Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Система моніторингу та адміністрування комп'ютерної мережі організації*

Виконав: студент *IV* курсу, групи *CIс-41*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

	(підпис)	*Дюк П. П.* (прізвище та ініціали)
Керівник	(підпис)	*Стадник Н. Б.* (прізвище та ініціали)
Нормоконтроль	(підпис)	*Луцик Н.С.* (прізвище та ініціали)
Завідувач кафедри	(підпис)	*Осухівська Г.М.* (прізвище та ініціали)
Рецензент	(підпис)	*Кряжич О.О.* (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Осухівська Г.М.
(підпис) (прізвище та ініціали)
« « 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студента *Дюка Петра Павловича*
(прізвище, ім'я, по батькові)

1. Тема роботи *Система моніторингу та адміністрування комп'ютерної мережі організації*

Керівник роботи *кандидат технічних наук, ст.викл каф. КС Стадник Наталія Богданівна*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*28* « *лютого* 2023 року № *4/7-237*

2. Термін подання студентом завершеної роботи *19.06.2023 р.*

3. Вихідні дані до роботи *Технічне завдання*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз технічного завдання
2. Проєктна частина
3. Практична частина
4. Безпека життєдіяльності, основи охорони праці.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. *Структурна схема системи моніторингу мережі.*
2. *Діаграми процесу управління локальною мережею.*
3. *Діаграма варіантів використання.*
4. *Результат роботи системи.*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	*Пилипець М.І., д.т.н., професор кафедри МТ*		

7. Дата видачі завдання 02.03.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Розробка технічного завдання*	*02.03-25.03.2023*	
2	*Аналіз технічного завдання*	*26.03-01.04.2023*	
3	*Аналіз вимог до системи моніторингу роботи мережі*	*02.04-16.04.2023*	
4	*Проектування структури системи*	*17.04-04.05.2023*	
5	*Проектування і реалізація програмної частини*	*05.05-31.05.2023*	
7	*Налаштування і тестування системи моніторингу мережі*	*01.06-06.06.2023*	
8	*Безпека життєдіяльності, основи охорони праці*	*07.06-08.06.2023*	
9	*Оформлення кваліфікаційної роботи*	*05.06-12.06.2023*	
10	*Попередній захист кваліфікаційної роботи*	*12.06-16.06.2023*	
11	*Захист кваліфікаційної роботи*	*19.06-24.06.2023*	

Студент _____ *Дюк Петро Павлович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник Наталія Богданівна*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Система моніторингу та адміністрування комп’ютерної мережі організації // Кваліфікаційна робота на здобуття освітнього ступеня бакалавр // Дюк Петро Павлович // ТНТУ, спеціальність 123 «Комп’ютерна інженерія» // Тернопіль, 2023 // с.– 60 , рис. – 32 , табл. – 1, аркушів А1 – 4, бібліогр. – 18.

Ключові слова: моніторинг, протоколи, чат, локальна мережа.

У даній кваліфікаційній роботі виконано розробку системи для моніторингу та адміністрування локальної мережі.

Пояснювальна записка містить 4 розділи.

В першому розділі здійснюється аналіз предметної області. Проведено огляд існуючих систем, визначені їх позитивні і негативні сторони, а також визначені задачі кваліфікаційної роботи.

В другому розділі описано розробелено структурну схему системи моніторингу, діаграму класів, діаграму послідовності.

В третьому розділі здійснена реалізація системи моніторингу. Наведено приклад роботи серверної і клієнтської частини

В четвертому розділі розглянуті питання охорони праці та вимоги з техніки безпеки.

ABSTRACT

System of monitoring and administration of the organization's computer network // Qualification work for the bachelor's degree // Duke Petro Pavlovich // TNTU, specialty 123 "Computer engineering" // Ternopil, 2023 // p.– 60, fig. – 32, tab. - 1, sheets A1 - 4, bibliography. - 18.

Keywords: monitoring, protocols, chat, local network.

In the qualification work, the development of a system for monitoring and administration of the local network was carried out.

The explanatory note contains 4 sections.

In the first section, the analysis of the subject area is carried out. An overview of the existing systems was carried out, their positive and negative sides were determined, and the tasks of the qualification work were determined.

In the second section, a detailed structural diagram of the monitoring system, a class diagram, and a sequence diagram are described.

In the third section, the monitoring system is implemented. An example of the work of the server and client parts is given

The fourth chapter deals with occupational health and safety requirements..

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

ОС (OS) – операційна система;

IP – Internet Protocol;

ПЗ - програмне забезпечення;

UML - Unified Modeling Language;

WMI - Windows Management Instrumentation.

ВСТУП

Система моніторингу мережі відіграє важливу роль у забезпеченні безпеки та ефективного керування мережею. Моніторинг мережі полягає у спостереженні за подіями, що відбуваються в мережі, з метою забезпечення її безпеки, стабільності та оптимальної продуктивності. Незважаючи на це, багато малих і середніх компаній і організацій уникають використання систем моніторингу мережі. Однією з найважливіших причин для цього є відсутність професійних мережевих адміністраторів, які б могли використовувати доступні на ринку системи моніторингу мережі. Це може призвести до значних витрат або навіть втрати капіталу в разі виникнення проблем у мережі.

У даній роботі пропонується система моніторингу локальної мережі, яка допоможе вирішити цю проблему завдяки простоті використання та наданню необхідних функцій для моніторингу мережі.

Основною перевагою використання запропонованої системи є її доступність навіть для користувачів-початківців, які мають лише базове уявлення про використання комп'ютерних додатків. Таким чином, запропонована програма моніторингу мережі може бути ефективно використана в малих та середніх організаціях, якщо вони не мають можливості залучити професійних мережевих адміністраторів.

Метою КРБ є проектування та реалізація системи моніторингу локальної мережі організації.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– описати існуючі моделі моніторингу комп'ютерної мережі;

– проаналізувати існуючі розробки та обґрунтувати вибір технології проектування;

– спроектувати систему моніторингу мережі;

– здійснити концептуальне проектування системи локальної мережі організації;

– виконати логічне моделювання системи моніторингу мережі;

– побудувати фізичну модель мережі організації;

– реалізувати систему моніторингу мережі організації.

Результатом виконання роботи є розроблений додаток для моніторингу локальної мережі організації, який забезпечить можливість автоматизованого відстеження продуктивності та ефективності мережі, що дозволить скоротити часові витрати у процесі вирішення цих завдань.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Огляд предметної області

У загальному випадку, під інформаційною інфраструктурою підприємства розуміють середовище, яке складається як з автоматизованої, так і з неавтоматизованої частин, що забезпечують необхідний інформаційний сервіс.

Основною метою створення інформаційної інфраструктури є надання будь-якого виду сервісу та послуг, які необхідні для функціонування підприємства.

Інформаційна інфраструктура підприємства складається з:

- різних програмних рішень;
- мережевих технологій та служб;
- засобів адміністрування ресурсів;
- засобів інформаційного захисту;
- засобів спам-захисту та ін.

Наприклад, за допомогою служб каталогу існує можливість упорядкувати інформацію про мережеві ресурси, що знаходиться в одному місці. Це можуть бути серверні папки, спільні принтери, багатофункціональні пристрої тощо. Усі ці рішення забезпечують централізоване управління всіма ресурсами, і навіть інформацією них.

Як і інші сучасні технології використання мережі Ethernet має деякі особливості. Наприклад, необмежений та нічим не контрольований доступ співробітників підприємства до глобальної мережі. Звичайно, трафік контролюється провайдером, але якщо одним каналом буде користуватися

кілька людей, а то й весь штат, може виникнути необхідність вважати трафік для кожного хоста окремо . Наступним кроком є аналіз цього трафіку. Завдяки аналізу, співробітникам, які відповідають за внутрішню безпеку організації, з'являється можливість стежити за діями користувачів.

Моніторинг мережевих систем дозволяє користувачам переглядати та керувати якістю продуктивності, аналізувати дані та виявляти помилки в мережі. Інструменти моніторингу є важливим активом для системних адміністраторів, оскільки вони дозволяють постійно відстежувати роботу мережі на основі зібраних даних протягом певних інтервалів часу. Типова мережа складається з різних апаратних пристроїв, таких як мости, репітери, комутатори, маршрутизатори і т.д. Моніторинг мережі включає перевірку правильності функціонування цих пристроїв, а також забезпечення доступності з'єднання між ними.

Система моніторингу мережі виконує три основні функції:

– забезпечення надійності;
– безперебійності роботи мережі;
– надання звітів про стан мережі і подій.

Широке впровадження комутованих мереж призвело до того, що традиційні засоби діагностики стали непопулярними, неінформативними та не задовольняють на запити адміністраторів. Насамперед, це можна пояснити тим, що в сильно сегментованих мережах найпростіші аналізатори протоколів можуть бачити лише лиж одноадресний трафік на окремому порту комутатора. Тому, такі аналізатори не здатні зібрати всю необхідну статистику, через те, що кожна пара «хостів, що спілкуються» між собою, користується, як би своєю власною мережею.

У тому випадку, якщо комутатор не буде дзеркально відображати кілька портів одночасно, то аналізатор «побачить» тільки єдиний сегмент мережі.

Виробники обладнання вирішили вище зазначену проблему шляхом запровадження різних засобів для відновлення повної «видимості» мережі.

Наприклад, у багатьох сучасних комутаторах підтримується дзеркальне відображення. Однак усі ці кошти мають свої мінуси:

По-перше, у кожен момент часу залишається видимим лише один порт комутатора. Це призводить до того, що виявлення проблем цілого сегмента мережі є дуже нелегкою справою.

По-друге, наприклад, теж «дзеркальне відображення», як правило, призводить до зниження продуктивності самого комутатора.

По-третє, найважливішим недоліком є проблема «дзеркального відображення» повнодуплексних каналів Ethernet.

За підсумком вище сказаного, можна дійти невтішного висновку, що проблема моніторингу мереж є актуальною.

Розглянемо типи програмних засобів які відносяться до моніторингу мережі:

1) Експертні системи. Це системи, які поєднують людські знання та досвід для виявлення проблем у мережах та пропонування можливих рішень. Вони можуть бути реалізовані у вигляді окремих підсистем, таких як мережеві аналізатори або аналізатори протоколів.

2) Системи управління мережею. Це системи які працюють з використанням єдиного ценру, ядра програмної системи, які збирають статистичну інформацію про вузли та пристрої в мережі. Вони також можуть збирати дані про мережевий трафік. Основними функціями таких систем є аналіз та моніторинг мережі, а також можливість управління мережевими пристроями.

3) Засоби управління системою. Ці засоби здатні виконувати функції управління комунікаційним обладнанням та моніторингу мережі. Вони можуть дублювати деякі функції систем управління мережею.

Ці програмні засоби допомагають у виявленні проблем у мережі, моніторингу її стану та наданні рекомендацій щодо вирішення проблем. Вони можуть бути використані для управління мережевими пристроями, аналізу

трафіку та забезпечення безпеки мережі.

Загальна структура системи моніторингу мережі може включати наступні компоненти:

1) Збір даних. Система збирає дані про події та стан систем, підключених до мережі. Це може включати моніторинг різних параметрів, таких як стан мережевих пристроїв, використання пропускної здатності, мережевий трафік тощо. Дані можуть бути зібрані за допомогою агентів, розташованих на кожному вузлі мережі, або за допомогою централізованих систем збору даних.

2) Аналіз даних. Зібрані дані проходять аналіз для виявлення аномальних патернів, проблем або важливих подій. Це може включати порівняння поточного стану з нормальними параметрами, виявлення аномалій, спостереження за тенденціями тощо. Алгоритми аналізу можуть бути побудовані на основі правил, машинного навчання або статистичних методів.

3) Візуалізація та звітність. Отримані результати аналізу даних можуть бути візуалізовані у зрозумілій формі, наприклад, у вигляді графіків, діаграм або табличних звітів. Це дозволяє адміністратору мережі легко спостерігати за станом мережі та робочих станцій, аналізувати продуктивність та виявляти проблеми.

4) Сповіщення та автоматизовані дії. Система може надсилати сповіщення адміністратору мережі про важливі події або виявлені проблеми. Це може бути здійснене шляхом електронної пошти, SMS-повідомлень або інших засобів сповіщення. Крім того, система може мати можливість виконувати автоматизовані дії, такі як перезавантаження пристроїв, налаштування параметрів мережі або запуск сценаріїв у відповідь на певні події.

Загальна структура системи моніторингу мережі може варіюватися в залежності від конкретного програмного засобу. Однак, основні компоненти

збору даних, аналізу, візуалізації та автоматизованих дій є типовими для багатьох таких систем (рис.1.1).

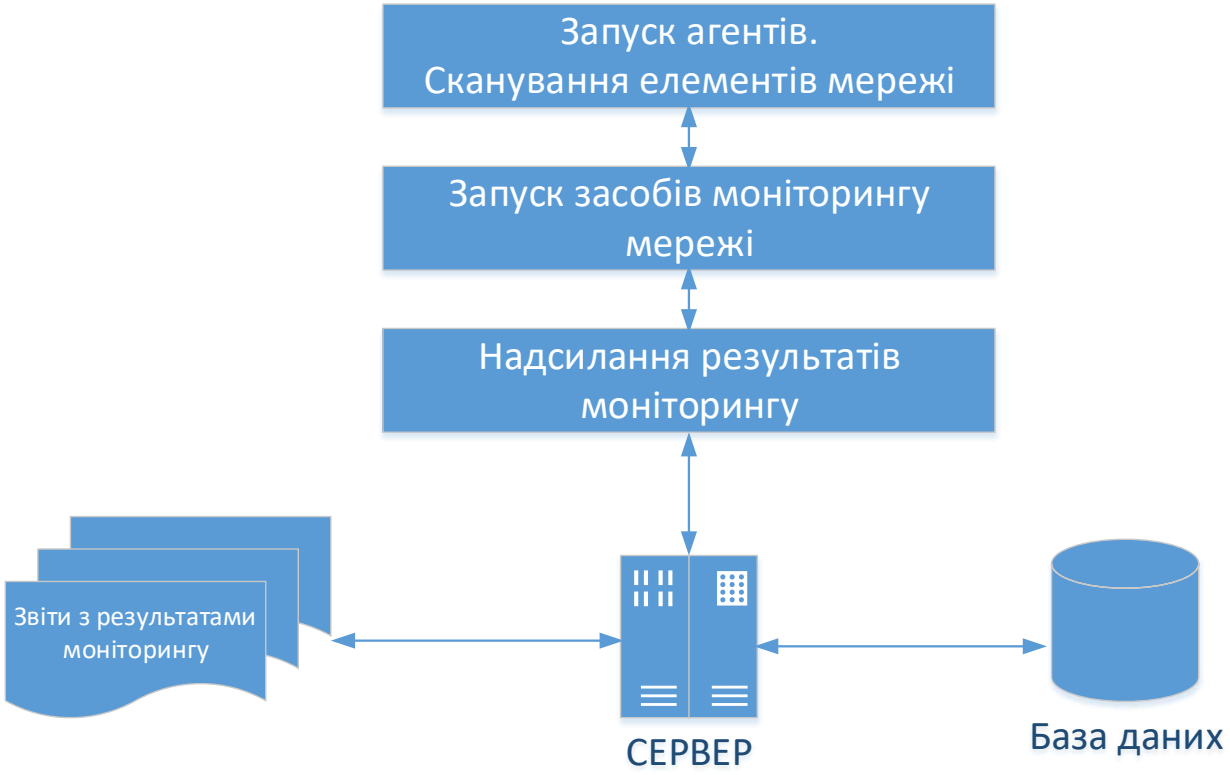


Рисунок 1.1 – Система моніторингу мережі

Як видно з рисунку система моніторингу як результат своєї роботи отримує ряд звітів. Типи осовних видів звітів наведені на рисунку 1.2.

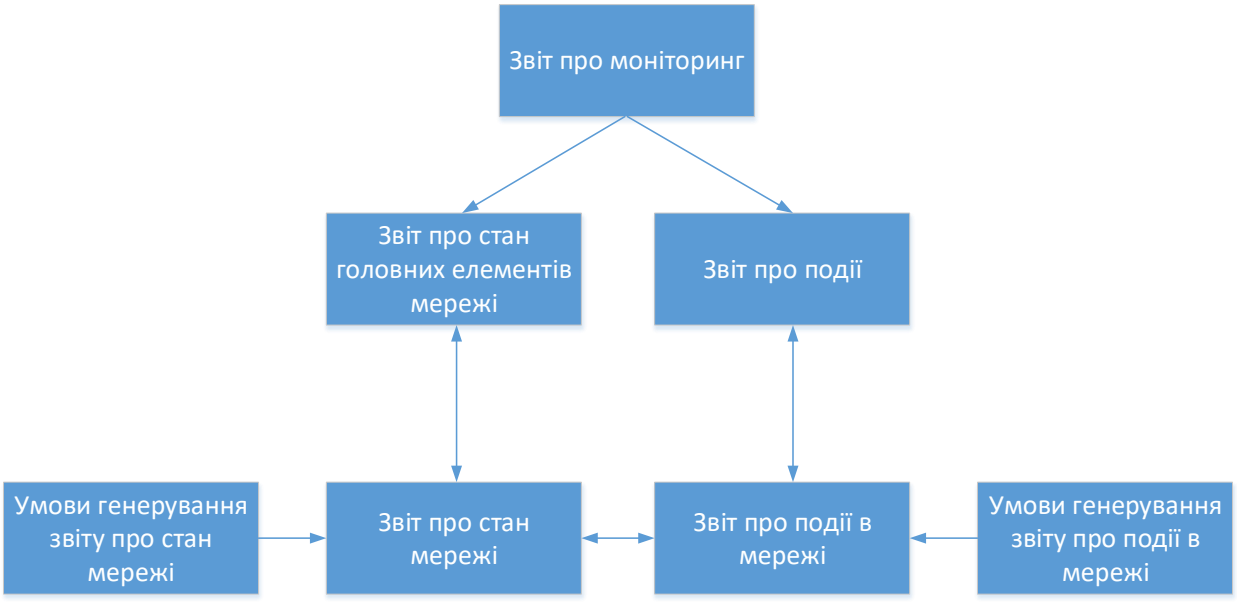


Рисунок 1.2 – Звіти системи моніторингу

У запропонованій системі моніторингу мережі, яка описана в даній роботі, робочі станції повинні бути оснащені клієнтською версією (агентом) системи моніторингу мережі. Використовуватиметься автоматичний метод моніторингу з можливістю запуску ручного сканування.

В заданий інтервал часу сервер відправлятиме пакети до робочих станцій, а робочі станції повертатимуть їх, створюючи стале з'єднання між робочими станціями і сервером.

У системі моніторингу мережі адміністратор мережі має віддалений доступ, який надає авторизований доступ для виконання необхідних дій.

1.2 Огляд існуючих рішень

У цьому пункті будуть розглянуті рішення, аналогічні до пропонованого додатку для моніторингу мережі. Для кожного згаданого програмного забезпечення будуть розглянуті плюси та, можливо, мінуси. Нижче наведено огляд деяких популярних додатків для моніторингу локальної комп'ютерної мережі:

– SolarWinds Network Performance Monitor [1]. Цей додаток надає засоби для моніторингу та управління мережею в реальному часі. Він включає в себе моніторинг пристроїв, пропускної здатності, трафіку, стану послуг та інших параметрів. Також забезпечує можливості аналізу та візуалізації даних, сповіщення про проблеми та автоматизовані дії для вирішення проблем.

– PRTG Network Monitor [2]. Цей додаток дозволяє моніторити всі аспекти мережі, включаючи пристрої, трафік, пропускну здатність, додатки та послуги. Він надає детальну інформацію про стан мережі через веб-інтерфейс та графічні звіти. PRTG також підтримує сповіщення про проблеми та автоматизовані дії.

– Nagios [3]. Це популярна система моніторингу з відкритим вихідним кодом. Вона дозволяє відслідковувати стан пристроїв, послуг, пропускної здатності та інших параметрів мережі. Nagios підтримує сповіщення про проблеми через електронну пошту, SMS та інші засоби. Також вона може інтегруватись з різними додатковими плагінами для розширення функціональності.

– Zabbix [4]. Ця система моніторингу також є відкритою та має широкий функціонал. Вона дозволяє моніторити стан пристроїв, мережевого трафіку, додатків та інших параметрів. Zabbix надає гнучкі можливості налаштування, графіки, сповіщення та автоматизовані дії.

– ManageEngine OpManager [6] Цей додаток забезпечує моніторинг пристроїв, послуг, трафіку та інших аспектів мережі. Він надає графіки, сповіщення про проблеми, аналіз пропускної здатності та інші корисні функції. OpManager також має можливості автоматизованого управління та конфігурації мережі.

– TCPdump [7] є інтерфейсом командного рядка для захоплення та аналізу мережевих пакетів. Він доступний на багатьох платформах, включаючи Unix, Linux і Windows. TCPdump дозволяє вам переглядати, аналізувати та зберігати мережевий трафік. Він може бути корисним для

вирішення проблем з мережею, відладки та безпекового аудиту.

– Wireshark [8] є повноцінним додатком для аналізу мережевих пакетів з графічним інтерфейсом користувача. Він підтримує багато протоколів і дозволяє вам захоплювати, відтворювати, аналізувати та візуалізувати мережевий трафік. Wireshark надає розширені фільтри, можливість відстежування трафіку в реальному часі, аналіз статистики пакетів, декодування протоколів та багато іншого.

Це лише кілька прикладів додатків для моніторингу локальної комп'ютерної мережі, існує багато інших рішень залежно від потреб та вимог користувача. Порівняння існуючих на ринку інструментів та пропонованої системи моніторингу мережі показано у таблиці 1.1.

Таблиця 1.1 - Порівняння пропонованої системи з іншими системами

Функції	Wireshark	Zabbix	Nagios	PRTG NM	TCPdump	OpManager	SolarWinds	Пропонована система
Читання пакетів	+	+	+	+	+	+	+	+
Захоплення пакетів	+	+	+	+	+	+	+	+
Фільтри даних	+	+	+	+	-	-	-	-
Графічний інтерфейс	+	+	+	+	-	+	+	+
На основі командного рядка	-	-	-	-	+	-	-	-
Моніторинг обладнання	-	+	+	+	+	+	+	+
Мережеве трасування	+	+	+	+	+	+	+	+
Система чату	-	-	-	-	-	-	-	+
Клієнт-серверна архітектура	-	+	+	+	-	+	+	+
Втрата пакетів	+	+	+	+	+	+	-	-
Збереження журналу	+	+	+	+	+	+	+	+
Статистичний звіт	+	+	+	+	-	-	+	+

Порівняння, представлене в таблиці 1.1 ґрунтується на функціональних можливостях кожного інструменту. Деякі функціональні можливості запропонованої системи у цій КРБ будуть аналогічні існуючим системам мережного моніторингу.

1.3 Вимоги до системи моніторингу

Функціональні можливості запропонованої системи у цій роботі будуть частково аналогічні існуючим системам мережного моніторингу.

Додатковим функціоналом запропонованої системи, порівняно з аналогічними системами, є система чату. Система чату є додатковою функцією, яку було надано для простоти взаємозвязку користувачів і адміністраторів.

Крім того, система моніторингу мережі буде мати простий у використанні інтерфейс користувача.

1.4 Висновки до розділу

Аналіз існуючих систем моніторингу продуктивності мережевих систем показав, що подібні системи дозволяють користувачеві переглядати та керувати якістю продуктивності, аналізом даних та помилками мережі Інтернет-протоколу (IP).

Було виявлено, що інструмент моніторингу продуктивності є важливим активом для системного адміністратора, що дозволяє постійно відстежувати роботу мережі на основі даних, що збираються через регулярні часові відтинки.

Грунтуючись на проведеному аналізі, можна дійти висновку, що типова мережу складається з різних апаратних пристроїв, як-от мости, , комутатори, маршрутизатори тощо.

Моніторинг мережі включає перевірку правильності функціонування цих пристроїв і іншого підключеного до мережі обладнання, а також забезпечення доступності сполучного середовища та необхідний, щоб забезпечувати безперебійну роботу обчислювальної системи в організації.

Пропоноване рішення буде аналогічно існуючим системам, але матиме інтерактивний інтерфейс та можливість швидкого обміну повідомленнями через чат для оперативного реагування адміністратора на проблеми які можуть виникнути в процесі роботи користувачів.

РОЗДІЛ 2 ПРОЄКТНА ЧАСТИНА

2.1 Концептуальне проектування системи

На рисунку 2.1 представлена модель, що описує процес управління локальною мережею.

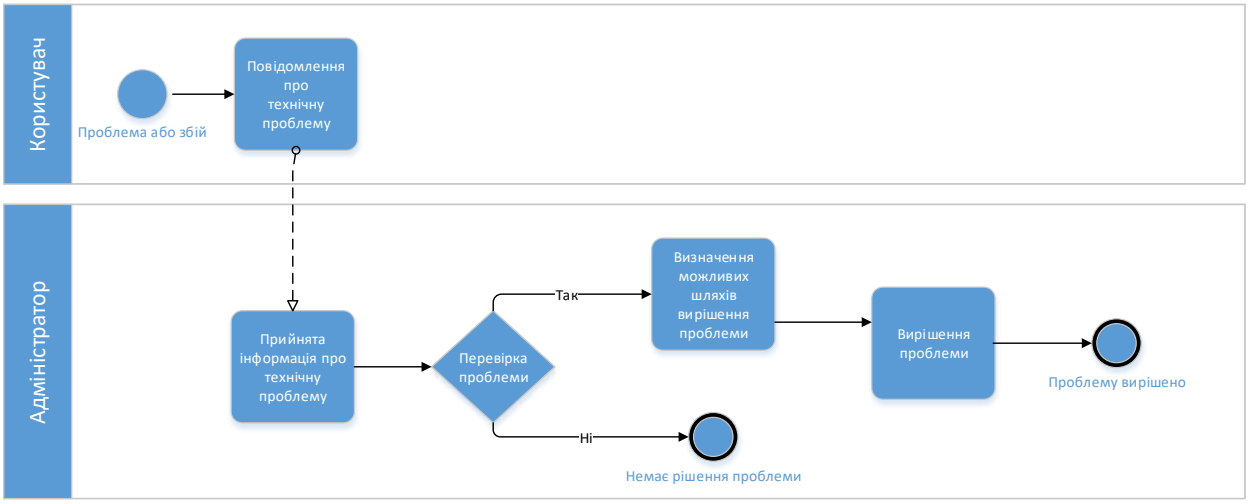


Рисунок 2.1 - BPMN -діаграма процесу управління локальною мережею (як є)

Процес управління локальною мережею включає такі особливості [9]:

- У разі виникнення проблеми у користувача необхідно викликати IT-фахівця;
- Перша оцінка проводиться фізично, IT-фахівець прямує на місце, де було повідомлено про проблему;
- Технічний фахівець перевіряє проблему і наскільки можна негайно надає рішення, інакше проблема буде вирішена через певний час;
- Всі види допомоги є фізичними, які потребують часу.

На рисунку 2.2 представлена блок-схема, що демонструє типовий алгоритм адмініструваня мережею.

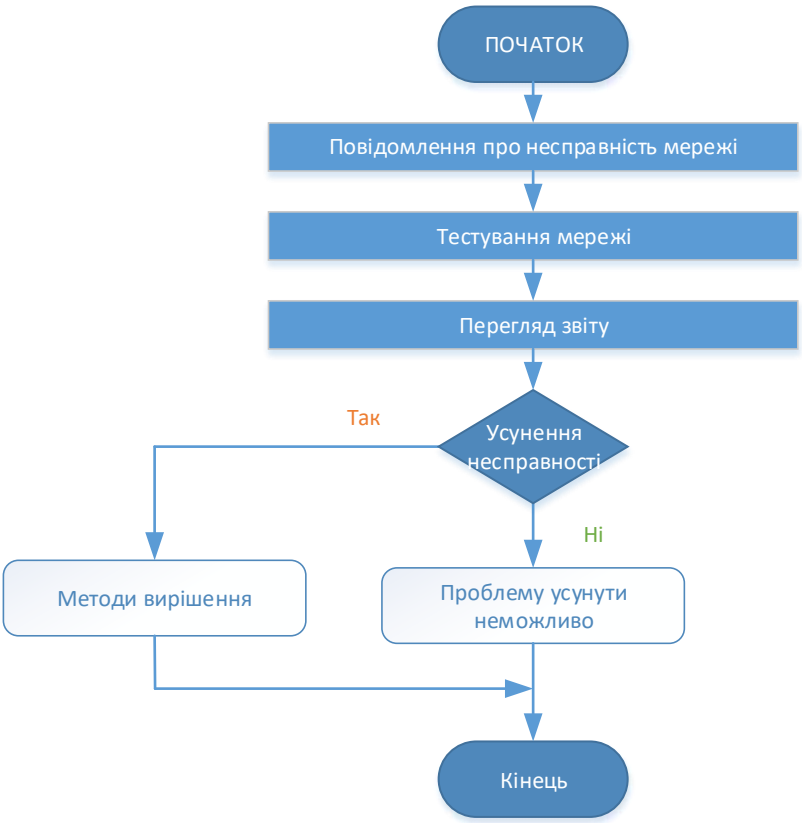


Рисунок 2.2 - Блок-схема процесу управління мережею

Аналізуючи 2.2 можна назвати такі проблеми:

- Немає посилання на попередню проблему;
- Ручна система;
- Повільний час відгуку призводить до неефективності та неефективності повсякденної діяльності;
- Відсутня постійна служба підтримки для вирішення повсякденних проблем та запитів користувачів/клієнтів.

На рисунку 2.3 представлено блок-схему роботи планованої системи моніторингу локальної мережі організації.

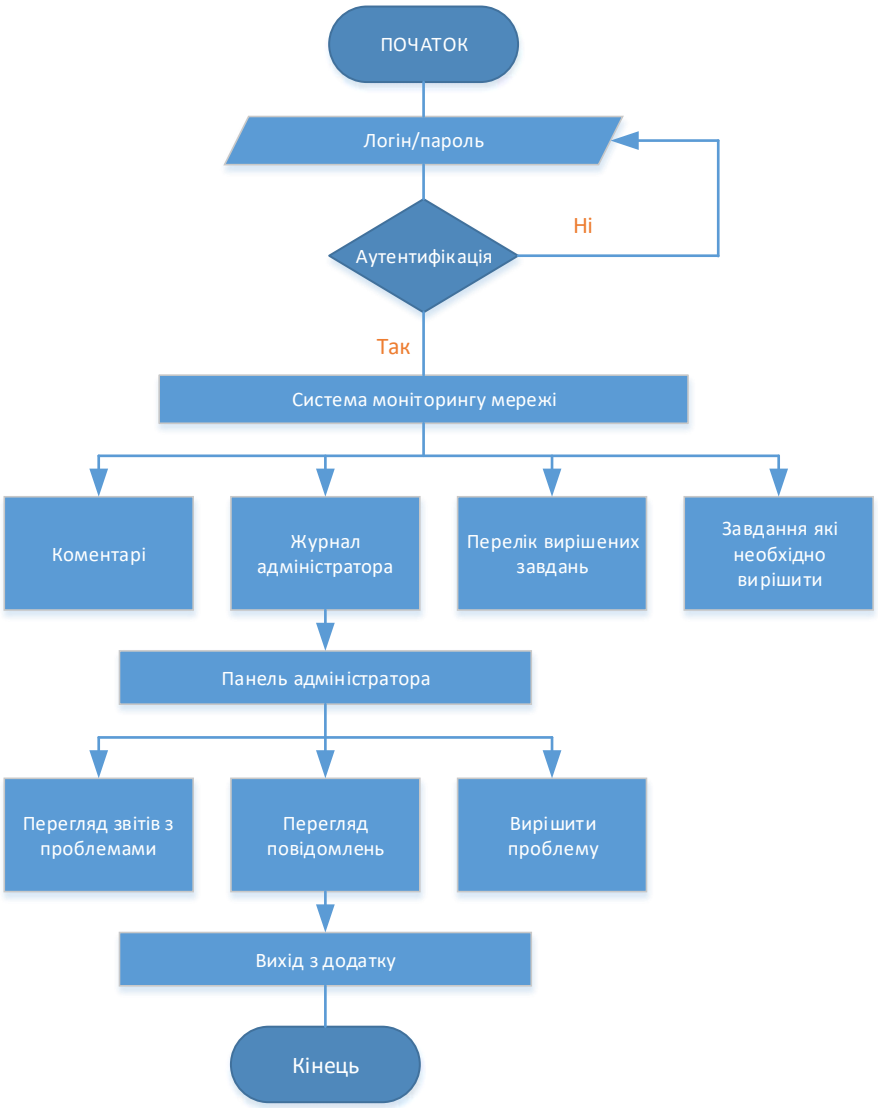


Рисунок 2.3 - Блок-схема алгоритму роботи запропонованої системи

Пропонується рішення, спрямоване на ефективне вирішення системних проблем. Основні можливості цього рішення включають:

1) Система, яка дозволяє користувачам публікувати свої проблеми та запити, а також запитувати онлайн-допомогу. Це забезпечить зручну платформу для комунікації між користувачами та службою підтримки, дозволяючи швидко та ефективно обмінюватися інформацією про проблеми та шукати рішення.

2) Система, що допомагає користувачам перевірити вирішення проблеми онлайн без допомоги служби підтримки. Це може включати базу знань або пошукову систему, яка надає користувачам доступ до інформації та

рекомендацій щодо вирішення типових проблем.

3) Система, що дозволяє заощадити час та ресурси, шляхом формування щотижневих звітів за запитами користувачів. Це дозволить службі підтримки ефективніше організовувати та пріоритизувати роботу над запитами, а також надавати статистику та аналітику щодо популярних проблем та їх вирішень.

4) Система, що дозволяє мережному адміністратору та технічному фахівцю відстежувати проблему залежно від розташування запиту. Це може включати моніторинг та аналіз мережі, щоб визначити місцезнаходження проблемного вузла та швидко реагувати на нього.

Таке рішення спрямоване на поліпшення комунікації з користувачами, самостійне вирішення проблем та забезпечення ефективного управління системними проблемами.

На рисунку 2.4 представлена модель, що описує автоматизоване рішення для управління локальною обчислювальної мережею.

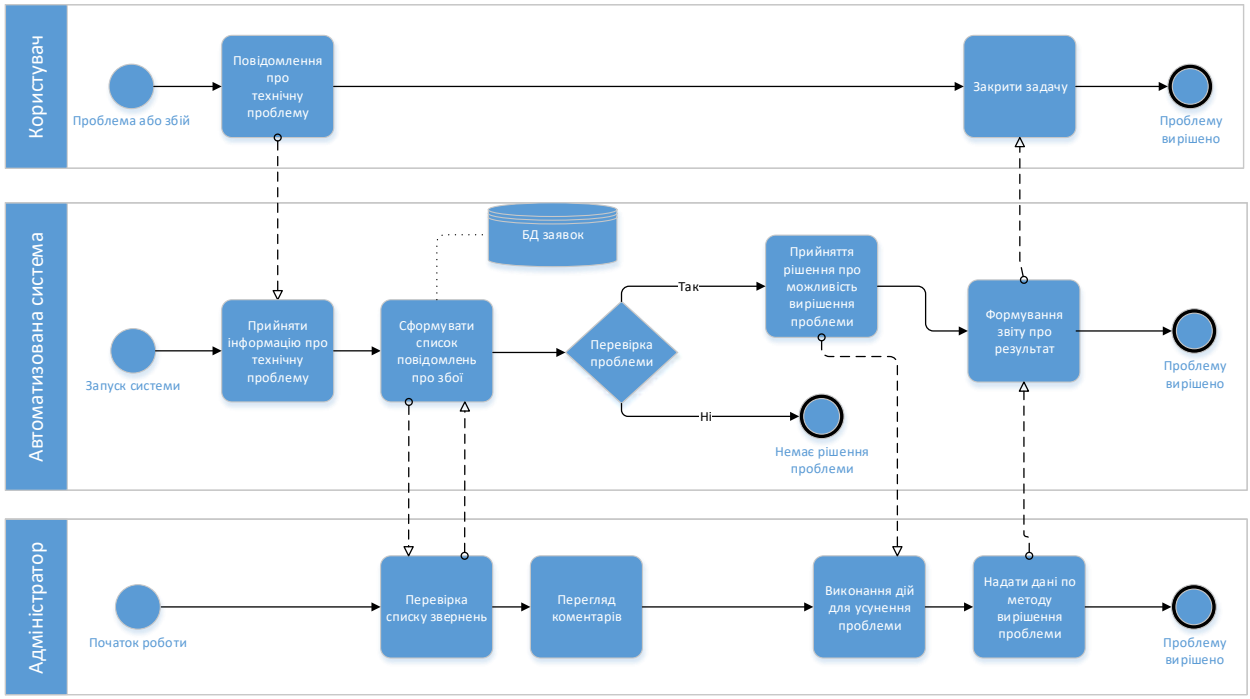


Рисунок 2.4 - BPMN -діаграма процесу управління локальною мережею (як буде)

Відстеження запитів насамперед автоматизує процес управління проблемами та запитами клієнта/користувача. Адміністрація зможе зберігати запити клієнтів/користувачів онлайн та відстежувати їх із будь-якого місця [1]. І, завдяки використанню бази даних, кожна проблема/запит буде однозначно ідентифікована, тому не буде проблем з використанням тих самих ідентифікаторів, а процес отримання файлів інцидентів буде швидше.

Ця програма заснована на архітектурі клієнт-сервер. Базова система побудована на основі наявності цієї програми як на клієнтських, і на серверних пристроях. Оскільки сервер підключено до мережі, клієнтам дозволено підключатися до сервера, використовуючи відповідний номер порту та IP - адресу сервера

У розділі дистанційного керування після запуску з'єднання між клієнтом та сервером надаються деякі параметри для використання адміністратором сервера.

Оскільки система підключена до мережі, адміністратор має доступ до історії запитів із будь-якого місця за наявності підключення до Інтернету та наявності відповідних облікових даних для входу [4].

2.2 Логічне проєктування системи моніторингу мережі

Використаємо уніфіковану мову моделювання (UML) для логічного проєктування системи моніторингу мережі Що дозволить з допомогою графічної символізації пояснити дизайн програмного забезпечення системи.

У процесі проєктування системи моніторингу можна використовувати різні діаграми та специфікації UML, що дозволяють краще ознайомитись з функціями, які пропонується в системі.

Першим кроком може бути побудова діаграми варіантів використання (Use Case Diagram), яка графічно відображає основні функції, доступні в системі. На цій діаграмі представлені актори (користувачі і сервер системи) і

варіанти використання (функціональні можливості системи), які можуть бути виконані.

Як правило, UML включає п'ять діаграм та специфікацій, щоб здійснити деяке знайомство з запропонованою системою кожної функції [7].

Першим кроком в UML побудуємо діаграму варіантів використання, яка є графічним представленням основних функцій запропонованої системи.

Наданий варіант використання в цій роботі показує доступність трьох акторів, які є клієнтом, адміністратором та сервером.

На наступній діаграмі показано основні функціональні можливості реалізованого додатку (рисунок 2.5).

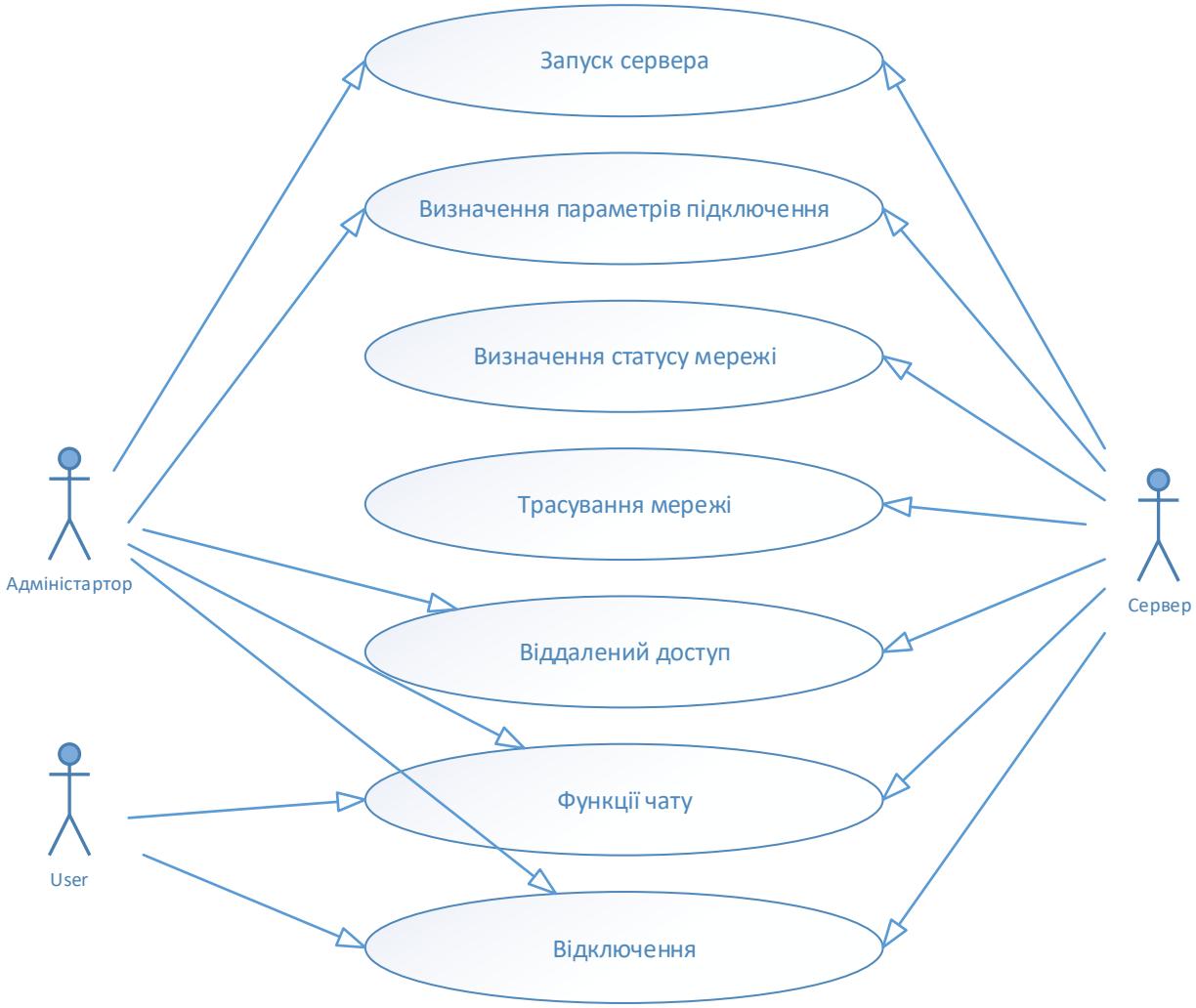


Рисунок 2.5 - Діаграма варіантів використання

У наступних рисунках представлена специфікація варіантів використання, тобто докладна інформація про представлені функціональні можливості.

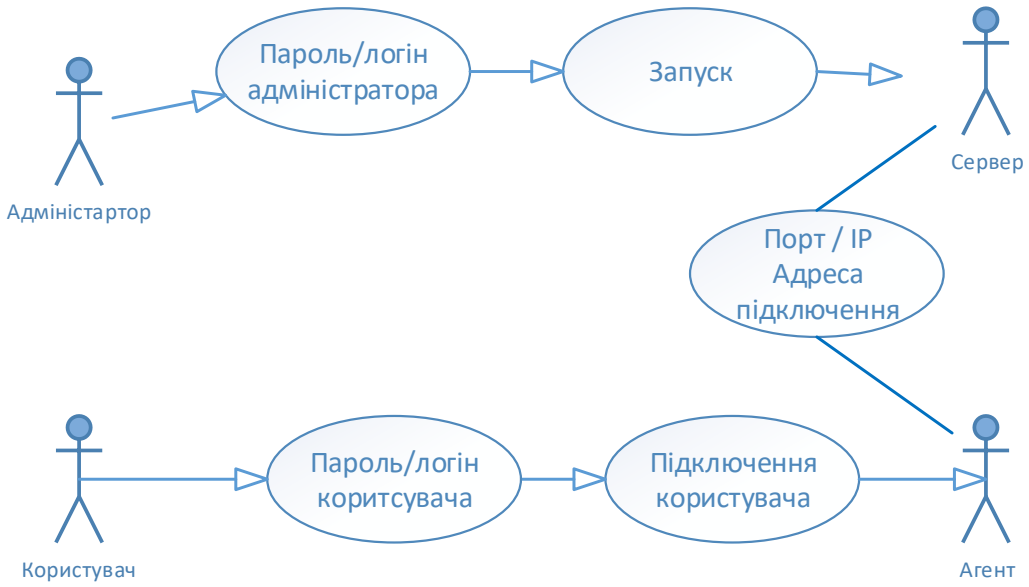


Рисунок 2.6 – Запуск і підключення користувачів системи

Перший крок це запуск сервера. Запуск доступний тільки для адміністратора після авторизації.

Після запуску сервера, агенти, розміщені на комп'ютерах користувачів, здійснюють підключення до нього.

На даному етапі для з'єднання клієнта з сервером використовуються номер порту та IP-адреса сервера. Агент клієнта використовує параметри інтерфейсу підключення які встановлює сервер це номер порту та IP-адреса. Для простоти роботи запропонованої системи параметри підлючення заздалегідь визначені.

Наступнми є визначення стану мережі (рис.2.7).

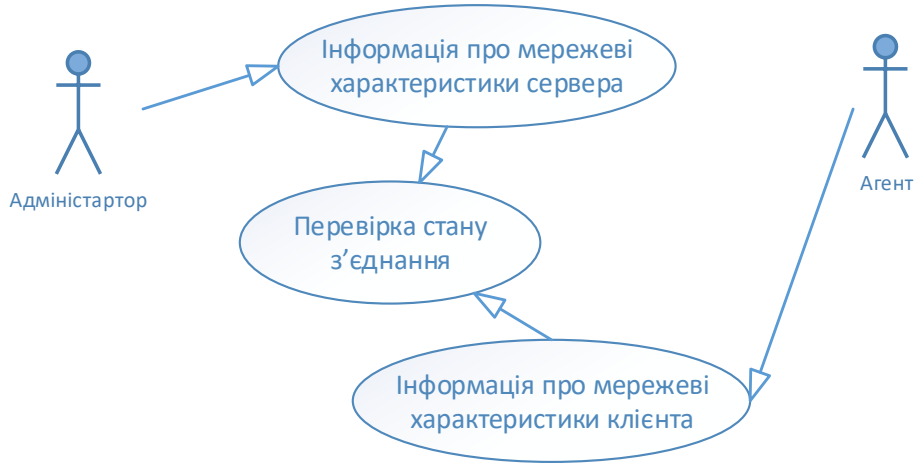


Рисунок 2.7 – Перевірка стану з’єднання сервера і клієнта

На даному етапі роботи відбувається обмін інформацією про пристрої на яких встановлений агент і які підключені до сервера. Ця функція реалізовується зі сторони сервера, так і зі сторони користувача.

Головна мета полягає в перевірці та оновленні інформації про мережеві адаптери та характеристики підключення. Ця функція дозволяє здійснювати контроль та керування, а у разі виникнення проблем система виявить їх і повідомить про несправність з'єднання. Клієнт може передати цю інформацію адміністратору для отримання допомоги.

Ділянку трасування мережі описано на рисунку 2.8.

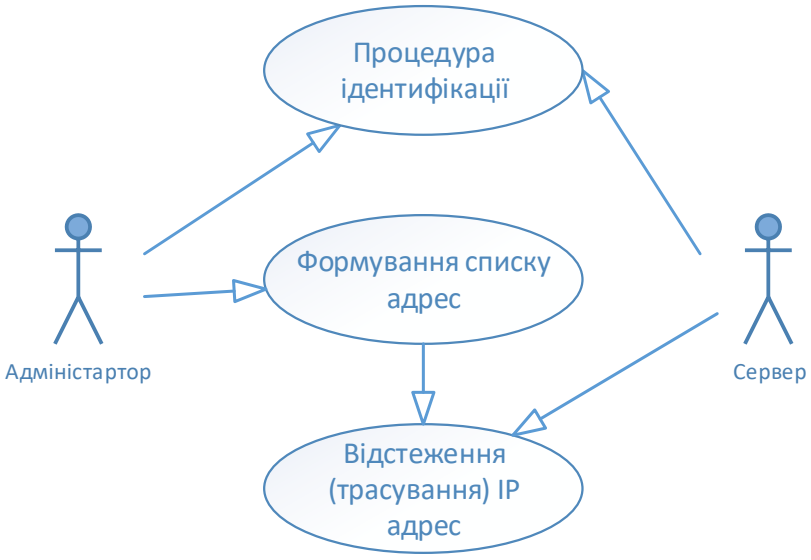


Рисунок 2.7 – Трасування мережі

Дана частина в основному здійснюється на сторноні сервера. Адміністратор складає список IP-адрес або імен хостів, які він хоче перевірити на наявність з'єднання. Це також дозволяє перевірити доступність активних мережевих пристроїв, які знаходяться між сервером і цільовим пристроєм.

Опис розділу віддаленого доступу наведено неа рисунку 2.8.

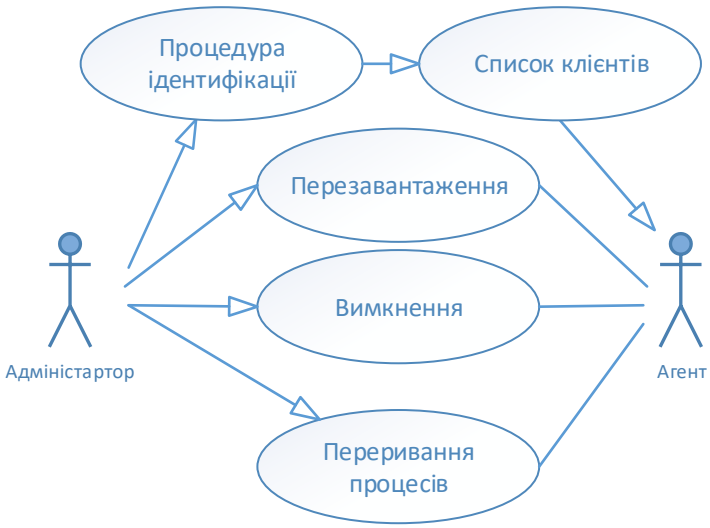


Рисунок 2.8 – Віддалений доступ

Функція віддаленого доступу дозволяє адміністратору здійснювати ряд дій на клієнтських пристроях. Це може бути завершення завислих процесів, перезавантаження, або вимкнення. Для цього реалізовано вибір зі списку пристроїів, які доступні серверу та вибір необхідної дії.

Функцію чату можна активувати як з боку клієнта, так і з боку сервера. Сторони можуть розпочати спілкування незалежно чи це клієнт чи сервер. Єдина відмінність полягає в тому, що клієнт може надсилати повідомлення лише на сервер, а дміністратор шляхом вибору клієнтів може надсилати повідомлення їм. Цей процес описаний на рисунку 2.9.

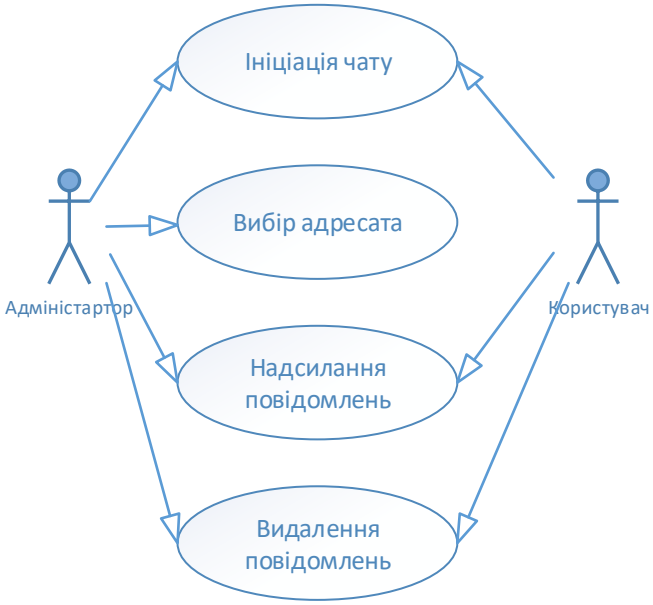


Рисунок 2.9 – Функція чату

На рисунку 2.10 показано опис процесу вимкнення.

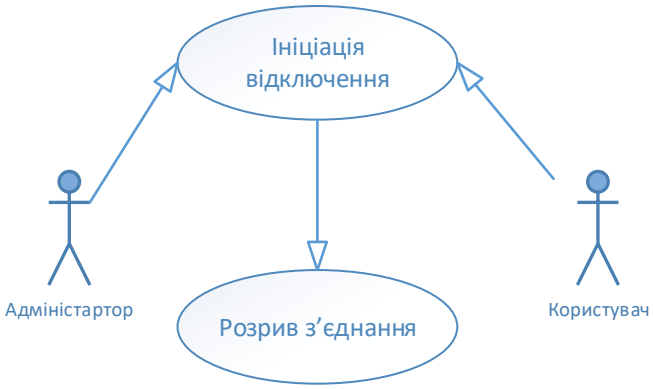


Рисунок 2.10 – Завершення зє'днання

Можливість відключення системи можна здійснювати з обох сторін.

2.3 Діаграма класів

Для опису функціональних можливостей системи скористаємось діаграмою класів (Class Diagram). Діаграма класів – це ще один крок проектування у нотації UML. Діаграми класів, як правило, використовуються

для об'єктно орієнтованого проектування та пропонують, як буде спроектована система [12].

На рисунку 2.11 показана діаграма класів системи моніторингу мережі, що розробляється.

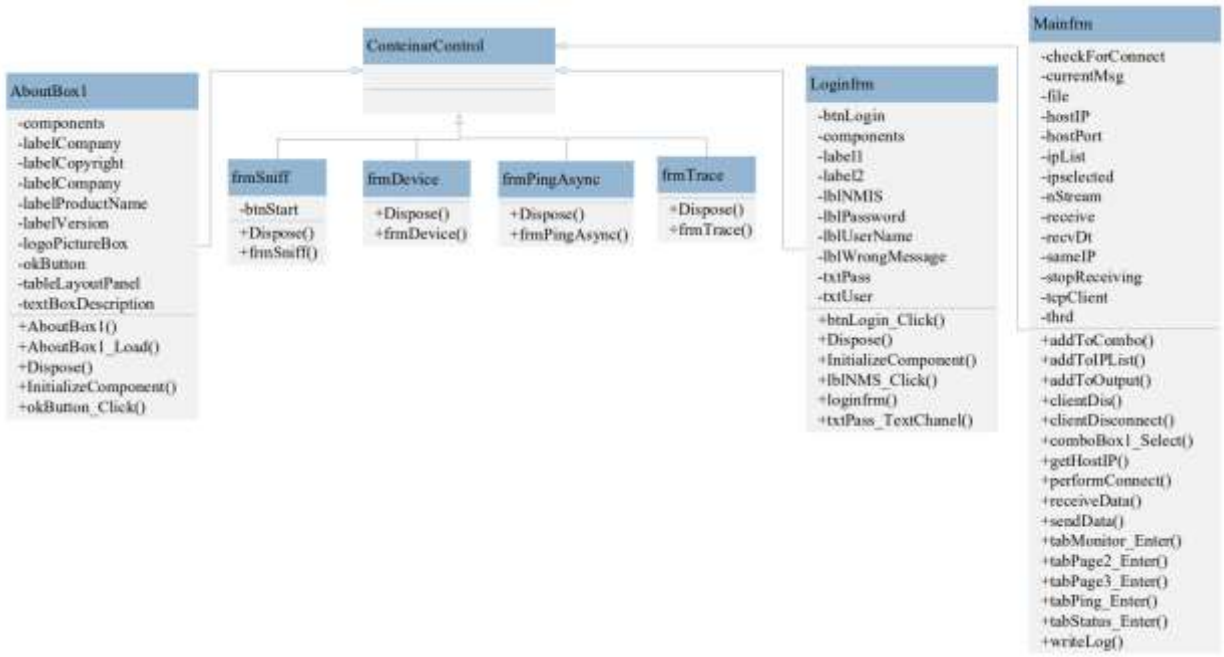


Рисунок 2.11 - Діаграма класів

Діаграма класів UML включає імена класів, відносини між класами, властивості та атрибути, що використовуються при реалізації запропонованої системи.

2.4 Діаграма послідовності

Побудуємо діаграму послідовності (Sequence Diagram), яка детально відображає послідовність взаємодії об'єктів у системі під час виконання певної функції.

На цій діаграмі стрілки представляють методи, а прямокутники – класи. Як правило, необхідна кількість діаграм послідовності має визначатись залежно від характеру застосування. Для додатка, реалізованого в даній

роботі, для процесу підключення, в якому беруть участь і клієнт, і сервер, було створено діаграму послідовності, представлену рисунку 2.12.

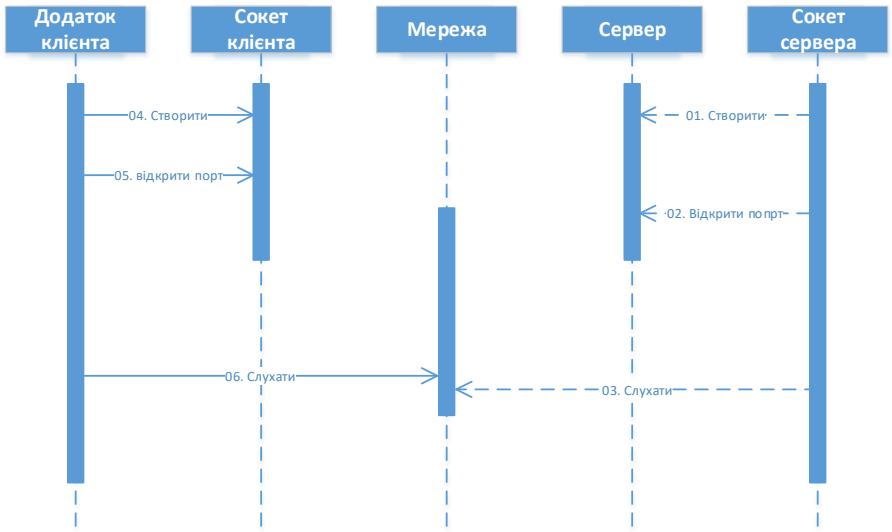


Рисунок 2.12 – Діаграма послідовності, що показує процес підключення

На рисунку 2.13 представлена послідовність дій, що виконується адміністратором.

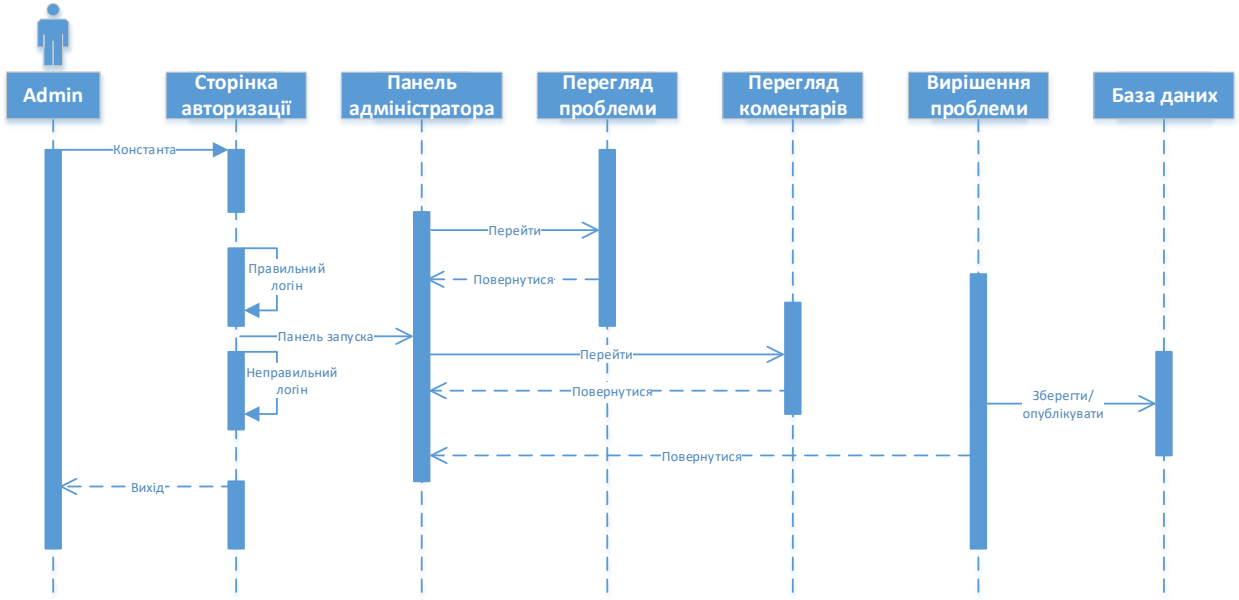


Рисунок 2.13 – Діаграма послідовності для завдань адміністратора

На рисунку 2.14 представлена послідовна дія, що виконується користувачем.

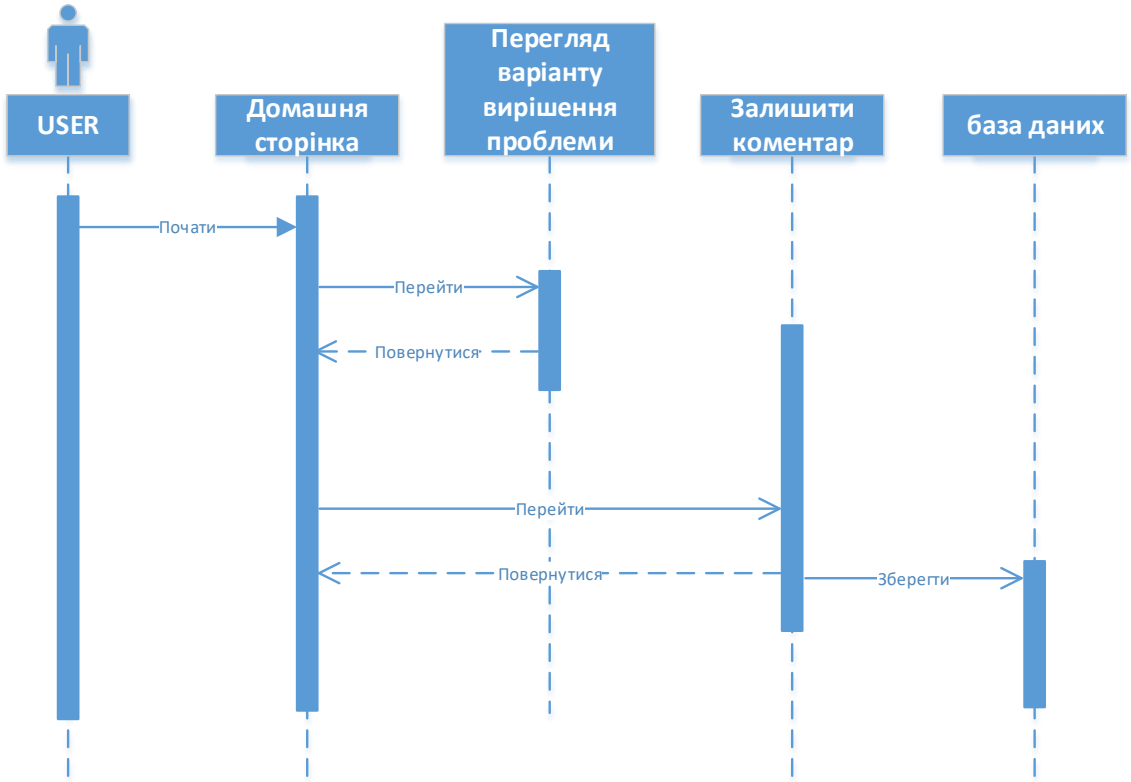


Рисунок 2.14 – Діаграма послідовності для користувача

Діаграма активності представляє структуру складних операцій шляхом поділу всього процесу більш дрібні дії для кращого розуміння функціональності реалізованого докладання. Як видно на рисунку 2.15, діаграма дій для реалізованого додатка представляє структуру дій, що відбуваються в процесі віддаленого доступу.

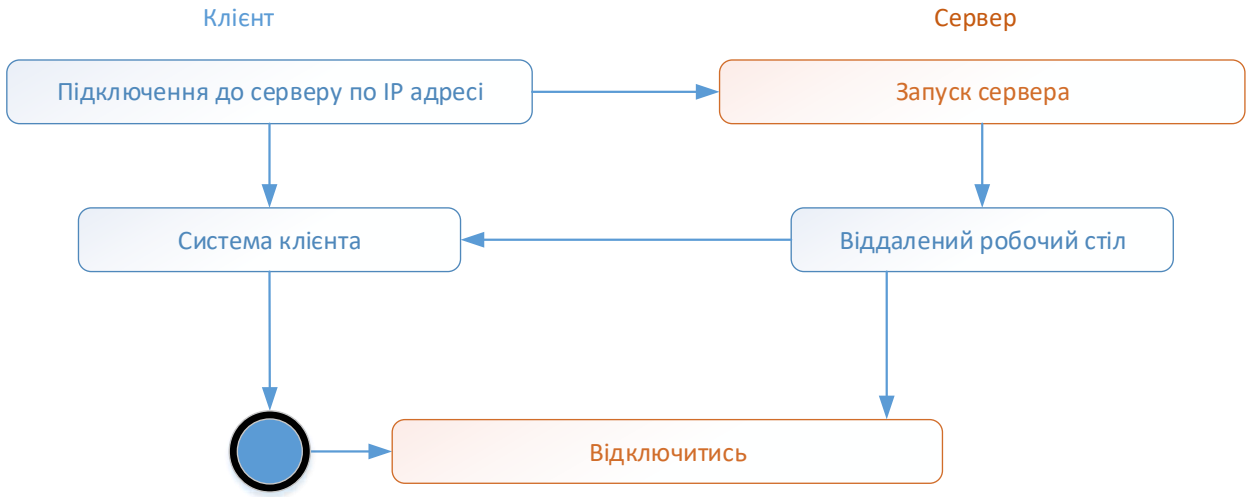


Рисунок 2.15 – Діаграма активності, що показує віддалений доступ

На рисунку 2.16 показано процес, в якому програмне забезпечення системи моніторингу перевіряє доступність віддаленого ресурсу перед запитом даних для моніторингу показників.

Цей процес розпочинається на сервері, де запущено програмне забезпечення системи моніторингу. Перший крок - перевірка доступності віддаленого ресурсу. Для досягнення цього використовується команда ping, яка відправляє невеликий сигнал до віддаленого ресурсу і очікує на відповідь. Це перевіряє, чи можлива подальша взаємодія з ресурсом.

Якщо контрольна точка доступу не пройдена, тобто віддалений ресурс недоступний, процес моніторингу завершується, оскільки неможливо отримати дані для моніторингу. Це важливо для забезпечення точності та надійності системи моніторингу, оскільки неможливо відстежувати показники, якщо ресурс недоступний.

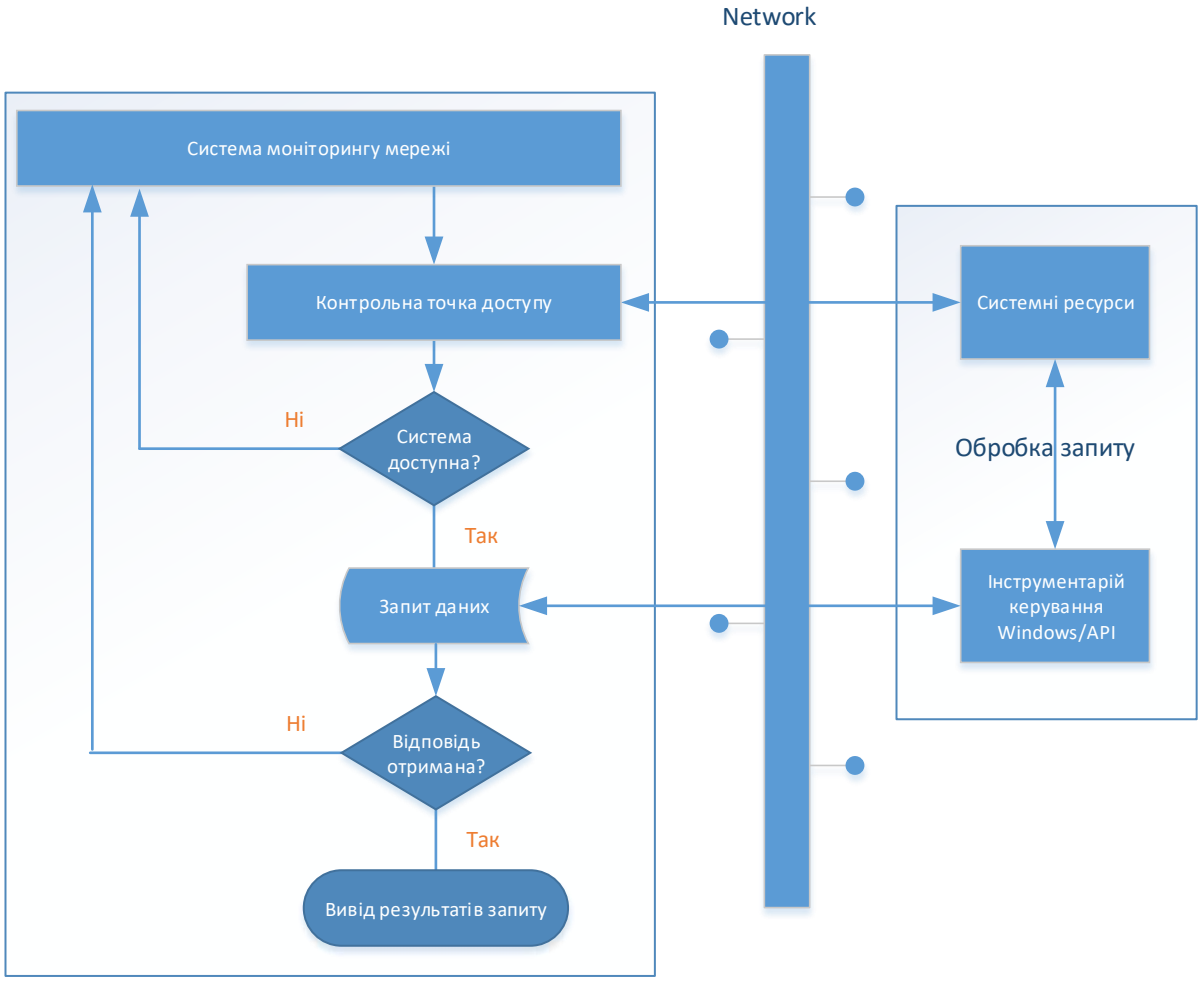


Рисунок 2.16 - Процес перевірки доступності віддаленого ресурсу

У разі успішної перевірки доступності програмне забезпечення системи моніторингу опитує віддалений сервер на наявність однієї події безпеки та трьох подій операційної системи. З'єднання встановлюється за допомогою технології Windows ManagementInstrumentation (WMI) або програми SysinternalsPsLogList, встановленої на сервері моніторингу. Тепер сервер, що відстежується, отримує спеціальні інструкції для звіту про поточні значення запитаних показників. Запит обробляється і дані повертаються на сервер моніторингу.

Результати можуть бути імпортовані безпосередньо до програмного забезпечення системи моніторингу або збережені у локальному файлі.

Структура клієнт-серверної архітектури , яка використовується для реалізації цієї програми, показана на рисунку 2.17.

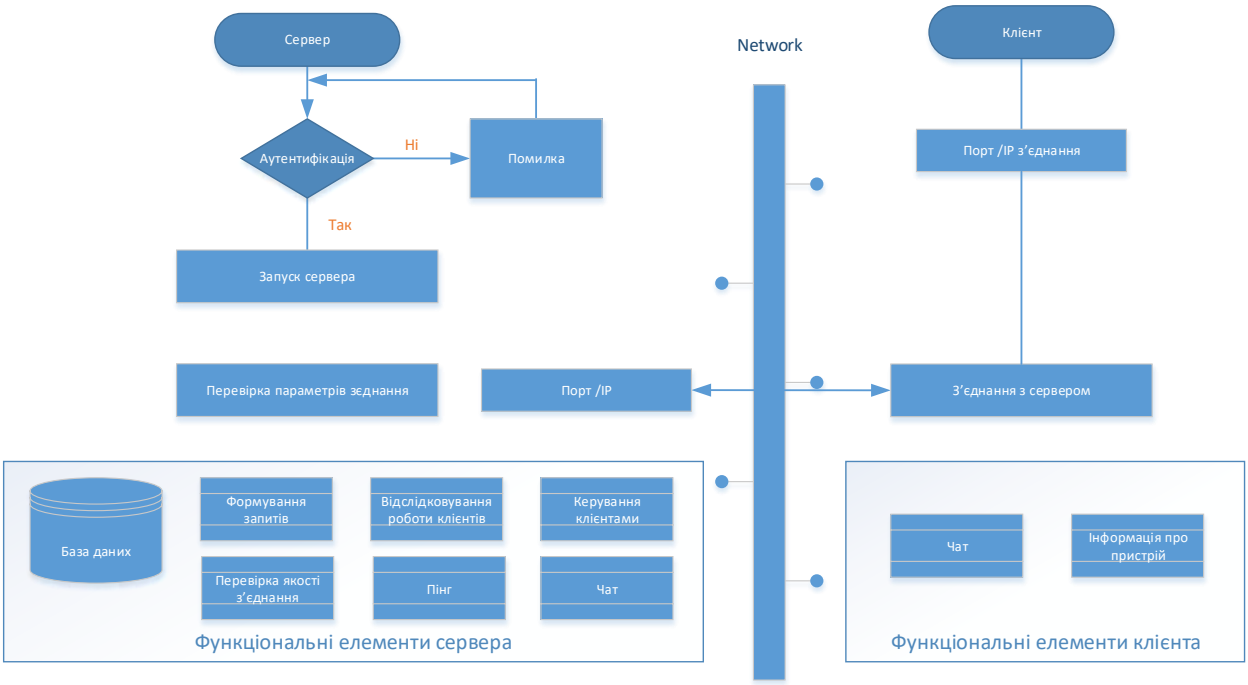


Рисунок 2.17 - Архітектура клієнт-сервер

2.5 Висновки до розділу

В даному розділі були описані концептуальна та логічні моделі проектованої системи моніторингу мережі. Було представлено клієнт-серверну архітектуру системи, включаючи різні компоненти та їх можливості.

Ця інформація надає основу для подальшої реалізації системи моніторингу мережі. Вона визначає, які компоненти повинні бути розроблені і як вони будуть взаємодіяти між собою. Клієнт-серверна архітектура дозволяє ефективно виконувати моніторинг мережі, дозволяючи адміністраторам відстежувати показники та виявляти проблеми.

Загалом, описана модель роботи та архітектура системи моніторингу мережі надають важливі вказівки для подальшого розвитку та реалізації проекту. Вони допоможуть команді розробників у визначенні потрібних функціональностей, взаємозв'язків між компонентами та загального напрямку роботи над системою моніторингу мережі.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

У цьому розділі представлена реалізація запропонованої системи моніторингу мережі. Ця система була реалізована з використанням мови програмування C# серед VisualStudio. Платформа Microsoft .Net - це хороше середовище для мережевих програмістів. Причина вибору C# полягає в тому, що ця мова програмування дозволяє програмістам розробляти мережеві програми з використанням мережевих функцій Windows. Таким чином, щодо використання .Netframework і мови програмування C#, реалізований додаток зможе працювати в операційній системі Windows.

Буде представлена докладна інформація про кожну частину програми. Крім того, структура цієї програми складається з двох частин: серверної та клієнтської. Таким чином, специфікацію кожної частини буде розглянуто окремо.

3.1 Реалізація системи моніторингу мережі організації

Ця програма заснована на архітектурі клієнт-сервер. Базова система побудована на основі наявності цієї програми як на клієнтських, і на серверних пристроях. Оскільки сервер підключено до мережі, клієнтам дозволено підключатися до сервера, використовуючи відповідний номер порту та IP-адресу сервера.

3.2 Серверна частина системи

На стороні сервера можна спостерігати усі функціональні можливості реалізованої системи. На першому етапі було розроблено сторінку входу.

Адміністратор зможе увійти на серверну частину системи, використовуючи наперед задане ім'я користувача та пароль. Ім'я користувача та пароль встановлені в програмі та зберігаються в базі даних.

Секція дистанційного керування. Цей розділ є першим розділом для адміністратора сервера.

У ікладці дистанційного керування, як видно на рисунку 3.1, виділено 4 основні частини: налаштування номера порту, віддалене керування, журнал показу та, нарешті, середовище чату.

Рисунок 3.1 - Дистанційне керування

Першим завданням для сервера має бути встановлення з'єднання, що дозволяє клієнтам підключатися до сервера. Хоча для простоти використання було встановлено попередньо встановлений номер порту, але в разі потреби адміністратор зможе змінити номер порту.

У вкладці дистанційного керування після запуску з'єднання між клієнтом та сервером надаються деякі параметри для використання адміністратором сервера.

На наступному кроці користувач сервера повинен вибрати бажану IP -

адресу клієнта зі списку в цьому вікні. Вибравши кращий клієнт, який є пристроєм, підключеним до сервера, сервер зможе надіслати саме цьому клієнту повідомлення, а також сервер отримає доступ до робочого столу клієнта для виконання необхідних дій. Натиснувши кнопку показати журнал у цьому вікні, адміністратор побачить збережені журнали у визначеній формі журналу.

Як видно на рисунку 3.1, при підключенні кожного клієнта до сервера в чат-частині цієї системи з'явиться повідомлення, що інформує користувача сервера про IP -адресу нового клієнта. Крім того, користувач Сервера, обравши бажану IP -адресу клієнта, зможе виконувати деякі зумовлені операції. Наприклад, у частині віддаленого контролера, після вибору бажаного IP -адреси, сервер може вимкнути пристрій клієнта, натиснувши кнопку віддаленої команди.

Розглянемо вкладку мережних пристроїв. Наступний приклад коду, показаний рисунку 3.2, описує одну з важливих частин цього розділу.

```
     private void frmMain_Load (object sender, EventArgs e)
     { ' try {
     mlndex = -1; NetworkManager . Instance . StarNonitor () ;
mlsAlive = true;
     Ullnvoke = new Metodlnvoker(UpdateUI); Initial();
     thread = New Thread (New Th readstart (UpdateStatus ) )
_thread . Start ( ) ;
     ) ' catch (Exception) {
     Messagebox. Show() } '
     }
```

Рисунок 3.2 – Лістинг коду моніторингу мережі

Спочатку визначено ціле число, яке називається m_Index, має бути порожнім, і для досягнення цієї мети значення встановлюється рівним -1, щоб бути ініціалізованим з 0. Для подання інформації про мережні пристрої хост повинен бути активним. Для перевірки доступності хоста в мережі використовувався вказаний метод StartMonitor. Якщо потрібний хост активний, то інтерфейс користувача повинен бути викликаний за допомогою

MethodInvoker, а потім буде направлений в заздалегідь задане місце в системному інтерфейсі.

Вкладка мережеві пристрої, як видно на рисунку 3.3, поділено на дві частини. Перша частина пов'язана з інформацією про мережні пристрої, яку можна вибрати з попередньо встановленого меню. Друга частина — це системне зведення, в якому відображатиметься інформація про вибраний мережевий пристрій.

Таким чином, при виборі кожного жевого пристрою, представленого в меню, що розкривається, відповідна інформація буде автоматично відображатися у вказаному місці.

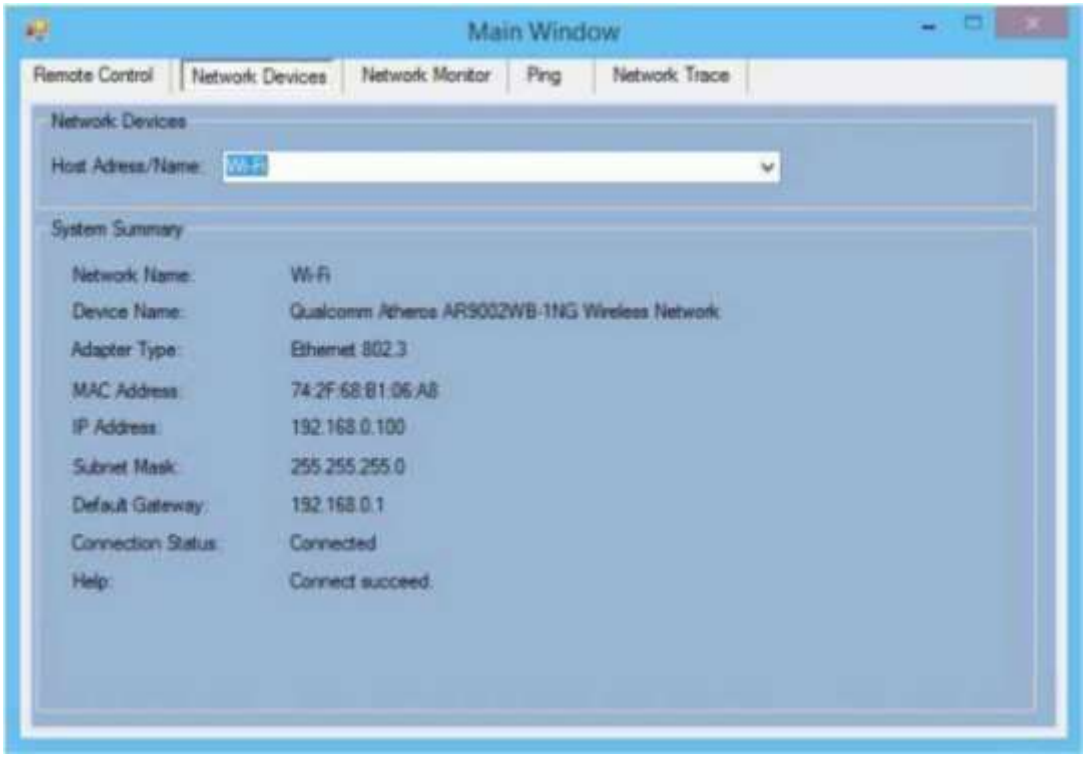


Рисунок 3.3 – Інформація про мережевий пристрій

На рисунку 3.3 вибрано з'єднання Wi-Fi, і надано всю необхідну інформацію.

Наприклад, інформація про марку процесора Wi-Fi карти, яка використовується у серверному пристрої. Цей приклад показаний у рядку імені пристрою. Також, показано стан з'єднання. У цьому прикладі з'єднання

успішно встановлено і, відповідно, допомоги не буде необхідності. У разі виникнення проблем із встановленням з'єднання в розділі довідки буде надана інформація для усунення проблеми.

У вкладці мережевий монітор користувач сервера зможе вибрати бажану IP -адресу з меню. При натисканні кнопки «Старт» вся інформація про пакети, надіслані або отримані з вибраної IP- адреси, буде відображатися у наведеному нижче вікні. Також зібрану інформацію можна очистити за допомогою кнопки поруч із кнопкою «Старт/Стоп» (рисунок 3.4).

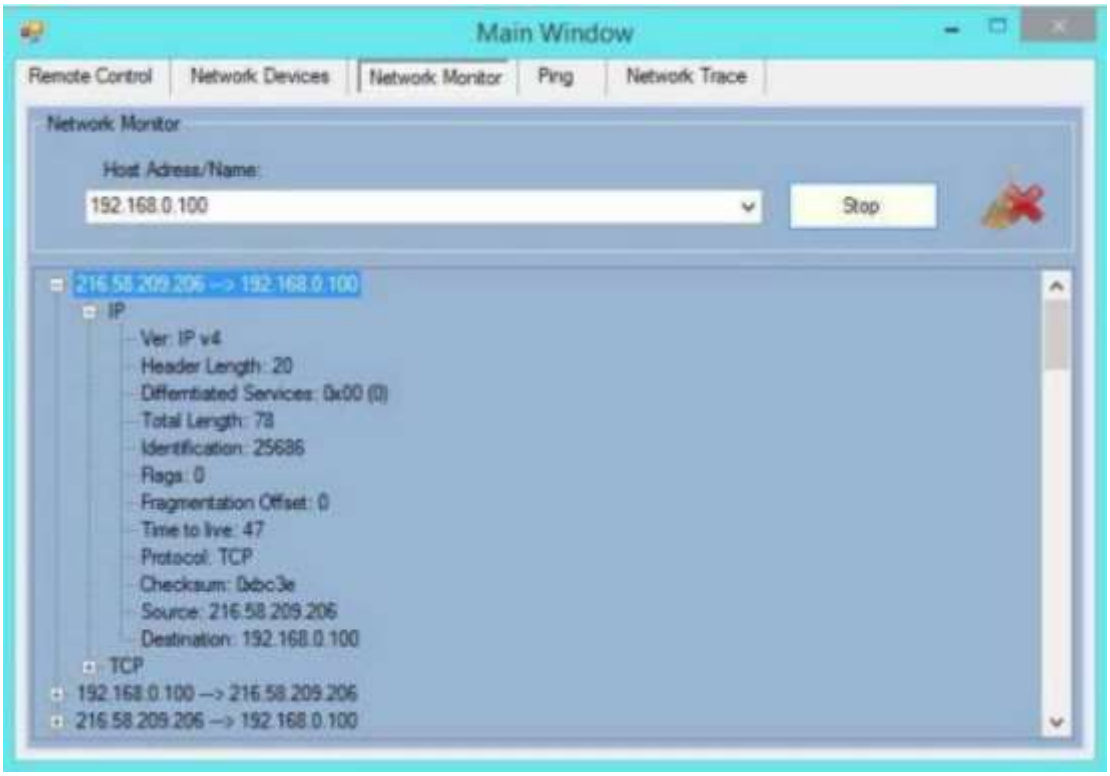


Рисунок 3.4 - Мережевий монітор показує IP

У цьому прикладі на рисунку 3.4 один з пакетів відкривається, щоб показати докладну інформацію про нього. У цьому прикладі детальна інформація виводиться по протоколу IP, в якому представлена версія IP, довжина заголовка пакета, протокол, IP -адреси джерела та одержувача та інша інформація. Надана інформація, як було описано вище, допомагає користувачеві сервера знати дії, які були виконані через мережу обраним клієнтом.

Протокол користувальницьких дейтаграм (UDP) — це протокол зв'язку, що пропонує обмежений обсяг послуг під час обміну повідомленнями між комп'ютерами у мережі, що використовує Інтернет-протокол (IP).

На рисунку 3.5 показаний приклад представлення розділу UDP, у якому дано докладну інформацію.

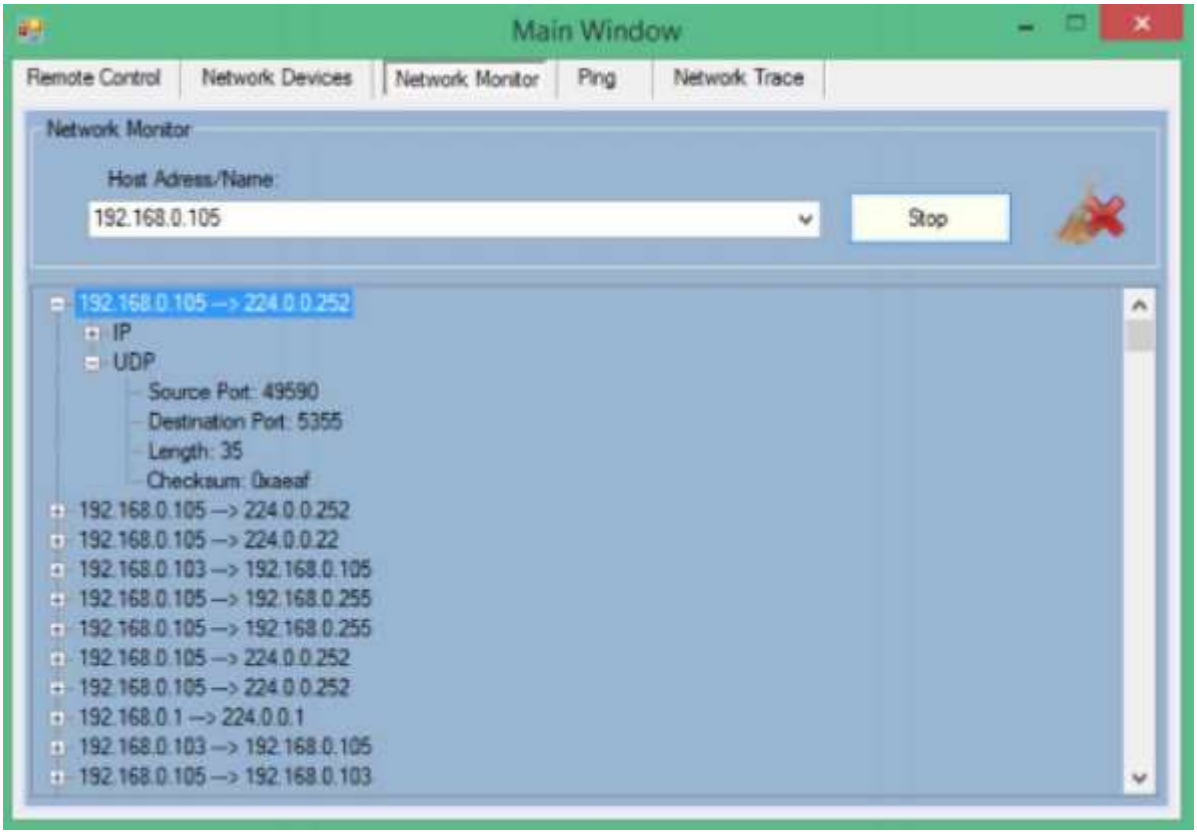


Рисунок 3.5 - Монітор показує UDP

Як видно на рисунку 3.5, інформація, представлена в розділі мережевого моніторингу, включає порт, що використовується в джерелі і одержувачі, довжину повідомлення і контрольну суму.

На рисунку 3.6 показаний приклад представлення розділу TCP. У цьому прикладі подана докладна інформація про заголовок кожного пакета, що передається по мережі, в розділі TCP.

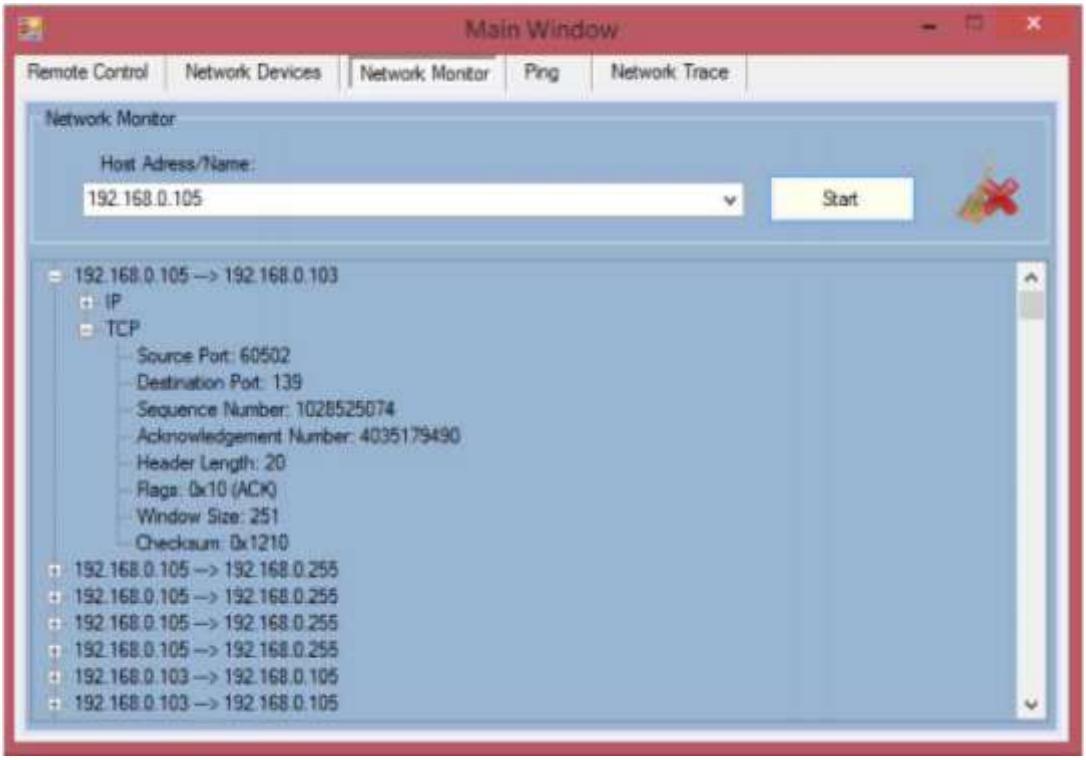


Рисунок 3.6 - Моніторинг мережі (демонстрація TCP)

Як видно з рисунку 3.6, інформація, представлена в цьому розділі, включає номер порту джерела та одержувача, порядковий номер пакета, номер підтвердження, довжину заголовка, прапори тощо.

На рисунку 3.7 показаний приклад уявлення розділу системи доменних імен (DNS). У цьому прикладі показано докладну інформацію про заголовки пакетів у розділі DNS.

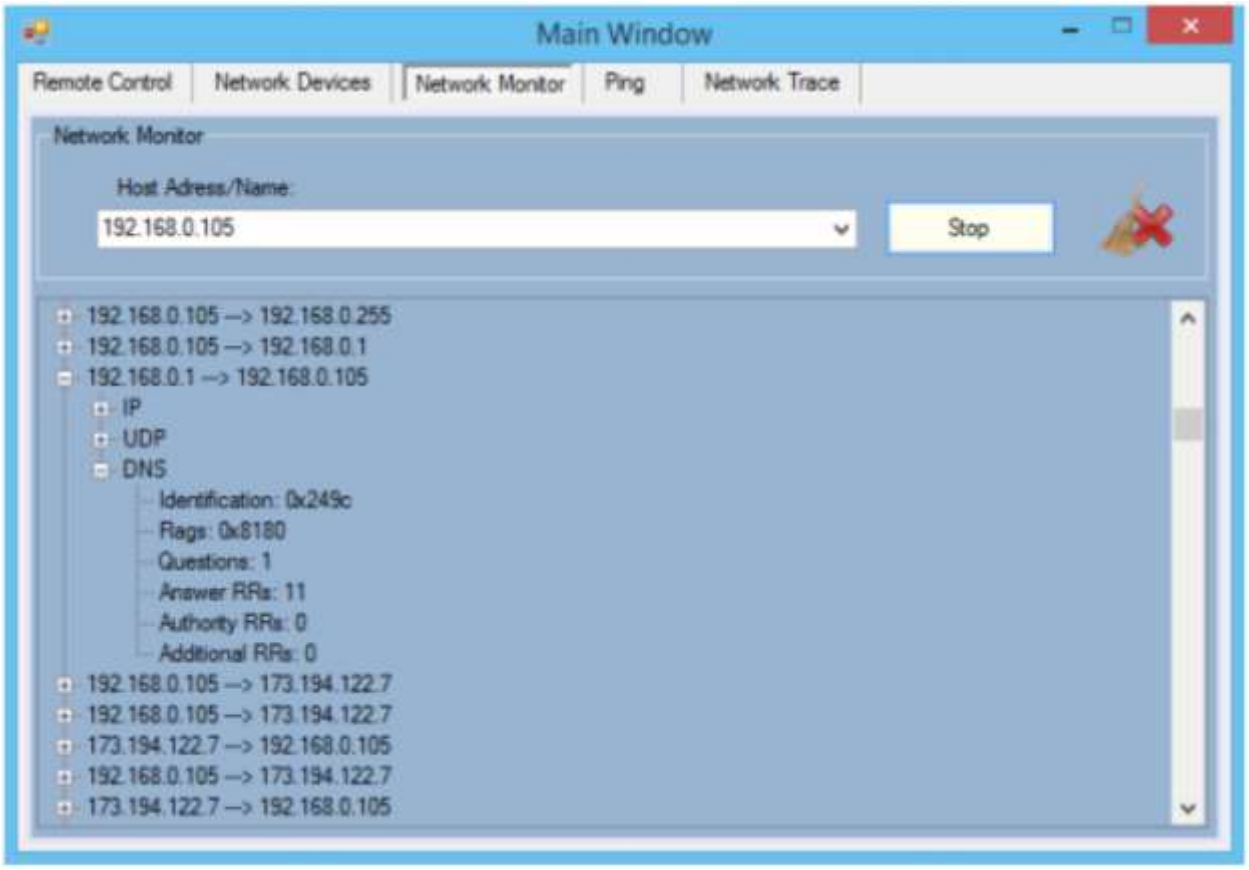


Рисунок 3.7 - Моніторинг мережі (демонстрація DNS)

Як видно на рисунку 3.7, інформація, представлена в цьому розділі, являє собою ідентифікаційний номер, прапори, кількість питань, кількість записів ресурсів відповідей (RR), кількість авторитетних RR та кількість додаткових RR.

Розглянемо докладніше розділ перевірки зв'язку. Приклад коду методу ping можна побачити рисунку 3.8.

Ця частина код розділена на дві умови, пов'язані з місцем для вставки імені хоста або IP -адреси. Перше умова пов'язана з нульовим значенням, що означає, що у текстової області нічого написано. В цьому випадку в передбаченому для збору інформації методом ping нічого не з'явиться. В іншому випадку програма почне застосовувати метод ping до адреси 4 рази за методом BeingPingHost, виходячи зі значення AsyncCallback. Результат цієї частини буде відображатися у вказаному місці, яке є полем списку. Друга умова пов'язана із збереженням результату в лог-листі. Якщо текстова область

не була нульовою, результат буде збережено в визначеному аркуші журналу.

```
     private   void   cmdPing_Click(object   sender,   System   .
EventArgs e)
   { ''''
     if (txtHostname.Text == null || txtHostname .Text . Length
== 0) return;
     cancel = false;
     lstResponses . Items .Clear ( ) ;
     result = netMon . BeginPingHost(New AsyncCallback(EndPing),
txtHostname, Text, 4);
     if (result != null)
   < ...
     cmdCancel.Visible = true;
     writelog("Ping \t + txtHostname. text + "\t- " + System .
Datetime . Now.ToString());" )
   } '
   }
```

Рисунок 3.8 – Лістинг фрагмента методу Ping

У розділі ping користувач сервера вставляє IP -адресу або ім'я бажаного хоста в текстове поле і, натиснувши кнопку «Пуск», вся інформація буде відображатися у вказаному місці нижче. Дана інформація буде про хост і показує серверу, що вибраний хост працює чи не працює. Рисунок 3.9 представляє розділ ping.

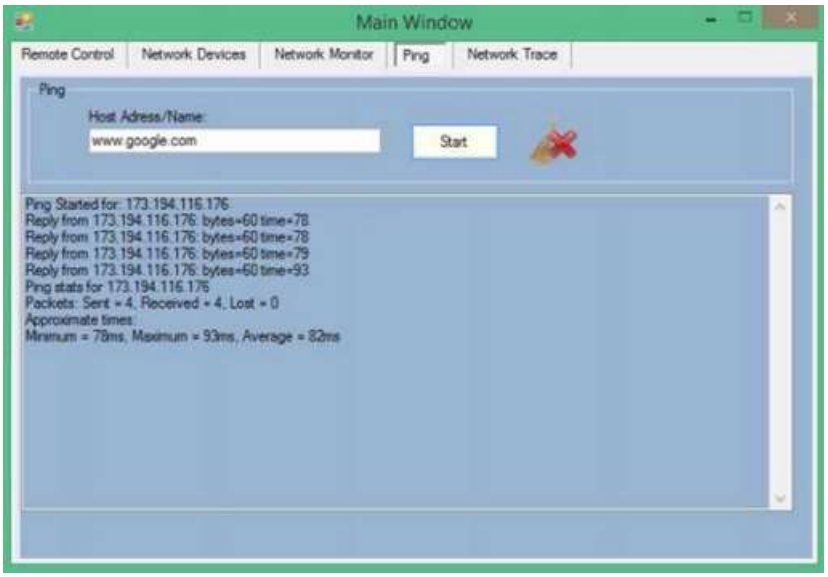


Рисунок 3.9 - Секція перевірки зв'язку

У наведеному прикладі, показаному на рисунку 24, наведено метод ping для веб-сайту Google з використанням його імені, а також показано всі процеси відправлення та отримання пакетів для встановлення з'єднання між серверним пристроєм і хостом. Ping виконується шляхом відправлення пакетів запиту на хост-отримувач та очікування відповіді. У цьому процесі він розраховує час від відправки до відповіді та записує будь-які втрати пакетів. Результати в цьому прикладі представлені у вигляді інформації про мінімальний, максимальний і середній час цього процесу, а також інформації про втрату пакетів, відправлених та отриманих пакетах.

Приклад коду розділу мережевого трасування показано на рисунку 3.10. Як видно з прикладу коду, IP -адреса або ім'я хоста, які були вставлені в дану текстову область доступні. Потім наданий список елементів для відображення інформації буде очищений, щоб бути готовим до нової інформації про трасування. Для відстеження мережі маршрут між хостом та сервером буде досліджуватися за допомогою методу tracert.Trace. Інформація, що відображається про цей процес буде зберігатися в журналі.

```
      private void startTrace_Click(object sender, EventArgs e)
      {''''try
      {
      tracert.HostNameOrAddress = destination.Text;
      routeList.Items.Clear() ;
      tracert.Trace();
      writeLog("Trace  \t"  +  destination.Text  +  "\t-  "  +
System.DateTime.Now.ToString())
      catch (SockedException ex) {
      Messagebox.Show(ex.Message, "Tracert Demo");
```

Рисунок 3.10 - Лістинг частини мережевого трасування

Як показано на рисунку 3.11, у закладці трасування мережі адміністратор сервера зможе вставити бажану IP -адресу хоста у надану область. При натисканні кнопки запуску вся інформація про шлях між серверним пристроєм та вибраним хостом відображатиметься у даному середовищі.

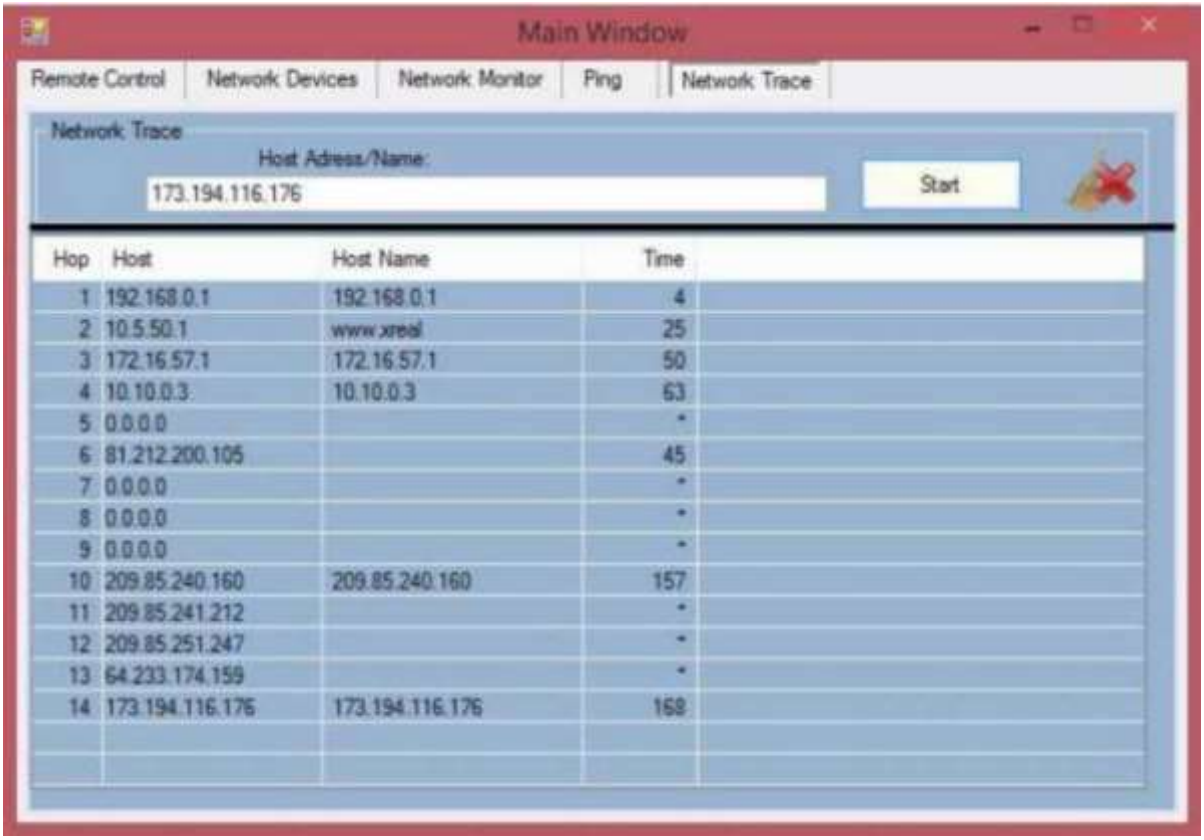


Рисунок 3.11 - Трасування мережі

У наведеному прикладі, показаному на рисунку 3.11, показаний шлях між серверним пристроєм і бажаною IP- адресою, якою в даному прикладі є IP - адреса www.google.com. Інформація містить маршрутизатори та точки доступу, що знаходяться в середині шляху між серверним пристроєм та веб-сайтом Google. Слід зазначити, що IP- адреси міжнародних маршрутизаторів не будуть ідентифіковані з міркувань безпеки. Однією з наданих відомостей є IP -адреса мережевих пристроїв у середині шляху між сервером та пунктом призначення. Інша інформація - це ім'я хоста, яке у разі наявності будь-якого імені відображатиметься. Час, як і інша інформація, вимірюється у мілісекундах. Час пов'язаний з розрахунковим часом отримання пакету кожним мережевим пристроєм на маршруті.

У розділі серверної частини слід враховувати, що пристрій сервера повинен мати статичну IP -адресу. У разі наявності динамічної IP - адреси в розділі моніторингу мережі IP -адреса клієнта не буде відображатися в списку,

що розкривається. Причина в тому, що ця система реалізована на третьому рівні TCP/IP, тобто на рівні мережі.

3.3 Клієнтська частина

На стороні клієнта цієї програми, як показано на рисунку 3.12, було надано деякі опції для підключення клієнта до сервера.

Рисунок 3.12 - Сторона клієнта

Вставивши IP -адресу сервера, а також встановивши номер порту, який повинен збігатися зі встановленим номером порту на стороні сервера, клієнт зможе підключитися до системи сервера. Після цього кроку клієнт зможе спілкуватися із сервером.

Наведений приклад, показаний на рисунку 3.12, показує надіслані повідомлення від клієнта до сервера.

У звіті про доступність (рис. 3.13) показані статуси станів серверного

обладнання по часом. Звіт сформовано протягом місяця.

Різними кольорами виділено такі стани:

– червоний – сервер вимкнений або не працює;

– зелений - повна працездатність;

– жовтий - агент не підключений до цього обладнання;

– сірий - простий обладнання.

Рисунок 3.13 - Звіт про доступність обладнання

Звіт дозволяє відстежити за будь-який період часу працездатність серверів та іншого обладнання, що дуже зручно для адміністратора, тому що показує статистику роботи обладнання. Також можна налаштувати цей звіт, щоб він приходив на електронну пошту як адміністратору, так і керівництву, для аналізу критичних ситуацій і швидкого прийняття рішень. Можливо, потрібен терміновий ремонт обладнання або перерозподіл навантаження.

3.4 Висновок до розділу

Було розроблено додаток, який базується на клієнт-серверній архітектурі. Система моніторингу була налаштована як на клієнтських, так і на серверних пристроях. Шляхом підключення сервера до мережі, клієнти

отримали можливість з'єднуватися з сервером, використовуючи відповідний номер порту та IP-адресу сервера.

Результатом реалізації системи моніторингу локальної мережі в організації стало визначення працездатності серверів та іншого обладнання протягом певного періоду часу. Система показала здатність до оцінки працездатності та надійності, що дозволяє вчасно виявляти проблеми та усунути їх.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при ураженні електричним струмом.

Так як мета роботи пов’язана з використанням різних електроприладів, що підключені до електричної мережі розглянемо питання дій при ураженні електричним струмом.

Перш за все, звільнити потерпілого від дії струму, оскільки від тривалості такої дії суттєво залежить важкість електротравми. Найбезпечніший спосіб звільнення потерпілого від дії електричного струму – це вимкнення електроприладу, до якого доторкається потерпілий, за допомогою найближчого вимикача, рубильника чи іншого апарата для знеструмлення.

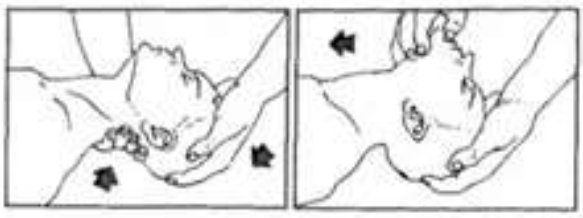
Потерпілий, після звільнення від дії електричного струму, зазвичай може перебувати в одному з трьох станів:

– Якщо потерпілий при свідомості, то його необхідно покласти на підстилку з тканини чи одягу, створити приплив свіжого повітря, розстібнути одяг, що стискає та перешкоджає диханню, розтерти та зігріти тіло і забезпечити спокій до прибуття лікаря.

– Потерпілому, що знаходиться в непритомному стані, треба дати понюхати нашатирний спирт або збризнути обличчя холодною водою. Коли потерпілий прийде до тями, дати йому випити 15-20 крапель настоянки валеріани та гарячого чаю.

– За відсутності ознак життя (дихання та пульсу) потрібно негайно розпочати серцево-легеневу реанімацію (СЛР), адже імовірність успіху тим менша, чим більше часу минуло від початку клінічної смерті. До заходів СЛР належать штучне дихання та непрямий масаж серця.

Штучне дихання виконується способом "з рота в рот" або "з рота в ніс". Людина, яка надає допомогу, робить видих зі своїх легень у легені потерпілого безпосередньо в його рот чи ніс, у повітрі, що видихається людиною є ще досить кисню. Попередньо потерпілого необхідно покласти спиною на тверду рівну поверхню, звільнити від одягу, що стискає (розстебнути комір сорочки, пасок, послабити краватку), підкласти під лопатки невеликий валик з будь-якого матеріалу, відхилити голову максимально назад (рис. 4.1).



а б

Рисунок 4.1 – Правильне положення голови потерпілого

а – рятівник відхиляє голову потерпілого лівою рукою, одночасно підтримуючи його шию правою;

б – рятівник утримує голову потерпілого у відхиленому положенні лівою рукою, відтягуючи одночасно нижню щелепу правою рукою.

Перш ніж розпочати штучне дихання, необхідно переконатися в прохідності верхніх дихальних шляхів, які можуть бути закриті запалим язиком, сторонніми предметами, накопиченим слизом [12, с.240].

Рятівник робить глибокий вдих, а потім, щільно притиснувши свій рот через марлю до рота потерпілого (при цьому, як правило, закриває ніс потерпілого своєю щокою), вдуває повітря в легені, як зображено на рис. 4.2. При цьому грудна клітка потерпілого розширяється. За рахунок еластичності легень та грудної стінки потерпілий робить пасивний видих. У цей час його рот повинен бути відкритим. Частота вдування повітря повинна становити 12 разів за хвилину. Аналогічно виконується штучне дихання способом "з рота в

ніс"; при цьому вдувають повітря через ніс, а рот потерпілого повинен бути закритим.

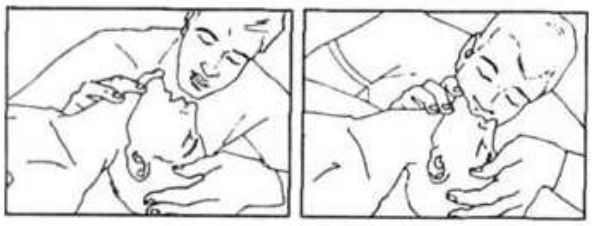


Рисунок 4.2 – Штучне дихання способом "з рота в рот"

При проведенні штучного дихання слід бути уважним: коли у потерпілого з'являються перші ознаки слабкого поверхневого дихання, необхідно до нього пристосувати ритм штучного дихання.

Існують спеціальні засоби для штучного дихання, які, перш за все, дозволяють уникнути прямого контакту між ротом потерпілого та ротом рятівника. Для того, щоб не завдати шкоди потерпілому, рятівник повинен уміти користуватись такими засобами.

У випадку зупинки серця, яку можна визначити за відсутністю у потерпілого пульсу на сонній артерії та розширенням зіниць або у разі фібриляції серця, необхідно одночасно зі штучним диханням проводити непрямий масаж серця. Потерпілого кладуть спиною на тверду поверхню, оголюють його грудну клітку, розстібають пасок. Рятівник стає ліворуч або праворуч від потерпілого, поклавши на нижню третину грудної клітки кисті рук (одна на одну), енергійно (поштовхами) натискає на неї. Натискати потрібно досить різко, використовуючи при цьому масу власного тіла, і з такою силою, щоб грудна клітка прогиналась на 4-5 см у бік хребта. Необхідна частота становить 60-65 натиснень на хвилину [12, с.241].

Масаж серця необхідно поєднувати зі штучним диханням. Якщо СЛР виконує одна людина, то заходи щодо рятування потерпілого необхідно проводити в такій послідовності: після двох глибоких вдувань у рот чи ніс зробити 15 натиснень на грудну клітку, потім знову повторити два вдування і

15 натиснень для масажу серця. Якщо допомогу надають двоє рятівників, то один повинен робити штучне дихання, а інший – непрямий масаж серця, причому під час вдування повітря масаж серця припиняють,

Заходи щодо оживлення можна вважати ефективними, якщо звузились зіниці, шкіра почала рожевіти (у першу чергу, шкіра верхньої губи), при масажних поштовхах явно відчувається пульс на сонній артерії.

Таким чином вміле надання допомоги при ураженні електричним струмом зможе спасти людині життя.

4.2 Загальні вимоги безпеки з охорони праці для користувачів ПК

Виконуючи роботи по моніторингу і адмініструванню локальної мережі необхідно дотримуватись вимог безпеки з охорони праці.

Через масовий характер робіт, що виконуються працівниками за допомогою комп'ютера, законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером [9].

Мінімальні вимоги безпеки та захисту здоров'я під час роботи, пов'язаної з використанням екранних пристроїв незалежно від їхнього типу та моделі, визначають Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, затверджені наказом Міністерства соціальної політики України від 14 лютого 2018 р. № 207 (далі — НПАОП 0.00-7.15-18) [10].

Приміщення, в яких планується установка та подальша робота з комп'ютерним обладнанням, повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, необхідно враховувати санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики

електромагнітного, ультрафіолетового та інфрачервоного полів. Конкретні показники зазначених санітарних норм визначені в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, затверджених Постановою Головного державного санітарного лікаря України №7 від 10 грудня 1998 року.

Правила поширюються на умови й організацію праці при роботі з візуальними дисплейними терміналами (ВДТ) усіх типів. Так, наприклад, роботодавцю заборонено установлювати комп'ютери в приміщеннях, розташованих у підвалах будинків. Для уникнення можливих аварій та замикань, поряд з приміщеннями, де вестиметься робота з комп'ютером (над чи під ними), також не дозволяється проведення робіт, що потребують здійснення надмірно вологих технологічних процесів. Відповідне приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря.

У кожній кімнаті, де обладнуватимуться робочі місця де працюватимуть на комп'ютері, повинні бути наявні елементи природного та штучного освітлення. При цьому, на вікнах слід встановити легко регульовані жалюзі чи штори, які дозволять працівникам коригувати рівень освітлення в приміщенні. Бажано розмістити комп'ютери в кімнаті таким чином, щоб світло потрапляло на екрани моніторів з півдня чи північного сходу. З метою досягнення максимального рівня безпечності і охорони праці при роботі з комп'ютером, виробничі приміщення необхідно обладнати аптечками першої медичної допомоги, системами автоматичної пожежної сигналізації і вогнегасниками. В приміщенні, в якому разом працюють 5 або більше комп'ютерів, на видимому місці установлюється службовий вимикач, який у разі потреби дозволить повністю відключити електричне живлення кімнати.

У виробничих приміщеннях на робочих місцях з візуальними дисплейними терміналами (ВДТ) забезпечуються оптимальні значення

параметрів мікроклімату: температури, відносної вологості й рухливості повітря відповідно до ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ВДТ, відповідають вимогам ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Інтенсивність потоків інфрачервоного випромінювання не перевищує допустимих значень, згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Інтенсивність потоків ультрафіолетового випромінювання не перевищує допустимих значень згідно з СН 4557-88 (ДНАОП 0.03-3.17-88) «Санітарні норми ультрафіолетового випромінювання у виробничих приміщеннях».

Організація робочого місця з ВДТ забезпечує відповідність конструкції всіх елементів робочого місця та їх взаємного розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності згідно з ДСТУ ISO 9241-5:2004 «Ергономічні вимоги до роботи з відеотерміналами в офісі».

У даному розділі були розглянуті питання безпеки життєдіяльності і охорони праці, які спрямовані на підвищення безпеки роботи на підприємствах. Охорона праці та безпека життєдіяльності є важливими аспектами в усіх галузях діяльності, оскільки вони спрямовані на запобігання нещасним випадкам та захист працівників від потенційних ризиків та небезпек.

ВИСНОВКИ

У рамках даної роботи були розглянуті концепції моніторингу мережі, віддаленого доступу. Було проведено дослідження аналогічних робіт, що раніше виконувались у цій галузі, та зроблено порівняння між додатком що проектується та існуючими інструментами. Крім того, були детально пояснені процеси, процедури та умови впровадження розробленого додатку крок за кроком.

Було встановлено, що інструменти моніторингу продуктивності є важливим активом для системних адміністраторів, оскільки вони дозволяють постійно відстежувати роботу мережі на основі зібраних даних у регулярних інтервалах часу.

Моніторинг мережі включає перевірку коректності функціонування цих пристроїв, а також забезпечення доступності зв'язку та необхідну інфраструктуру для безперебійної роботи обчислювальної системи організації. Запропоноване рішення є аналогічним існуючим системам, але має інтерактивний інтерфейс та можливість швидкого обміну повідомленнями через чат.

Основною метою даного проекту було створення простої у використанні комп’ютеризованої системи моніторингу мережі, яка містить більшість необхідних функцій. Моніторинг та аналіз пакетів дозволяє адміністратору користувача контролювати безпеку всієї мережі.

Розроблена система відповідає всім поставленим функціональним вимогам, зокрема:

– Система може вирішити проблему, з якою зіткнувся клієнт, і дозволяє клієнту опублікувати цю проблему.

– Інформація зберігається у базі даних, до якої має доступ уповноважений персонал.

– Забезпечується краще управління IP-адресами.

Комп’ютеризована система управління мережею може успішно вирішити всі поставлені перед нею завдання, включаючи:

– Безпечну роботу для надсилання відомостей про проблему.

– Розроблену універсальну базу даних для обміну даними про записи проблем.

– Систему, яка буде запитувати інформацію про проблеми та рішення відносно клієнтів, відділів та будівель з будь-якого місця.

Отже, була реалізована система моніторингу локальної мережі в організації, яка демонструє здатність оцінювати працездатність серверів та іншого обладнання протягом певного періоду часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SolarWinds Network Performance Monitor (NPM). URL: https://softprom.com/vendor/solarwinds/product/solarwinds-network-performance-monitor-npm- (дата звернення: 30.05.2023).
2. Monitor your network with the network monitoring tool PRTG. URL: https://www.paessler.com/network_monitoring_tool (дата звернення: 18.05.2023).
3. Nagios Network Analyzer. Netflow Analysis, Monitoring, and Bandwidth Utilization Software. URL: https://www.nagios.com/products/nagios-network-analyzer/ (дата звернення: 17.05.2023).
4. Огляд Zabbix URL: https://www.zabbix.com/documentation/6.0/ua/manual/introduction/overview (дата звернення: 17.05.2023).
5. CSS: Український веб-довідник. URL: https://css.in.ua/ (дата звернення: 30.05.2023).
6. Trusted network and server monitoring software for over 15 years. URL: https://www.manageengine.com/network-monitoring/ (дата звернення: 30.05.2023).
7. Приклади tcpdump в Linux. URL: https://uk.soringpcrepair.com/examples-tcpdump-in-linux/ (дата звернення: 30.05.2023).
8. Аналізатор пакетів Wireshark. URL: http://eportal.ho.ua/inform/im_Wireshark.pdf (дата звернення: 30.05.2023).
9. Софт для локальної мережі. локальні мережі. URL: https://gadgets-room.ru/software-for-the-local-network-local-area-networks/ (дата звернення: 30.05.2023).
10. Martin Fowler UML Distilled: A Brief Guide to the Standard Object Modeling Language 3rd Edition Addison-Wesley Professional; 3rd edition, 2003. 208 p.

11. SNMP протокол (основи). URL: https://www.k-max.name/linux/snmp-protocol/ (дата звернення: 18.05.2023).

12. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyi R. Technology of relational database management systems performance evaluation during computer systems design. Scientific Journal of TNTU.Tern.: TNTU. 2023. Vol 109. No 1. P. 54–65.

13. Yatsyshyn V., Pastukh O., Zharovskyi R., Shabliy N.Software tool for productivity metrics measure of relational database management system. Mathematical Modeling. No 1 (48). 2023. P. 7-17.

14. Катренко Л.А., Катренко А.В. Охорона праці в галузі комп'ютинґу. Львів: Магнолія-2006. 2012. 544 с.

15. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Київ. 2018.

16. Бедрій Я. Основи охорони праці користувачів персональних комп'ютерів: навчальний посібник для студентів ВНЗ та інженерів-практиків. Навчальна книга-Богдан. 2014. 144 с.

17. Жидецький, В. Ц. Основи охорони праці : підручник / В. Ц. Жидецький. – Вид. 3-є, перероб. і доп. – Львів : Українська академія друкарства, 2006. - 200 с.

18. Осухівська Г.М., Тиш Є.В., Луцик Н.С., Паламар А.М. Методичні вказівки до виконання кваліфікаційних робіт здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль, ТНТУ. 2022. 28 с.

Додаток А.

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп’ютерно-інформаційних систем і програмної інженерії

Кафедра комп’ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС

_____ Осухівська Г.М.

“___” _____2023 р

СИСТЕМА МОНІТОРИНГУ ТА АДМІНІСТРУВАННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

ТЕХНІЧНЕ ЗАВДАННЯ

на _*9*_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІс-41
_____ к.т.н., ст.викл. Стадник Н. Б.	_____ Дюк П. П.
«____» _____ 2023 р.	«____» _____ 2023 р.

Тернопіль 2023

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Система моніторингу та адміністрування комп’ютерної мережі організації».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.349.00.00

1.2 Виконавець

Студент групи СІс-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Дюк Петро Павлович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№4/7-237 від 28.02.2023 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 02.03.2023 р.

Плановий термін завершення виконання кваліфікаційної роботи – 19.06.2023 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ISO, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи. Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Система моніторингу що розробляється призначена для:

– Збору інформації функціонування компонентів локальної мережі,
– Аналізу протоколів які використовуються в локальній мережі,
– Системи комунікації між користувачами і адміністратором.

2.2 Мета створення системи

Метою КРБ є проектування та реалізація системи моніторингу локальної мережі організації.

2.3 Характеристика об'єкту

Характеристика об'єкту проектування, для якого розробляється система моніторингу програмного забезпечення:

1. Організація. Об'єктом проектування є організація, яка володіє локальною мережею.
2. Локальна мережа. Ця мережа може бути заснована на провідному або безпровідному з'єднанні і дозволяє обмін даними та ресурсами між комп'ютерами.
3. Комп'ютери. У локальній мережі розташовані різноманітні комп'ютери, які використовуються в організації.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

3.1.1 Вимоги до структури та функціонування системи

Комп’ютерна система моніторингу порграмного забезпечення повинна складатись з:

– Клієнтська частина. Це програмне забезпечення, що відповідає за збір даних та надсилання цих даних на сервер моніторингу, а також дозволяє здійснювати комунікацію між користувачем і адміністратором.

– Сервер моніторингу. Це центральний компонент системи, який отримує дані від агентів і зберігає їх для подальшої обробки та візуалізації. Сервер може мати базу даних для зберігання історичних даних, а також може виконувати аналіз і сповіщення про стан програмного забезпечення.

– Інтерфейс користувача. Інтерфейс, який дозволяє адміністратору переглядати та аналізувати дані моніторингу. Через інтерфейс користувач

може переглядати статистику, отримувати сповіщення про проблеми, налаштовувати моніторингові правила тощо.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Основна вимога, яка ставиться до способів та засобів інформаційного обміну – це їх узгодженість.

3.1.3 Вимоги до режимів функціонування системи

Для системи визначено два режими функціонування:

– нормальний режим функціонування;

– аварійний режим функціонування.

Основним режимом функціонування є нормальний режим.

Для забезпечення нормального режиму функціонування системи необхідно виконувати вимоги і дотримуватись умов експлуатації програмного забезпечення і комплексу технічних засобів системи, вказані у відповідних технічних документах (технічна документація, інструкції з експлуатації і т. д.).

Аварійний режим функціонування системи характеризується відмовою одного або декількох компонент програмного і (або) технічного забезпечення. При цьому функції роботи системи продовжують підтримувати роботу системи моніторингу в межах базових налаштувань.

3.1.4 Вимоги по діагностуванню системи

Для діагностування системи моніторингу використовуються інструменти діагностування основних процесів системи, які вмонтовані в операційну систему, а також програм для діагностики роботи комп’ютерних мереж.

Інструменти повинні забезпечувати зручний інтерфейс для можливості перегляду діагностичних подій, моніторингу процесу виконання програм.

3.1.5 Перспективи розвитку, проектування системи

Дана система може бути розширена завдяки використанню протоколу SNMP для збільшення своїх функціональних можливостей.

3.2 Показники призначення

Система повинна передбачати можливість масштабування. Можливості масштабування повинні забезпечуватися засобами використовуваного базового програмного і технічного забезпечення.

3.2.1 Вимоги до надійності

Система повинна забезпечувати працездатність та відновлення своїх функцій при виникненні наступних ситуацій:

– при збоях в системі електропостачання апаратної частини;

– при помилках в роботі апаратних засобів;

– при помилках, пов'язаних з програмним забезпеченням (ОС і драйвери пристроїв).

Для захисту апаратури від стрибків напруги і комутаційних завад повинні застосовуватися мережні фільтри.

3.3 Вимоги до безпеки

Зовнішні елементи технічних засобів системи, що перебувають під напругою, повинні мати захист від випадкового дотику, а самі технічні засоби мати занулення або захисне заземлення .

Система електроживлення повинна забезпечувати захисне вимикання при перевантаженнях і коротких замиканнях в колах навантаження, а також аварійне ручне вимикання.

Загальні вимоги пожежної безпеки повинні відповідати нормам на побутове електрообладнання. У разі пожежі не має виділятися отруйних газів і димів. Після зняття електроживлення має бути доступне застосування будь-яких засобів пожежогасіння.

3.3.1 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Мікроклімат в приміщеннях повинен відповідати нормам виробничого мікроклімату по ДСН 3.3.6.042-99:

– температуру повітря в межах від +10°С до +35°С;

– відносну вологість повітря при 25°С в межах від 30% до 80%;

– атмосферний тиск 760±25 мм рт. ст.

Періодичне технічне обслуговування використовуваних технічних засобів має проводитися відповідно до вимог технічної документації, але не рідше ніж один раз на рік.

Періодичне технічне обслуговування і тестування технічних засобів повинні включати обслуговування і тестування всіх використовуваних засобів, датчики, контроллери, системи передачі даних, пристрої безперебійного живлення.

На підставі результатів тестування технічних засобів повинні проводитися аналіз причин виникнення виявлених дефектів і прийматися заходи по їх ліквідації.

3.4 Вимоги до захисту інформації від несанкціонованого доступу

Система повинна забезпечувати захист від несанкціонованого доступу на рівні не нижче встановленого вимогами, що пред'являються до категорії 1Д по класифікації документа, що діє, “Автоматизовані системи. Захист від

несанкціонованого доступу до інформації. Класифікація автоматизованих систем".

Компоненти підсистеми захисту від НСД повинні забезпечувати:

– ідентифікацію користувача;

– перевірку повноважень користувача при роботі з системою;

– розмежування доступу користувачів.

Рівень захищеності від несанкціонованого доступу засобів обчислювальної техніки, що здійснюють обробку конфіденційної інформації, повинен відповідати вимогам класу захищеності згідно вимогам документу "Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Показники захищеності від несанкціонованого доступу до інформації".

3.4.1 Вимоги по збереженню інформації при аваріях

Інформація, при виникненні аварійних ситуацій повинна бути збережена на резервних носіях.

3.4.2 Вимоги по стандартизації і уніфікації

Система повинна відповідати вимогам ергономіки і зручності користування за умови комплектування високоякісним обладнанням (ЕОМ, монітор і інше обладнання), що має необхідні сертифікати відповідності і безпеки.

3.4.3 Вимоги до функцій (завдань), що виконуються системою:

– забезпечення зручного інтерфейсу;

– забезпечення безпечного зберігання шаблонів;

– пошук необхідної інформації;

– забезпечення високої швидкодії.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

Структурна схема системи моніторингу мережі.

Діаграми процесу управління локальною мережею.

Діаграма варіантів використання.

Результат роботи системи.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка технічного завдання	02.03-25.03.2023
2	Аналіз технічного завдання	26.03-01.04.2023
3	Аналіз вимог до системи моніторингу роботи ПЗ	02.04-16.04.2023
4	Проектування структури системи	17.04-04.05.2023
5	Проектування і реалізація програмної частини	05.05-31.05.2023
7	Налаштування і тестування системи моніторингу ПЗ	01.06-06.06.2023
8	Безпека життєдіяльності, основи охорони праці	07.06-08.06.2023
9	Оформлення кваліфікаційної роботи	05.06-12.06.2023
10	Попередній захист кваліфікаційної роботи	12.06-16.06.2023
11	Захист кваліфікаційної роботи	19.06-24.06.2023

6 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.