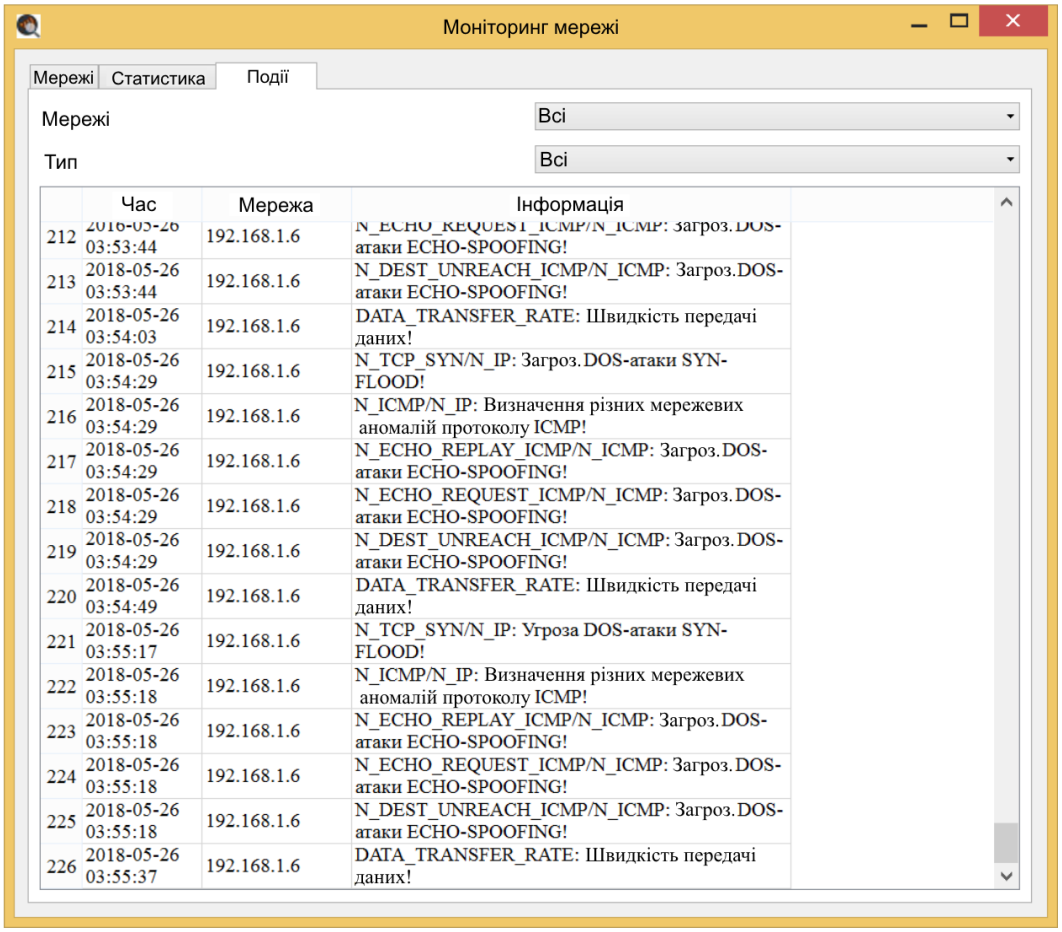

Рисунок 3.3 - Вивід подій інформаційної безпеки

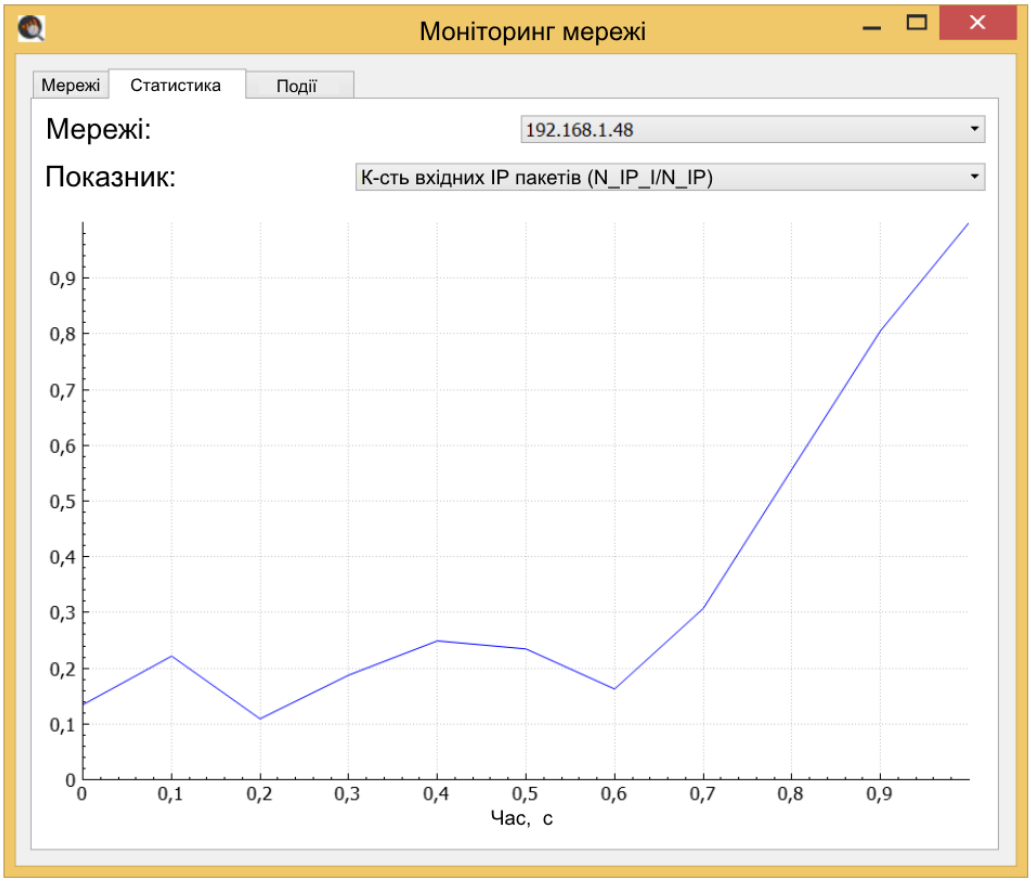

Рисунок 3.4 - Візуалізація накопиченої інформації про вхідні IP пакетах

Розроблена нами система має перспективи до застосування в складі комплексу заходів при розв'язку класу задач, що стосуються забезпечення безпеки сегмента комп'ютерної мережі, освітніх і дослідницьких задач.

У процесі роботи над розділом були вирішені наступні задачі:

– була сформульована й описана архітектура системи аналізу трафіка;

– описані модулі розроблювальної системи;

– розроблене клієнтське застосування для аналізу трафіка.

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

В даному розділі дипломного проекту проводиться економічне обґрунтування доцільності розробки програмного забезпечення. Зокрема, здійснюється розрахунок витрат на розробку програмного забезпечення, експлуатаційних витрат, ціни споживання проектного рішення. В заключній частині визначаються показники економічної ефективності нового програмного продукту, обґрунтовуються відповідні висновки.

Розроблене програмне забезпечення призначене для планування трафіку комп'ютерної мережі.

4.1 Розрахунок витрат на розробку програмного забезпечення

Витрати на розробку і впровадження програмних засобів (К) включають:

$$К = К_1, + К_2,$$

де $К_1$ - витрати на розробку програмних засобів, грн.

$К_2$ - витрати на відлагодження і дослідну експлуатацію програми рішення задачі на комп’ютері, грн.

Витрати на розробку програмних засобів включають:

- витрати на оплату праці розробників ($В_{ОП}$);
- витрати на відрахування у спеціальні державні фонди ($Вф$);
- витрати на покупні вироби ($Пв$);
- витрати на придбання спецобладнання для проведення експериментальних робіт ($Об$);
- накладні витрати ($Н$);
- інші витрати ($Ів$).

Розрахунок витрат на оплату праці.

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт у людино-днях та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломант; консультант техніко-економічного розділу.

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

№ п/п	Посада виконавців	Місячний оклад, грн.
1	Керівник ДП, ст.викладач	5000
2	Консультант техніко-економічного розділу,доцент	6025
3	Студент	1100

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N}\sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij}\,, \qquad (4.1)$$

де n_{ij} – чисельність розробників i-ої спеціальності j-го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником i-ої спеціальності j-го тарифного розряду, год;

C_{ij} – годинна ставка працівника i-ої спеціальності j-го тарифного розряду, грн.

Середньо годинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_{i}}, \qquad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника *i*-ої спеціальності *j*-го тарифного розряду, грн.;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ - місячний фонд робочого часу працівника *i*-ої спеціальності *j*-го тарифного розряду, год. (приймаємо 168 год.).

Результати розрахунку записують до таблиці 4.2.

Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

$$B_Ф = \frac{20,5}{100} \cdot 1100 = 225,5 \text{ грн.}$$

Таблиця 4.2 - Розрахунок витрат на оплату праці

№ п/п	Посада виконавців	Час розробки, год	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн
1	Керівник ДП, ст. викладач	16	29,76	476,19
2	Консультант техніко-економічного розділу, доцент	2	35,86	71,73
3	Студент	144	6,55	942,86
			Разом	1490,77

Величину відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства єдиний соціальний внесок складає 20,5 % від суми заробітної плати:

$$B_Ф = 0,205 * B_{ОП},$$

$$B_Ф = 0,205 * 1490,77381 = 305,61.$$

У таблиці 4.3 наведений перелік купованих виробів і розраховані витрати на них $B_{ПВ}$.

Витрати на використання комп'ютерної техніки включають витрати на амортизацію комп'ютерної техніки, витрати на користування програмним забезпеченням, витрати на електроенергію, що споживається комп'ютером. За даними обчислювального центру ТНЕУ для комп'ютера типу IBM PC/ATX вартість години роботи становить 6 грн. Середній щоденний час роботи на комп'ютері – 2 години.

Таблиця 4.3- Розрахунок витрат на матеріали та комплектуючі

№ п/п	Найменування купованих виробів	Одиниця виміру	Ціна, грн.	Кількість купованих виробів	Сума, грн.	Транспортні витрати (10% від суми)	Загальна сума, грн.
1	Папір (формат А4)	уп.	70	2	140	14	154
2	Ручка кулькова	шт.	4	2	8	0,8	8,8
3	Олівець простий	шт.	2	2	4	0,4	4,4
4	Диски CD-R	шт.	5	2	10	1	11
5	Зошит, 96 арк	шт.	9,5	1	9,5	0,95	10,45
6	Тонер для принтера	уп.	60	1	60	6	66
Разом							254,65

Розрахунок витрат на використання комп'ютерної техніки приведений в таблиці 4.4.

Таблиця 4.4 - Розрахунок витрат на використання комп'ютерної техніки

№ п/п	Назва етапів робіт, при виконанні яких використовується комп'ютер	Час використання комп'ютера, год.	Витрати на використання комп'ютера, грн.
1	Проведення досліджень та оформлення їх результатів	60	270
2	Оформлення техніко-економічного розділу	8	36
4	Оформлення ДП	12	54
Разом		80	360

Накладні витрати проектних організацій включають три групи видатків: витрати на управління, загальногосподарські витрати, невиробничі витрати. Вони розраховуються за встановленими відсотками до витрат на оплату праці. Середньостатистичний відсоток накладних витрат приймемо 150% від заробітної плати:

$$H = 1{,}5 * 1490{,}77 = 2236{,}16.$$

Інші витрати є витратами, які не враховані в попередніх статтях. Вони становлять 10% від заробітної плати:

$$I = 0{,}1 * 1490{,}77 = 149{,}08 \text{ грн.}$$

Витрати на розробку програмного забезпечення складають:

$$K_1 = B_{ОП} + B_{Ф} + B_{ПВ} + H + I,$$
$$K_1 = 1490{,}77 + 305{,}61 + 254{,}65 + 2236{,}16 + 149{,}08 \text{ грн.}$$

Витрати на відлагодження і дослідну експлуатацію програмного продукту визначаємо за формулою:

$$K_2 = S_{м.г.} \cdot t_{від},$$

де $S_{м.г.}$ - вартість однієї машино-години роботи ПК, грн./год.

$t_{від}$ - комп'ютерний час, витрачений на відлагодження і дослідну експлуатацію створеного програмного продукту, год.

Загальна кількість днів роботи на комп'ютері дорівнює 30 днів. Середній щоденний час роботи на комп'ютері – 2 години. Вартість години роботи комп'ютера дорівнює 6 грн. Тому

$К_2$= 6·60 = 360 грн.

Таблиця 4.5 - Кошторис витрат на розробку програмного забезпечення

№ п/п	Найменування витрат	Сума витрат, грн.
1	Витрати на оплату праці	1490,77
2	Відрахування у спеціальні державні фонди	305,61
3	Витрати на куповані вироби	254,65
4	Накладні витрати	2236,16
5	Інші витрати	149,08
6	Витрати на відлагодження і дослідну експлуатацію програмного продукту	360,00
	Разом	4796,27

4.2 Розрахунок ціни проекту

Величина можливої (договірної) ціни повинна визначатися з урахуванням ефективності, якості і термінів її виконання на рівні, що відповідає економічним інтересам замовника (споживача) і виконавця. Договірна ціна ($Ц_Д$) для проектних рішень розраховується за формулою:

$$Ц_Д = B_{КС} \cdot \left(1 + \frac{p}{100}\right),$$

де $B_{КС}$ – кошторисна вартість, грн.;

p - середній рівень рентабельності, % (приймаємо 25% за погодженням з керівником).

$$Ц_Д = 4796,27 * (1 + 0,25) = 5995,33 \text{ грн.}$$

Економічне обґрунтування вибору комплексу технічних і програмних засобів

Для впровадження більшості КС необхідно:

- придбання та встановлення засобів комп’ютерної техніки;
- придбання та інсталяція системного програмного забезпечення;
- інсталяція і адаптація спеціалізованого програмного забезпечення

Кожен з перерахованих пунктів допускає безліч різних варіантів, так як існує велика кількість конфігурацій комп'ютерів, обладнання та різноманітних програмних продуктів. Кожен з варіантів передбачає різні за величиною і структурою витрати.

Для виконання даного дипломного проекту спеціального програмного забезпечення не використовувалось і не закуплялося.

4.3 Розрахунок зведених економічних показників

Економічна ефективність – це співвідношення між отриманим прибутком та затраченими коштами. Вона обчислюється за формулою:

$$E_ф = П_р/К_В,$$

де $П_р$ – очікуваний прибуток ;

$К_В$ – кошторисна вартість.

Очікуваний прибуток можна розрахувати із співвідношення:

$$П_Р = Ц_Д – К_В.$$

$$П_Р = 5995{,}34 - 4796{,}27 = 1199{,}07 \text{ грн.}$$

Після проведених розрахунків отримуємо:

$$E_ф = 1199,07 / 4796,27 = 0,25$$

Термін окупності додаткових капітальних вкладень визначається як :

$$T = 1/E_ф = 1 / 0,25 = 4 \text{ роки}.$$

Таблиця 4.6 - Зведені економічні показники розробки

Показник	Значення
Собівартість, грн.	4796,27
Плановий прибуток, грн.	1199,07
Ціна, грн.	5995,34
Економічна ефективність	0,25
Термін окупності, рік	4

В даному розділі проведено розрахунок витрат на розробку програмного засобу. Зокрема, обчислені витрати на заробітну плату, єдиний соціальний внесок, витрати на куповані вироби, а також накладні та інші витрати. На основі цих розрахунків складено кошторис проектного рішення та визначена прогнозована ціна.

Проведений розрахунок економічної ефективності, очікуваного прибутку та терміну окупності капітальних вкладень

Провівши аналіз отриманих значень економічних показників робимо висновок, що розробка програмного засобу є економічно доцільною.

ВИСНОВКИ

1. Проаналізовано основні етапи планування трафіку та вплив мережевих загроз на трафік. Дослідження систем моніторингу трафіка показало, що існуючі підходи по плануванню трафіка комп'ютерної мережі не враховують вплив загроз.

2. Формалізовано методику розрахунку параметрів трафіку. В основі розрахунків трафіку комп'ютерної мережі лежать імовірнісні характеристики потоку даних, які генеруються різними мережними пристроями. Для виконання розрахунків необхідно мати інформацію про приблизну структуру мережі, кількість абонентів у кожному вузлі мережі, розподіл абонентів по різних класах обслуговування, перелік мережних послуг. Трафік розраховується окремо для кожного виду послуги на кожному мережному вузлі. Розроблене програмне забезпечення розраховує пропускну здатність каналів зв'язку та затримку передачі пакетів.

3. Розроблено програмне забезпечення розрахунку трафіку та аналізу існуючого трафіку. Розроблювальна система складається з таких компонентів: модуль розрахунку параметрів трафіку, модуль збору даних у мережному сегменті, база даних, модулі аналізу зібраних даних і виводу інформації.

4. В якості інструментальних засобів розроблення обрано мову C++ та бібліотеку розроблення графічних інтерфейсів Qt. Розроблено графічний інтерфейс програмного засобу. Система пройшла тестування й може виконувати поставлені їй задачі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Назаров А.Н. Модели и методы расчета структурно-сетевых параметров сетей АТМ. – М.: Изд-во «Горячая линия-Телеком», 2002. – 256 с.

2. Вишневский В.М. Теоретические основы проектирования компьютерных сетей – Москва, 2003. – 506с.

3. Современные компьютерные сети. 2-е изд. / В.Столлингс. – Спб.: Питер, 2003. – 783 с..

4. Крылов В.В. Теория телетрафика и ее приложения. / Крылов В.В., Самохвалова С.С. – Спб.: БХВ-Петербург, 2005. – 288 с.

5. Теорія телетрафіку: навч.посіб./ В.Я. Воропаєва, В.І. Бессараб, В.В. Турупалов, В.В. Червинський. – Донецьк: ДВНЗ «ДонНТУ», 2011. –202 с.

6. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 4 изд. / В.Г. Олифер, Н.А. Олифер – СПб: Питер, 2010. – 944 с.

7. McCabe J. Network Analysis, Architecture, and Design. Third edition. / James D. McCabe - Morgan Kaufmann, 2007 – 495 p.

8. Яковина В.С. Основи безпеки комп'ютерних мереж: Навчальний посібник – Львів: НВФ "Українські технології", 2008. – 396 с.

9. Демида Б.А. Основи адміністрування LAN у середовищі MS Windows: навч. посіб. / Б.А. Демида, К.М. Обельовська, В.С. Яковина. – Львів: Видавництво Львівської політехніки, 2013. – 488 с.

10. Семенов А. Б. Структурированные кабельные системы. 4-е изд./ Семенов А. Б., Стрижаков С. К., Сунчелей И. Р. - М.: ДМК-Пресс, 2002. - 640 с.

11. Новиков Ю. В. Локальные сети: Архитектура, алгоритмы, проектирование / Новиков Ю. В., Кондратенко С. В. - М.: ЭКОМ, 2002. - 311 с.

12. Виденье отказоустойчивой, надежной, масштабируемой сети передачи данных - [Електронний ресурс] Режим доступу - http://habrahabr.ru/ blogs/personal/93629/

13. Хелеби С. Принципы маршрутизации в Internet, 2-е издание./ Хелеби С. Мак-Ферсон Д. Пер. с англ. - М.: "Вильямс", 2001. - 448 с.

14. Документація з настройки обладнання фірми Cisco. [Електронний ресурс]: Режим доступу http://www.cisco.com

15. Чекмарев А. Windows 7. Руководство администратора. - Спб.: БХВ-Петербург, 2010 – 896 с.

16. Визерспун Д. Освой самостоятельно LINUX за 24 часа, 3-е изд. - М.: Издательский дом "Вильямс", 2001.- 352 с.

17. Жуматий С.А. Программная среда поддержки эффективного выполнения задач на параллельных вычислительных системах [Текст] / С.А. Жуматий – М.:МГУ им М.В. Ломоносова, 2005. - 95 с.

18. Корнеев В. В. Параллельные вычислительные системы [Текст] / В. В. Корнеев - М.: Нолидж, 1999. - 320 с.

19. Трофимов С. А. CASE-технологии: Практическая работа в Rational Rose [Текст] / С. А. Трофимов - М.: БИНОМ, 2002. - 288 с.

20. Штайнер Г. HTML/XML/CSS. Справочник [Текст] / Г. Штайнер - М: Лаборатория базовых знаний, 2001. – 512 с.

21. Гифт Н. Python в системном администрировании - 2009 - 511 с.

22. Лутц М. - Изучаем Python - O'Reilly, 2011 – 1280 с.

23. Головатый А. Django. Подробное руководство / Головатый А., Каплан-Мосс Дж. – Символ,2010 – 552 с.

24. Бизли Д. Python. Подробный справочник – Символ,2010 – 500 с.

25. Саммерфилд М. Программирование на Python 3 – Символ,2009 -608 с.

26. Сузи Р.А. Язык программирования Python - Бином-пресс – 300 с.

27. Уэсли Дж. Чан Python. Создание приложений - Вильямс, 2016 – 816 с.

28. Свейгарт Э. Автоматизация рутинных задач с помощью Python: практическое руководство для начинающих - Вильямс, 2016 – 592 с.

29. Шоттс У. Командная строка Linux. Полное руководство – Питер, 2017 -480 с.

30. Мэтиз Э. Изучаем Python. Программирование игр, визуализация данных, веб-приложения – Питер, 2017 – 496 с.

31. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102

«Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та мережі» / О.М. Березький, Л.О.Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2013.–65с.

32. Паздрій І.Р. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» – Тернопіль: Економічна думка 2014.- 36 с.