ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА КОМП`ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

Магістра
(освітньо-кваліфікаційний рівень)

на тему *Дослідження систем моніторингу мережного трафіку*

Research of network traffic monitoring systems

Виконав: студент *2* курсу, групи *6КСМ*
напряму підготовки (спеціальності)
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки, спеціальності)
Терещенко Ян Іванович
(прізвище та ініціали)
Керівник *Веселовська Г. В.*
(прізвище та ініціали)
Рецензент *Огнєва О. Є*
(прізвище та ініціали)

Хмельницький – 2024 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут, факультет, відділення *Інформаційних технологій та дизайну*

Кафедра, циклова комісія *Комп`ютерних систем та мереж*

Освітньо-кваліфікаційний рівень *Магістр*

Напрям підготовки _____
(шифр і назва)

Спеціальність *123 «Комп'ютерна інженерія»*
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії *Комп`ютерних систем та мереж*
_____ Григорова А. А
«*18*» *жовтня* 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ
Терещенку Яну Івановичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Дослідження систем моніторингу мережного трафіку (Research of network traffic monitoring systems),*

керівник проекту (роботи) *Веселовська Галина Вікторівна, к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «18» *жовтня* 2024 року № 569-с

2. Строк подання студентом проекту (роботи) *8 грудня 2024 р.*

3. Вихідні дані до проекту (роботи) *Методичні рекомендації до виконання, оформлення та захисту кваліфікаційної роботи магістра для студентів всіх форм навчання за спеціальністю 123 «Комп'ютерна інженерія»*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз середовища та основні методи моніторингу. 2. Аналіз систем мережевого моніторингу та обгрунтування вибору для дослідження. 3. Реалізація системи моніторингу на сервері для поточного використання мережі. 4. Особливості системи моніторингу Paessler PRTG. 5. Покращення роботи системи моніторингу Paessler PRTG.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1.Вступ. 2. Актуальність роботи. 3. Мета та завдання. 4. Об'єкт та предмет дослідження. 5. Засоби моніторингу та аналізу мережі. 6. SNMP. 7. RMON. 8. Netflow. 9. Zabbix. 10 Nagios. 11 Cacti. 12 Paessler. 13 Порівняльна характеристика. 14. Оптимальна система. 15-20. Експлуатаційні показники. 21. Наукова новизна і практичне значення. 22. Висновок.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
-	-	-	-

7. Дата видачі завдання *18 жовтня 2024 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	*Аналіз стану питання за тематикою роботи*	*жовтень 2024*	*виконано*
2.	*Аналіз літературних джерел*	*жовтень 2024*	*виконано*
3.	*Аналіз предмету дослідження та предметної області*	*жовтень 2024*	*виконано*
4.	*Оформлення розділу «Аналіз середовища та основні методи моніторингу»*	*жовтень 2024*	*виконано*
5.	*Оформлення розділу «Аналіз систем мережевого моніторингу та обгрунтування вибору для дослідження»*	*жовтень 2024*	*виконано*
6.	*Оформлення розділу «Реалізація системи моніторингу на сервері для поточного використання мережі»*	*листопад 2024*	*виконано*
7.	*Оформлення розділу «Особливості системи моніторингу Paessler PRTG»*	*листопад 2024*	*виконано*
8.	*Оформлення розділу «Покращення роботи системи моніторингу Paessler PRTG»*	*листопад 2024*	*виконано*
9.	*Подання роботи на кафедру для затвердження*	*грудень 2024*	*виконано*
10.	*Захист кваліфікаційної роботи магістра*	*грудень 2024*	*виконано*

Студент _____ *Терешенко Я. І.*
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ *Веселовська Г. В.*
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ARPAnet (англ. Advanced Research Projects Agency Network) – мережа агентства передових досліджень у США.

CLNS (англ. Connection Less Network Protocol) – мережевий протокол передачі даних без встановлення з’єдання.

DDP (англ. Distributed Data Protocol) – клієнт-серверний протокол для запитів та оновлення серверної бази даних, а також синхронізації тих оновлень поміж усіма клієнтами.

DICOM (англ. Digital Images and Communication On Medicine) – стандарт для комунікації і управління медичною візуальною інформацією та суміжних даних.

ERP (англ. Entreprise Resource Planning System) корпоративна інформаційна система, призначена для автоматизації обліку й керування.

HL7 (англ. Health Level 7) – це міжнародний стандарт збереження, передачі медичної інформації та адміністративних даних у програмному забезпеченні.

ICMP (англ. Internet Control Message Protocol) – міжмережевий протокол керуючих повідомлень.

IETF (англ. Internet Engineering Task Force) відкрита міжнародна організація проектувальників, вчених, мережевих операторів та провайдерів.

iLO2 (англ. Integrated Lights-Out) – механізм керування серверами в умовах відсутності фізичного доступу до них.

InfiniBand – високошвидкісна комутована послідовна шина, що застосовується для внутрішніх та міжсистемних з’єднань.

IPFIX (англ. Internet Protocol Flow Information Export) – стандарт

IPMI (англ. Intelligent Platform Management Interface) – інтелектуальний інтерфейс управління платформою, призначений для автономного моніторингу і керування функціями, вбудованих у апаратні платформи.

IPX (англ. Internetwork Packet Exchange) – протокол мережевого рівня моделі OSI, призначений для передачі дейтаграм у системах, неорієнтованих на з'єднання.

iSCSI (англ. Internet Small Computer System Interface) – протокол, розроблений для взаємодії та управління системами зберігання даних, серверів і клієнтів.

JMX (англ. Java management Extensions) технології мови Java, призначені для контролю та керування додатками, приладами та комп'ютерними мережами.

MIB (англ. Management Information Base) – віртуальна база даних, яка використовується для управління об'єктами в мережі зв'язку.

MySQL – вільна реляційна система керування базами даних.

NAS (англ. Network Attached Storage) – сервер для збереження даних на файловому рівні.

NMS (англ. Network Management Systems) – система керування мережею.

NNTP (англ. Network News Transfer Protocol) – протокол поширення, запиту, розміщення і отримання груп новин при взаємодії з сервером або клієнтом.

OID (англ. Object Identifier) – механізм ідентифікації.

OSI (англ. Open Systems Interconnection Basic Reference Model) – абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

PACS (англ. Picture Archiving and Communication System) – технологія, о використовується в медичній візуалізації для зберігання і доступу до зображень.

PDU (англ. Protocol Data Unit) – одиниця інформації яка транспортована через всю комп'ютерну мережу.

QNAP – компанія-виробник мережевих систем зберігання даних NAS.

QoS (англ. Quality of Service) – набір методів для керування ресурсами мережі.

RDMA (англ. Remote Direct Memory Access) – програмне рішення для забезпечення прямого доступу до оперативної пам’яті другого комп’ютера.

RMON (англ. Remote Network MONitoring) – протокол дистанційного моніторингу комп’ютерної мережі.

RTT (англ. Round-Trip Time) – це час, потрібний для пересилання сигналу від передавача до отримувача, а потім у зворотному напрямку.

SAS (англ. Serial Attached SCSI) – комп’ютерний інтерфейс, розроблений для обміну даними з жорсткими дисками та накопичувачами.

SCNM (англ. Self Configuring Network Monitor) – моніторинг мережі з власною конфігурацією для транспортування інформації з комутаторів та маршрутизаторів.

SMTP (англ. Simple Mail Transfer Protocol) – простий протокол передачі, призначений для передачі електронної пошти в мережі.

SNMP (англ. Simple Network Management Protocol) – протокол керування мережами зв’язку на основі архітектури TCP/IP.

SSL (англ. Secure Sockets Layer) – криптографічний протокол, який має хороший рівень безпеки.

TCP/IP (англ. Transmission Control Protocol, англ. Internet Protocol) – набір або стек протоколів мережі Інтернет.

TDP (англ. Thermal Design Power) – величина, яка показує, на відведення якої теплової енергії може бути розрахована система охолодження комп’ютера.

TOE (англ. TCP Offload Engine) – технологія реалізована в деяких мережевих адаптерах для розгрузки центрального процесора і перенесення функцій по обробці мережевих пакетів на мережевий адаптер.

UDP (англ. User Datagram Protocol) – протокол датаграм користувачів, один з протоколів стеку TCP/IP.

ULV (англ. Ultra Low Voltage) – технологія високої енергоефективності.

UNIX – сімейство багатозадачних і багатокористувацьких операційних систем, які розроблені в 1970-х роках.

VoIP (англ. Voice over IP) – технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP.

WMI (англ. Windows Management Instrumentation) – базова технологія для централізованого керування і стеження за роботою інфраструктури на Windows.

WREN (англ. Watching Resources from the Edge of the Network) – перегляд ресурсів на кінцях мережі.

ВСТУП

Актуальність теми дослідження.

Виявлення несправностей передачі даних у сучасних комп’ютерних мережах є однією з найважливіших проблем.

Невелика втрата пакетів під час роботи з мережевими сервісами чи пристроями може призвести до коротких затримок або пошкодження файлів, які можна відновити.

Разом із тим, підприємства або організації можуть зазнати значних і навіть непоправних втрат, якщо дані сервісу або пристроїв повністю відключені від діяльності.

Моніторингові системи використовують для запобігання та прогнозування випадків затримки, простою або повного відключення даних сервісів і пристроїв.

Системи моніторингу постійно спостерігають за процесами, об’єктами та явищами, щоб оцінити їх стан, контролювати їх і прогнозувати майбутнє.

Також вони контролюють обробку великої кількості даних, що полегшує процеси прийняття рішень.

За допомогою моніторингу мереж, як локальних, так і глобальних, можливе виявлення критичного стану пристроїв і попередження про збій чи неполадки в мережі.

В інформаційному контексті, системи моніторингу спостерігають та аналізують інформаційні процеси в глобальних і локальних мережах.

Питання дослідження систем моніторингу мережного трафіку, незважаючи на численні напрацювання в цій предметній галузі, на даний час, продовжують бути надзвичайно актуальними.

Такий стан справ обумовлений тим, що зазначені системи ще недостатньо вивчені та потребують подальшого вдосконалювання, а також відповідного розвитку для цього методологічних, технологічних і практичних підґрунть.

Мета дослідження.

Головними цілями роботи є:

– пошук оптимальних підходів і способів для підтримки вибору найкращої системи моніторингу для відповідних потреб мережі, впровадження систем моніторингу в різних центральних вузлах і зниження витрат на встановлення та налаштування системи;

– дослідження експлуатаційних показників системи моніторингу, що використовує систему серверів, з метою зменшення навантаження на мережу а також покращення якості та швидкості функціонування мережі.

Основні завдання дослідження.

Щоб досягти мети, необхідно виконати наступні завдання:

1) проаналізувати як локальні, так і міжнародні мережі, використовуючи інструменти та підходи до аналізу мереж;

2) порівняти поточні варіанти систем моніторингу;

3) технологічно обґрунтувати оптимальну систему моніторингу для мережевих пристроїв;

4) розробити та налаштувати обрану систему моніторингу на центральному вузлі;

5) тестувати та аналізувати експлуатаційні показники;

6) технологічно забезпечити покращення роботи обраної системи моніторингу.

Наукова новизна.

Створено нові технологічні підходи та способи підтримки оптимального вибору систем моніторингу мережного трафіку.

Практичне значення.

Виконане дослідження надає можливість отримання вдосконаленої (оптимізованої) комплексної системи моніторингу, щоб спростити керування мережею та процесами, діагностику та запобігання критичним станам мережі та покращення інформаційних процесів.

Також створюється можливість покращення якості та швидкості роботи системних і мережевих пристроїв.

Публікації.

Результати роботи було опубліковано в форматі тез у матеріалах наукової конференції.

Структура й об’єм роботи.

До складу роботи входять титульний аркуш, завдання, зміст, перелік скорочень, вступ, п’ять розділів, висновки, перелік джерел посилань і додатки.

Роботу було викладено на 108 сторінках тексту, що містить 38 рисунків, 3 таблиці та 40 джерел посилань.

Основний зміст роботи.

Кваліфікаційна робота призначена дослідженню систем моніторингу та аналізу інформаційних процесів у локальних та глобальних мережах.

У першому розділі було проведено аналіз наукових робіт та літератури, по темі дипломної роботи.

Проаналізовано середовище та основні методи моніторингу мережі.

В ході виконання другого розділу, було проведено аналіз існуючих систем мережевого моніторингу, проведено порівняльну характеристику даних систем.

Технологічно обґрунтовано вибір оптимальної для використання системи моніторингу для подальшого дослідження.

В третьому розділі було технологічно реалізовано систему моніторингу на сервері.

Проведено аналіз системи серверів, на яких проводиться дослідження.

Проаналізовано експлуатаційні показники підприємства при моніторингу серверів.

Під час виконання дослідження особливостей Paessler PRTG, було проведено встановлення системи моніторингу, опис основних елементів даної системи та їх налаштування.

У цілому, основним завданням кваліфікаційної роботи стало дослідження існуючих технологій систем моніторингу, їх порівняння та вибір оптимальної системи під специфічні вимоги мережі, реалізація її на системі серверів, дослідження експлуатаційних показників реалізованої системи моніторингу на основі існуючого навантаження серверів.