МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМ. С.З. ҐЖИЦЬКОГО
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему: **«Інформаційно-аналітична система моніторингу функціонування комп'ютерної мережі закладу освіти»**

Виконав: студент 4 курсу групи Іт-41

Спеціальності 126 «Інформаційні системи та технології»
(шифр і назва)

Балух Віталій Олегович
(Прізвище та ініціали)

Керівник: к.т.н., доцент Падюка Р.І.
(Прізвище та ініціали)

ДУБЛЯНИ-2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА
ІНФОРМАЦІЙНИХ ТЕХНЕОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри_____

д.т.н., проф. А. М. Тригуба
«____» _____2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту

Балуху Віталію Олеговичу

1. Тема роботи: «Інформаційно-аналітична система моніторингу функціонування комп'ютерної мережі закладу освіти»

Керівник роботи Падюка Роман Іванович, доцент
затверджені наказом по університету від 25.02.2025 року № 123/к-с.

2. Строк подання студентом роботи 10.06.2025 р.
3. Вихідні дані до роботи: *вимоги до проектування інформаційних систем; методика проектування інформаційних систем; моніторингу функціонування комп'ютерної мережі закладу освіти.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)
Вступ.
1. Аналіз предметної області.
2.Розробка структурної схеми інформаційної системи моніторингу функціонування корпоративної комп'ютерної мережі
3.Проектування інформаційної системи моніторингу корпоративної комп'ютерної мережі закладу освіти
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки та пропозиції.
Список використаної літератури.
5. Перелік ілюстраційного матеріалу (з точним зазначенням обов'язкових креслень): *Актуальність теми, проблеми моніторингу ККМ Функції системи моніторингу, сучасні методи моніторингу, постановка задачі, структура системи*

управління мережею, вибір програмного забезпечення, опис та аналіз інформаційних потоків корпоративних мереж , алгоритм роботи інформаційної системи моніторингу мережі закладу освіти, проєктування і реалізація.

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3	*Падюка Р.І., доцент кафедри ІТ*		
4	*Городецький І.М., доцент кафедри інженерної механіки*		

7. Дата видачі завдання 26 лютого 2025 р.

Календарний план

№ з/п	Назва етапів дипломного проекту	Терміни виконання етапів роботи	Примітка
1	*Написання першого розділу*	*26.02.25-20.03.25*	
2	*Виконання другого розділу та аркушів ілюстраційного матеріалу до нього*	*21.03-15.04.25*	
3.	*Виконання третього розділу та аркушів ілюстраційного матеріалу до нього*	*16.04-30.04.25*	
4.	*Написання розділу «Охорона праці»*	*01-15.05.25*	
5.	*Завершення оформлення розрахунково-пояснювальної записки та аркушів ілюстраційного матеріалу*	*15-30.05.25*	
6.	*Завершення роботи вцілому*	*01 - 10.06.25*	

Студент _____ Балух В.О.
(підпис)

Керівник роботи _____Падюка Р.І.
(підпис)

УДК 004.9 : 631.1

Інформаційно-аналітична система моніторингу функціонування комп'ютерної мережі закладу освіти. Балух В.О. Кафедра ІТ – Дубляни, Львівський НУВМБ ім. С.З. Гжицького, 2025.

Кваліфікаційна робота: 55 с. текст. част., 13 рис., 2 табл., 13 арк. ілюстраційного матеріалу, 22 джерел.

У кваліфікаційній роботі розглянуто актуальну проблему моніторингу та управління корпоративними комп’ютерними мережами, зокрема в закладах освіти. Проаналізовано сучасні підходи до моніторингу мереж, визначено основні труднощі, вимоги до систем спостереження та оцінено існуючі програмні рішення. Обґрунтовано вибір відкритого програмного забезпечення для реалізації функцій моніторингу, зокрема системи Nagios Core, яка була налаштована для відстеження стану мережі та виявлення критичних подій. Розроблено структурну схему інформаційної системи, описано її архітектуру, алгоритм функціонування та порядок налаштування ключових компонентів. У роботі також приділено увагу питанням охорони праці, безпеки в надзвичайних ситуаціях та технічним аспектам безпечної експлуатації обладнання.

Запропоноване рішення дозволяє підвищити ефективність контролю мережевої інфраструктури навчального закладу, забезпечити стабільність роботи та своєчасне реагування на збої.

Ключові слова: моніторинг комп’ютерної мережі, програмне забезпечення, сервер

Key words: computer network monitoring, software, server.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SNMP – Simple Network Management Protocol

NM – network monitoring

NMS – Network Management System

TCP/IP – Transmission Control Protocol/Internet Protocol

MIB – Management Information Base

UDP – User Datagram Protocol

ISO – International Organization for Standardization NdoUtils –

Nagios Data Output Utilities

UPnP – Universal Plug & Play

RT – Request Tracker

NB-ITMS – Nagios Based - IT Management System

OS – operating system

SCNM – Self-Configuring Network Monitor

RMON – Remote Monitoring

LAN – Local area network WAN – Wide Area Network

ПЗ – програмне забезпечення

БД – база даних

ВСТУП

Інформаційна структура великої корпоративної комп’ютерної мережі є поєднанням численних мереж і систем різного масштабу. З часом кількість мережевого обладнання зростає, що ускладнює процес спостереження та забезпечення стабільної роботи всієї мережі. Необхідно не лише відстежувати поточний стан обладнання, а й оперативно реагувати у разі виходу з ладу або відмови окремих вузлів. Із збільшенням кількості клієнтів і навантаження на мережу зростає потреба в постійному контролі її стану.

У більшості сучасних середовищ перевірка справності здійснюється вручну. Всі ці дії мають виконуватися в межах загального сценарію управління продуктивністю серверів і мережі загалом за допомогою стандартних засобів моніторингу. Більшість проблем виявляються вже після того, як вони починають впливати на кінцевих користувачів. Це, своєю чергою, призводить до перевантаження технічного персоналу та системних адміністраторів, а також до поступового зниження якості послуг.

Отже, мережевий моніторинг є важливим інструментом для контролю стану мережі, забезпечення її працездатності та своєчасного реагування на збої, зловмисні дії чи інші критичні події. Його основна мета — ефективне управління мережею та оперативне виявлення й усунення проблем у її функціонуванні.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Проблеми моніторингу корпоративних комп'ютерних мереж

Несанкціонований доступ до мережі в даний час є однією з головних загроз мережевим операційним системам, де зберігаються та передаються секретні та конфіденційні дані. Інформація може бути розголошена, втрачена або змінена, якщо її не виявити та не вжити належних заходів у належний час. Для безпечної та ефективної роботи мережі та систем необхідна корпоративна платформа моніторингу мереж з інтегрованими інструментальними функціями.

Важливо відзначити, що карантин, який був запроваджений через пандемію коронавірусу COVID-19 та триваюча війна приділяє особливу увагу віддаленій роботі, яка необхідна для збереження активності значної частини співробітників, щоб вони залишалися здоровими та продовжували працювати безперебійно в безпечних умовах. Адже як вітчизняні, так і зарубіжні дослідники відзначають, що більшість опитаних працівників і деякі роботодавці все ж готові працювати дистанційно або в змішаному режимі на постійній основі або в окремих випадках. Однак перехід на віддалену роботу підвищує технологічні ризики несанкціонованого доступу до серверів, доступності системи, витоку конфіденційної інформації та втрати даних.

Моніторинг і керування мережами завжди виявляється складним завданням для великих організацій зі складною мережевою топологією. Для мережевих інженерів і мережевих адміністраторів справді дуже трудомістко перевіряти вручну робочий стан сотень або, можливо, тисяч пристроїв у топології мережі. Фактично, збій мережі лише на кілька годин може призвести до втрати великої кількості грошей з боку організації, разом із втратою задоволеності клієнтів. У багатьох організаціях досі існує система скарг, коли співробітник, клієнт реєструє скаргу на підключення до мережі до того, як мережеві адміністратори починають вирішувати проблеми. Завдяки автоматизованій

інформаційній системі моніторингу та управління мережею повідомлення, виявлення та усунення несправностей мережі можуть бути значно швидшими.

1.2 Аналіз функцій системи моніторингу функціонування корпоративних комп’ютерних мереж

Для ефективності діагностики адміністратор повинен вивчити особливості мережі на етапі її проектування та розробки, ознайомитися зі схемою мережі, детальним описом програмного та апаратного забезпечення з повним визначенням усіх параметрів та інтерфейсів. Існують спеціальні програмно-технічні комплекси мережевої документації, які можна використовувати для проектування та зберігання інформації. Ті, яких знає системний адміністратор, допоможуть заздалегідь дізнатися про всі можливі приховані проблеми та деталі системи, щоб у аварійній ситуації можна було визначити, що пішло не так — пов’язано це з обладнанням, програмним забезпеченням, пошкодженням програми чи помилкою користувача.

Діагностика корпоративної мережі – це процес (безперервний) аналізу стану інформаційної мережі. У разі несправності мережевих пристроїв фіксується факт несправності, визначається її місце та тип, і ця інформація заноситься до лог-файлів. Передається повідомлення про несправність, пристрій або вузол відключається і замінюється на резервний або налагоджується. Для підтримки її в працездатному стані необхідний постійний моніторинг роботи локальної мережі, яка становить основу будь-якої корпоративної комп’ютерної мережі [1].

Основними функціями моніторингу комп’ютерної мережі є спостереження та збір даних про стан системи, аналіз отриманої інформації, визначення рівня критичності стану, ймовірних причин збою та прийняття рішення щодо подолання критичного стану комп’ютерної мережі.

Питання моніторингу корпоративних комп'ютерних мереж можна визначити як збір, обробку та аналіз даних, спрямований на підвищення

продуктивності системи, і може бути вирішено за допомогою різноманітних програм моніторингу мережі.

Тому основним завданням моніторингу комп’ютерних мереж є забезпечення надійного функціонування шляхом своєчасного виявлення погіршень роботи, аналізу цих факторів та звітності для прийняття правильних управлінських рішень.

Функціями моніторингу мережі повинні бути:

– перевірка стану усього мережевого обладнання, наприклад маршрутизаторів, комутаторів, комп’ютерів користувачів;

– запис та аналіз повідомлень автоматизованих систем контролю та користувачів про помилки обладнання та працездатність усіх пристроїв.

1.3 Аналіз сучасних методів вирішення проблеми моніторингу функціонування корпоративної комп’ютерної мережі

Як вітчизняними, так і зарубіжними вченими було виконано багато роботи з проблем моніторингу комп'ютерних мереж, і їх висновки можна прочитати на сторінках багатьох джерел [3, 4, 6, 10].

Наприклад, в роботі [3] розглядаються проблеми моніторингу комп'ютерної мережі при перевантаженнях і збоях. У цьому дослідженні на перший план були висунуті типові причини та наслідки перевантаження комп’ютерної мережі. Вважається, що ефективність комп’ютерної мережі функціонує в умовах перевантажень і збоїв, оскільки це є причиною надмірної буферизації системи. Автор наведеного нище уривку з тексту далі пояснює, що «найкращий спосіб пом’якшити підвищений вплив перевантажень на мережу — це зарезервувати пропускну здатність каналу та компенсувати її частку в найбільш постраждалих каналах». Автор, однак, не займався аналізом динамічних властивостей комп'ютерної мережі.

Автори [4] описують ефективну автоматичну систему моніторингу в режимі реального часу, яка контролює всю мережу, комутатори, а потім

повідомляє адміністратору за допомогою електронних листів або SMS, коли будь-який мережевий комутатор чи інше обладнання не працює. Він також повідомляє про розташування проблеми в топології мережі та її вплив на решту мережі. Система моніторингу мережі описувала інтелектуальну взаємодію між Request Tracker (RT) і Nagios, програмним забезпеченням у середовищі ОС Linux. Топологія мережі побудована в Nagios, яка постійно стежить за всіма вузлами мережі на основі визначених для них послуг. Щойно будь-який мережевий вузол вийде з ладу, Nagios створить повідомлення та надішле його програмному забезпеченню RT. Це повідомлення призведе до отримання квитка в базі даних RT з інформацією про проблемні вузли та те, як це впливає на решту мережі. Програмне забезпечення RT налаштовано на інформування мережевого адміністратора електронною поштою та SMS-повідомленням одразу після створення. Ця система моніторингу мережі є повністю автоматичною, і адміністратору достатньо перевірити свою електронну пошту та повідомлення. Представлена система моніторингу мережі є інтелектуальною, щоб дуже швидко визначити місце проблеми в мережі, а також її вплив на решту мережі, що є високоефективним і забезпечує повний контроль над мережею.

У документі [4] представлено ідею та налаштування системи, призначеної для спостереження та догляду за комп’ютерною мережею для великої компанії з поєднанням спільного та розподіленого налаштування. Налаштування використовує програмне забезпечення Nagios, програмне забезпечення Multi Router Traffic Grapher, NdoUtils, систему керування реляційною базою даних MySQL, системи візуалізації Nagios (NagVis, NagMap) і унікальну програму, створену для системи, яка допомагає показувати переглянуті ресурси.

У ще одній статті [6] розповідається про методи моніторингу на основі маршрутизатора, а не на основі маршрутизатора. У ньому наведено короткий опис трьох найпоширеніших інструментів моніторингу мережі — SNMP, RMON і Cisco Netflow, а також інформацію про два нових методи моніторингу, які працюють як з пасивним, так і з активним методами моніторингу та намагаються використовувати найкращі функції обох (WREN і SCNM).

Концепція системи моніторингу, описана авторами, допомагає налаштувати користувальницьку програму, ефективну для моніторингу мереж LAN і WAN, використовуючи набори інструментів на основі програмного забезпечення з відкритим кодом. Запропоновані рішення дозволяють масштабувати таку систему для впровадження на малих, середніх і великих підприємствах. Система не вимагає високих вимог до обладнання. Це робить низькими витрати як на їх створення, так і на впровадження на підприємстві, а потім на технічне обслуговування. Рішення, описані авторами, були встановлені, налаштовані та протестовані в лабораторії.

Сьогодні великі корпоративні та інституційні комп'ютерні мережі, як правило, неоднорідні. Вони поєднують різноманітні технології з інструментами від різних виробників, які працюють на різних ОС. Крім того, мережеве спостереження та обробка не залишаються на одному місці, а часто потребують доступу до віддалених сайтів. У таких ситуаціях один спеціальний інструмент не виконує своїх обов'язків або доводиться використовувати кілька різних інструментів разом, що значно ускладнює та дорожчає керування мережею (купівля кількох інструментів, навчання працівників, як ними користуватися).

Очевидно, що точний і ефективний моніторинг мережі підтримуватиме надійну роботу мережі з підтримкою дисципліни для виправлення будь-яких відхилень. З іншого боку, те, що робиться в наш час, дуже залежить від ручного керування мережевим моніторингом, тому підприємства витрачають значну частину свого бюджету на персонал, який здійснює моніторинг своїх мереж.

Вибираючи більш специфічний інструмент моніторингу [6], адміністратор повинен спочатку визначитися з тим, чи хоче він використовувати більш перевірену систему чи нову систему. Якщо перевірена система є напрямом, який здається кращим, NetFlow є найкориснішим інструментом, оскільки його можна використовувати з пакетом аналізу даних для представлення даних у зручному середовищі; однак, якщо адміністратор хоче випробувати новішу систему, тоді найкраще підійде комбінований підхід моніторингу, наприклад WREN або SCNM.

SNMP, RMON і Cisco NetFlow – це деякі з методів, які використовуються маршрутизатором і які коротко обговорюються. Методи на основі маршрутизатора, які будуть обговорюватися, це активні, пасивні та комбіновані засоби моніторингу. За останні роки спостерігався величезний розвиток бездротових технологій, що дозволило розробити нові бездротові системи [7]. Сучасна бездротова мережа розміщує передачу в основі, і було розроблено численні методи моніторингу мережевого потоку трафіку. Фраза «моніторинг трафіку» описує метод, за допомогою якого ідентифікуються всі дані, надіслані та отримані мережею, виявляються збої та небезпечні події, і якісні пакети даних можуть проходити через мережу. Із зростанням рівня мережевої інтеграції та загрозою мережевих атак, що розвиваються проти мережі, моніторинг мережевого трафіку став необхідним засобом кібербезпеки для виявлення мережевих атак. Методи моніторингу на основі маршрутизаторів нещодавно викликали великий інтерес завдяки простоті застосування, можливості експериментів і ефективності моніторингу бездротових мереж. Основною метою даної наукової роботи є розробка системи моніторингу мережевого трафіку. Ця запропонована система працює з підвищенням продуктивності вдвічі порівняно з існуючими системами.

Точний моніторинг мережевого трафіку є величезним завданням через величезний розмах Інтернету. Передбачення дивної відповіді сервера є дуже важким завданням. Аналіз продуктивності мережі може бути досягнутий за допомогою моніторингу трафіку. Відстежуючи трафік, користувач може дізнатися про стан цієї мережі. Крім того, він надає повну інформацію про дані та ресурси, пов’язані з цією мережею.

Неавтентифіковані служби або сервер будуть відомі шляхом моніторингу трафіку до сервера. Правила мережі та статистика трафіку будуть відомі з легкістю, що також допоможе у вирішенні проблем мережі. Події безпеки, а також відповідальний вхід користувачів також будуть досліджені. У мережі не повинно бути маршруту від вузла джерела до вузла призначення. Вихідний вузол буде транслювати запит маршруту для пакетів даних усім вузлам, коли він зможе

надіслати пакети. У нинішньому конкурентному контексті немає управлінського рішення, яке можна застосувати до всіх сценаріїв. Доступні відкриті та безкоштовні рішення не охоплюють усі різні аспекти управління, навіть ті, які необхідні для якісної операційної роботи.

Нарешті, пропрієтарні рішення, коли вони використовуються - дуже часто дорогі з обмеженим оглядом мережевої карти. І ці обмежені патентовані рішення зазвичай потребують спеціального та дорогого навчання. Для аналізу централізованого підходу, який усуне використання кількох інструментів управління в одній кімнаті, автори Matei розробили нову платформу, відому як NB-ITMS (Nagios Based - IT Management System). Nagios — це програмне забезпечення для моніторингу з відкритим вихідним кодом, яке легко налаштувати та, крім того, є безкоштовним. NB-ITMS має ще два дуже важливі та критичні вдосконалення порівняно з Nagios: керування конфігурацією та вдосконалений графічний інтерфейс для роботи та обслуговування. Через дефекти складних програмних засобів із відкритим вихідним кодом, які існують у середовищі сучасних великих мереж, системні оператори, або в даному випадку мережеві адміністратори, змушені інтегрувати кілька програмних засобів, щоб мати можливість налаштувати середовище моніторингу з інструментами, відповідними для конкретної ситуації. Nagios, інструмент із відкритим кодом і багатьма функціями, є одним із інструментів, який найчастіше використовують досвідчені адміністратори. Завдяки своїй гнучкій модульній архітектурі Nagios дозволяє користувачам розвивати свої модулі далі, щоб систему можна було розширити різними способами. У цій статті представлено концептуальний дизайн для інтеграції Nagios як серця нової багатофункціональної системи моніторингу [9].

Натомість у статті [10] описано автоматизовану систему моніторингу та керування мережею, у якій завдання мережевого адміністратора відносно спрощено, щоб підтримувати доступність серверів і пристроїв 24/7. Він має дозволити системі надсилати електронний лист адміністратору мережі одразу після виявлення будь-якої проблеми з мережею. Запропонована система є

портативною, має динамічну мережеву масштабованість і не викликає проблем із сумісністю та інтеграцією для моря різнорідних пристроїв від різних постачальників. Усі функції моніторингу є безперервними та автоматичними та не вимагають жодних спеціальних вводів чи уваги з боку адміністратора. Крім того, запропонована система забезпечує гнучкість для мережевого адміністратора: якщо адміністратор зайнятий і не виправляє мережевий збій або будь-яку проблему протягом заздалегідь визначеного періоду, тоді система надішле новий електронний лист наступній відповідальній особі в списку пріоритетів тощо. Суттєві особливості та їх експериментальна перевірка вказують на видатність запропонованої системи моніторингу та управління мережею. У [10] розроблено та впроваджено цікаву систему моніторингу та звітності для великих організацій. Він заснований на програмуванні інструментів з відкритим вихідним кодом (наприклад, Nagios і RT) і їх всебічної інтеграції для моніторингу мережевих пристроїв, таких як комутатори та маршрутизатори. Набір програм, які використовують технологію Universal Plug & Play (UPnP), був розроблений для моніторингу пристроїв кінцевих користувачів у мережі. Автори [10] описують систему, яка однаково може бути застосована до різних типів підприємств та організацій. Тому відомі системи моніторингу для великих організацій будуть доступні, але вони незручні в середньому навчальному закладі з відносно невеликою кількістю користувачів більшість функцій такого програмного забезпечення, які будуть доступні, залишаться невикористаними, але досвід їх застосування можна успішно використовувати в ході розробки власного програмного продукту.

1.4. Постановка задачі кваліфікаційної роботи

Щоб визначити оптимальний робочий стан комп’ютерної мережі, адміністратори мережі використовують програмне забезпечення для моніторингу мережі, яке може заздалегідь виявляти дефекти мережі, покращувати та контролювати продуктивність мережі та визначати критичні

стани.

Очевидно, що метою моніторингу мережі є здійснення управління мережею, своєчасне виявлення, аналіз та усунення проблем комп'ютерної мережі.

Метою даної кваліфікаційної роботи є розробка інформаційної системи моніторингу комп’ютерних мереж закладу освіти, яка повинна мати підвищену безпеку, особливо здатність запобігати несанкціонованому доступу, атакам, критичним станам і аномаліям, а також бути здатною своєчасно попереджати про можливі збої в роботі.

Для досягнення цілей, поставлених у цій роботі, необхідно виконати наступні завдання:

- ✓ Визначити функції моніторингу роботи комп'ютерної мережі підприємства та проаналізувати його завдання;
- ✓ Розробити архітектуру системи моніторингу комп'ютерної мережі підприємства;
- ✓ На основі аналізу вибрати платформу для розробки інформаційних систем і програмного забезпечення;
- ✓ Розробити алгоритм роботи моніторингу інформаційних систем комп'ютерної мережі підприємства.

На основі наведеного вище аналізу мереж і систем моніторингу, проведене формулювання вимог до систем моніторингу допоможе вибрати програмне забезпечення, яке максимально відповідає функціональним вимогам сучасних навчальних закладів. Проте слід зазначити, що обраний продукт не може повною мірою реалізувати всі поставлені завдання, оскільки потребує розробки додаткових додатків та модулів.

РОЗДІЛ 2

РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Структура системи моніторингу функціонування корпоративної комп'ютерної мережі

Структура системи визначає її компонентний склад, взаємозв'язки між елементами, а також технологію функціонування. Архітектура мережі задає концепцію її побудови, що включає:

– основні компоненти мережі;

– топологію мережі та ролі кожного її елемента;

– спосіб налаштування та з'єднання елементів для забезпечення їхньої взаємодії [11].

Розуміння структури системи моніторингу мережі забезпечує прозорість її функціонування за будь-якої конфігурації та у будь-яких умовах. Існує кілька підходів до мережевого моніторингу, як із використанням маршрутизаторів, так і без них. До методів, заснованих на маршрутизаторах, належать SNMP, RMON і Cisco NetFlow. Також застосовуються інструменти активного, пасивного й комбінованого моніторингу. На додачу до базових утиліт на зразок ping та ipconfig, які дозволяють перевірити якість і надійність мережевих з'єднань, сучасні програмні рішення для моніторингу — такі як Zabbix, Nagios та інші — підтримують роботу з обладнанням у комп'ютерних мережах, що базуються на архітектурі TCP/IP.

У мережах типу Ethernet ключовими вузлами для підключення комп'ютерів та інших мережевих пристроїв є концентратори та комутатори. Пристрої, підключені до одного такого вузла, утворюють сегмент мережі, в межах якого комп'ютери можуть безпосередньо обмінюватися даними.

Структура системи керування мережею включає кілька рівнів і складається з таких основних компонентів:

– Система керування мережею (NMS) — програмне забезпечення, яке виконує функції моніторингу та керування мережевими пристроями;

– Протокол керування мережею — забезпечує обмін інформацією між NMS та керованими пристроями;

– Керовані пристрої, наприклад маршрутизатори, які підлягають адмініструванню через систему керування;

– Агенти керування — програмні модулі, встановлені у мережевому обладнанні, що збирають і зберігають дані про його стан.

Розуміння складу цих компонентів дає змогу описати повний процес управління мережею — від збору інформації до аналізу та прийняття рішень щодо функціонування мережевої інфраструктури.

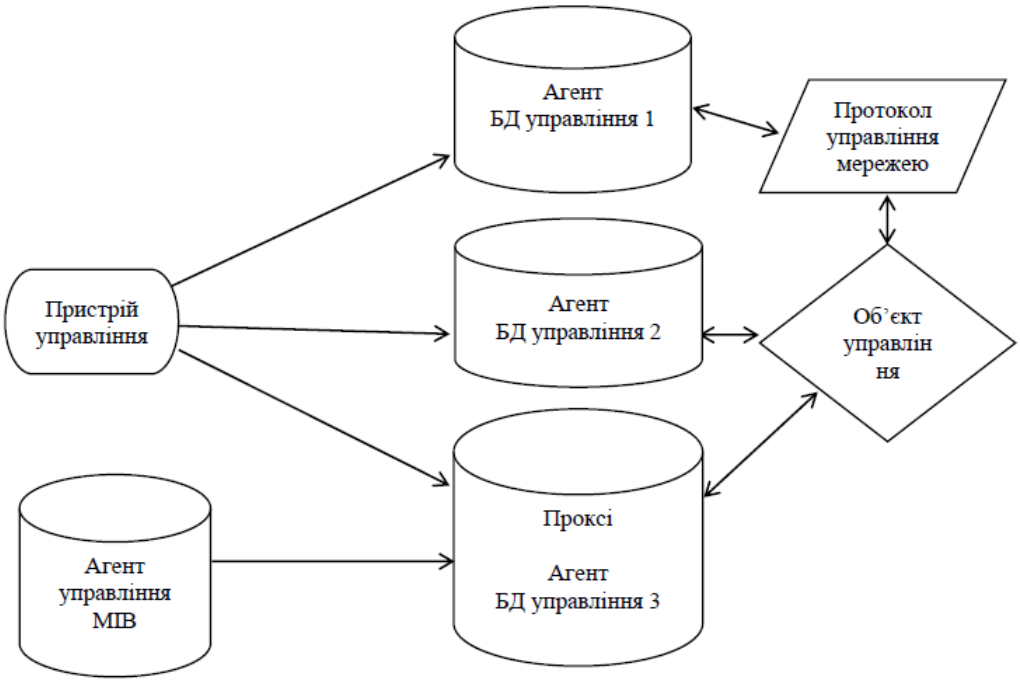


Рисунок 2.1 – Структура системи управління мережею

Під час моніторингу стану мережі може використовуватися широкий спектр програмного забезпечення для керування, вибір яких залежить від

мережевої платформи, апаратного забезпечення та операційної системи. Інформація про стан мережі зберігається безпосередньо на мережевих пристроях, а агенти керування, що функціонують на цих пристроях, здійснюють її збір та збереження у базах даних (MIB).

MIB (Management Information Base) — це структура даних, яка містить детальну інформацію про мережеві пристрої. Доступ до цієї інформації забезпечується через протокол керування мережею SNMP. Програма керування мережею використовує SNMP як механізм взаємодії між менеджером і агентами. Агент виконує функції управління, хоча безпосередньо не взаємодіє з іншими мережевими елементами.

Зібрані дані зазвичай обробляються та візуалізуються через графічний інтерфейс користувача, який надає засоби для керування пристроями, а також для налаштування програм моніторингу. Ініціатором звітності виступає агент: він повідомляє менеджера про аномальні події, які фіксує на стороні пристрою.

Застосунок керування мережею, або менеджер, виконує функції централізованого моніторингу, автоматично отримуючи дані від SNMP-агентів на керованих пристроях. Це дозволяє системі керування відображати поточну інформацію за допомогою графічного інтерфейсу. Менеджер також відповідає за збір і збереження даних про стан пристроїв та параметри їх роботи.

Основним недоліком періодичного опитування SNMP є потенційна затримка між моментом виникнення події та її реєстрацією в системі моніторингу. Це пов’язано з частотою опитування та навантаженням на пропускну здатність мережі.

SNMP (Simple Network Management Protocol) — простий протокол керування мережею. Керованим пристроєм може бути, наприклад, маршрутизатор, а програмою менеджера — відповідне застосування для адміністрування.

Агенти SNMP є складовою частиною пристроїв, які управляються через базу даних MIB. Вони виконують функції збору інформації та локального збереження даних. У мережах моніторингу також застосовуються протокол SNMP

та протокол користувацьких датаграм (UDP).

Протокол SNMP є стандартом мережевого керування, який зазвичай використовується як основа архітектури систем керування. Він дозволяє програмам-менеджерам і агентам обмінюватися інформацією про стан мережі. Створений у 1988 році, SNMP був розроблений для керування пристроями, що працюють з IP-протоколом. Це простий набір операцій і структур даних, який дає змогу змінювати стан певних пристроїв. Попри асоціацію з маршрутизаторами, SNMP також працює з концентраторами, мостами, принтерами, серверами, робочими станціями тощо.

Цей протокол дає змогу відстежувати такі параметри, як обсяг трафіку, завантаження вхідних та вихідних інтерфейсів, а також температуру пристроїв. Він використовує UDP як транспортний протокол для обміну даними між менеджером і агентом, не встановлюючи постійного з’єднання. SNMP працює через певний порт і не динамічно виділяє порти на стороні агента для обробки запитів від системи моніторингу.

Еталонна модель взаємозв’язку відкритих систем (OSI) була розроблена Міжнародною організацією зі стандартизації (ISO). Згідно зі стандартом ISO 10303 "Системи промислової автоматизації та інтеграція — Представлення та обмін даними про продукт", модель керування мережею включає п’ять концептуальних функціональних областей:

Управління продуктивністю — забезпечує контроль над параметрами мережі, такими як пропускна здатність, час відгуку, рівень використання каналів тощо, для підтримки її ефективності.

Управління конфігурацією — фіксує зміни в апаратному й програмному забезпеченні, здійснює облік і контроль впливу змін на загальний стан мережі.

Управління обліком ресурсів — оптимізує розподіл ресурсів, знижує кількість збоїв і забезпечує рівномірний доступ до мережі для всіх користувачів.

Управління несправностями — відповідає за виявлення, усунення та повідомлення про збої в роботі мережевих пристроїв або систем.

Управління безпекою — здійснює контроль доступу до мережевих ресурсів на основі заданих політик, забезпечуючи захист від несанкціонованого втручання.

Таким чином, управління мережею або мережевий моніторинг (Network Management, NM) охоплює функції планування, організації, координації та контролю ресурсів мережі. До його обов'язків входить моніторинг продуктивності, виявлення і ліквідація несправностей, конфігурування елементів мережі, ведення облікових даних та забезпечення безпеки інформаційних потоків.

2.2. Вибір програмного забезпечення для моніторингу корпоративної комп'ютерної мережі

Програмне забезпечення з відкритим кодом, призначене для моніторингу корпоративних комп'ютерних мереж, має низку переваг над комерційними аналогами із закритим кодом. Насамперед, воно є загальнодоступним для широкого кола користувачів і здебільшого не потребує додаткових фінансових витрат. Такий підхід дозволяє організаціям оптимізувати витрати, зберігаючи при цьому високий рівень функціональності та гнучкості.

Сучасне програмне забезпечення для моніторингу забезпечує контроль за всіма пристроями, серверами, трафіком та використанням пропускної здатності мережі. У конфігураціях корпоративних мереж, де окремі вузли можуть працювати за схемою клієнт-сервер, а іноді — виконувати обидві ролі одночасно [15], постає потреба у програмному забезпеченні, яке здатне забезпечити високу продуктивність, стабільність та відповідність вимогам якості.

Програмне забезпечення з відкритим кодом відповідає ряду вимог, визначених міжнародними стандартами, зокрема:

– забезпечення збереження інформації та надійної передачі даних;

– висока ймовірність безвідмовної роботи протягом усього терміну служби;

– можливість моніторингу окремих вузлів та програмного забезпечення

користувача, що демонструє ознаки низької продуктивності (за параметрами часу відгуку, пропускної здатності, затримок);

– підтримка механізмів запобігання несанкціонованому доступу, хакерським атакам, спробам шахрайства;

– сумісність з різними операційними системами вузлів (локальних комп'ютерів, серверів тощо);

– масштабованість — здатність підтримувати ефективну роботу зі зростанням кількості вузлів у мережі;

– зручність у використанні та простота обслуговування.

Варто зауважити, що не кожне програмне забезпечення, навіть сучасне й популярне, може відповідати всім зазначеним вимогам. Тому вибір конкретного інструмента моніторингу потребує ретельного аналізу ряду альтернатив, оцінки їх ключових функцій та виключення надлишкових можливостей, що не використовуватимуться в обраному середовищі.

Фактично, вибір програмного забезпечення для моніторингу корпоративної інформаційної системи — це складна задача оптимізації. Вона не має однозначного рішення, а передбачає пошук найкращого варіанту, який би максимально відповідав сукупності визначених критеріїв. Процес вибору передбачає декілька етапів аналізу й оцінювання, кожен з яких супроводжується звуженням множини альтернативних рішень. На виході формується один оптимальний варіант — програмне забезпечення, що найповніше відповідає технічним і функціональним вимогам.

Таким чином, процес вибору програмного забезпечення для моніторингу корпоративної мережі можна представити як послідовність етапів прийняття рішення, де на кожному етапі розглядається підмножина варіантів, що відповідає заданим умовам. Вибраний варіант є найкращим з точки зору інтегрального показника якості. Це і є суть багатоетапного вибору з використанням відповідної методології проектування систем підтримки прийняття рішень [16], як проілюстровано на рисунку 2.2.

Групу сучасного програмного забезпечення, яке може бути використане

для вирішення завдання моніторингу мереж, з урахуванням напрацьованої практики та потенціалу заміщення, наведено в таблиці 2.1.

На кожному етапі моделі вибору, представленої на рисунку 2.2, реалізується пошук оптимального варіанту. Результати, отримані на кожному з попередніх кроків, слугують вхідними даними для наступних. Варіанти, відсіяні на одному з етапів, у подальшому не розглядаються. Такий підхід забезпечує логічну послідовність дій і дає змогу прийняти обґрунтоване рішення щодо вибору програмного забезпечення для моніторингу корпоративної комп'ютерної мережі.

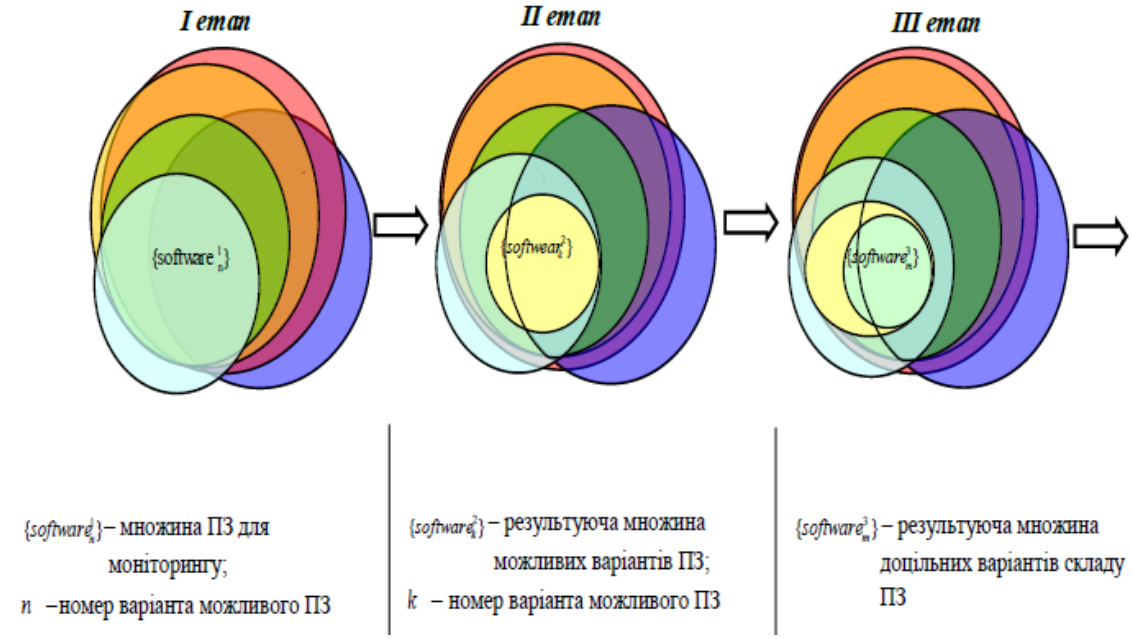


Рисунок 2.2 – Малюнок, що пояснює вибір програмного забезпечення для спостереження за комп'ютерними мережами на основі відомого способу вибору частин системи ГВП [16].

У контексті розгляду задач моніторингу корпоративних комп'ютерних мереж доцільно розглянути приклади програмних рішень з відкритим кодом, які довели свою ефективність у різних масштабах використання — від невеликих локальних мереж до складних розподілених інфраструктур.

Zabbix — одна з найпопулярніших систем моніторингу з відкритим кодом. Вона підтримує активний та пасивний моніторинг серверів, мережевого

обладнання, віртуальних машин, баз даних тощо. Zabbix дозволяє збирати різноманітні метрики за допомогою SNMP, IPMI, агентів, скриптів, API, а також забезпечує високий рівень візуалізації у вигляді графіків, карт, дашбордів. Перевагами є масштабованість, розгалужена система сповіщень, інтеграція з популярними платформами, підтримка тригерів та сценаріїв. Основним недоліком є відносна складність первинного налаштування.

Nagios Core — перевірене часом рішення, орієнтоване на моніторинг серверів і мереж. Його основною перевагою є модульність: тисячі плагінів дозволяють адаптувати систему під конкретні потреби. Nagios активно використовується у корпоративному середовищі завдяки надійності, але його інтерфейс вважається дещо застарілим, а налаштування складнішими в порівнянні з новішими системами. Для покращення взаємодії часто використовуються надбудови, як-от Nagios XI, які додають більш зручний веб-інтерфейс та аналітику.

Prometheus — система моніторингу з фокусом на збирання метрик, орієнтована на хмарні середовища та контейнеризовані додатки. Вона інтегрується з Grafana для побудови потужних графіків, а також добре поєднується з Kubernetes. Prometheus не використовує SNMP у класичному розумінні, однак завдяки експортерам може підключатися до великої кількості сторонніх джерел. Його перевагами є висока гнучкість, підтримка проміжного кешування та потужна мова запитів PromQL. Недоліком можна вважати обмежену підтримку активного моніторингу й складність налаштування для початківців.

Icinga 2 — це форк Nagios, який значно перевершив свого попередника за функціональністю та зручністю. Icinga має сучасний інтерфейс, REST API, підтримує розподілений моніторинг та автоматизацію розгортання конфігурацій. Серед переваг — гнучка система сповіщень, сумісність з плагінами Nagios та можливість глибокої інтеграції з DevOps-інструментами. Недоліком є те, що для повноцінної роботи може бути потрібне розгортання супутніх сервісів (наприклад, бази даних, веб-сервера тощо).

OpenNMS — потужна корпоративна платформа для моніторингу мереж, яка надає можливості як активного, так і пасивного моніторингу, автоматичне виявлення вузлів, підтримку SNMP, візуалізацію даних, а також аналітичні функції. Її використовують у великих мережах завдяки високій масштабованості та підтримці складних політик моніторингу. Основним недоліком є складність інсталяції та потреба в значних ресурсах при великій кількості об'єктів моніторингу.

Observium — ще одне поширене рішення для моніторингу мереж, особливо пристроїв, які підтримують SNMP. Воно надає приємний веб-інтерфейс, детальну інформацію про інтерфейси, графіки використання, підтримує автодетекцію пристроїв. Основною перевагою є простота встановлення й зручна робота з мережевим обладнанням. Недоліком є дещо обмежена масштабованість у порівнянні з Zabbix чи Prometheus.

У таблиці 2.1 наведено порівняльну характеристику вищезазначених систем з акцентом на функціональні можливості, вимоги до ресурсів, складність налаштування та масштабованість.

Таблиця 2.1 – Аналіз програмних рішень які можуть використовуватись для моніторингу комп'ютерних мереж та їх порівняльні характеристики

Назва	Параметри та характеристики, переваги та недоліки	Призначення	Архітектура
1	2	3	4
Nagios Core	Має широкий спектр додаткових плагінів що дозволяє, – зберегти всі налаштування у конфігураційному файлі; – налаштувати архітектуру програмного забезпечення на основі роботи з плагінами; Переваги: – забезпечує високий рівень продуктивності, оскільки використовує низькі ресурси сервера; – працює практично з будь-яким іншим програмним забезпеченням сторонніх виробників за допомогою плагінів; – має велику кількість користувачів, – легко налаштувати Недоліки: – масштабування без додаткових плагінів стає дуже важким; – не має вбудованих засобів візуалізації; – кожен потік запускається як окремий процес.	Відслідковує стан серверів мережі, мережевого обладнання та проміжного програмного забезпечення, використовується як для окремого ПК, так і для локальної мережі.	Архітектура клієнт-сервер.

Продовження таблиці 2.1

OpenNMS	Здатний контролювати роботу мережевих топологій на різних рівнях моделі OSI, що дозволяє оптимізувати IT-інфраструктуру, підходить для рішень промислового масштабу. Недоліки: – Важко контролювати невеликі мережі – Складний веб-інтерфейс Переваги: – Написано мовою Java – Гнучкість – Масштабованість	Здійснює моніторинг мереж корпоративного рівня.	Побудована з використанням подійно-орієнтованої архітектури.
Zabbix	Моніторинг Java-серверів можливий за допомогою розширення функціональності за допомогою підтримуваних користувальницьких сценаріїв. Плюси: – -зберігання різноманітних типів файлів; ○ відмінна візуалізація. – Мінуси: – -недоступні плагіни; – -історія та конфігурація, що зберігаються в базі даних, обмежують масштабованість через неефективність.	Здійснює моніторинг великої кількості параметрів мереж та серверів.	Архітектура клієнт-сервер.

Cacti	Використовуючи протокол SNMP здійснює опитування мережевого комутатора або інтерфейсу маршрутизатора. Використовує утиліту RRDtool як зовнішню програму. Використовується в якості графічного інструменту моніторингу мережі. Переваги: - Зручний із сучасним виглядом - Чудова інформативна графіка - Використовує скрипти Недоліки: - Важко налаштувати - Лише візуалізація параметрів та показників мереж	Використовується, як інструмент для відстеження мережевого трафіку.	Архітектура сервер-клієнт.
Zenoss Core	Містить систему моніторингу за допомогою ICMP запитів і SNMP. Переваги: відстежує параметри мережі від потоку трафіку до HTTP та FTP. Недоліки: - непопулярний; - складний в налаштуванні.	Моніторинг мереж корпоративного рівня.	Побудована На подійно-орієнтованій архітектурі.

Компанії та підприємства намагаються скоротити свої витрати та збалансувати бюджет за допомогою відкритого програмного забезпечення для моніторингу мережі. Згідно з порівняльним аналізом, програмне забезпечення Nagios Core було вибрано для розробки інформаційної системи, яка максимізує продуктивність, разом із найшвидшим способом вирішення конкретних завдань, що забезпечує обслуговування працюючого обладнання, а також працездатність усієї системи [17].

Через складність сучасної мережі та недостатність існуючих утиліт з відкритим кодом адміністраторам доводиться комбінувати кілька інструментів, щоб створити середовище моніторингу, яке відповідає їхнім потребам.

Інструменти моніторингу, які мають бути більш зручними для досягнення бажаного результату та працювати з мінімальними ресурсами, є невід’ємною частиною процесу моніторингу.

Таким чином, вибір конкретного програмного забезпечення для моніторингу корпоративної мережі повинен ґрунтуватися на цілях використання, типі інфраструктури, вимогах до масштабування, підтримки стандартів, інтеграції з іншими системами, а також на рівні підготовки персоналу. За результатами попереднього аналізу та з урахуванням доступних рішень, рекомендовано провести практичне тестування 2–3 систем у контрольному середовищі, що дозволить зробити остаточний вибір з урахуванням особливостей конкретної мережі.

РОЗДІЛ 3

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗАКЛАДУ ОСВІТИ

3.1 Опис та аналіз інформаційних потоків корпоративних мереж.

Корпоративна комп'ютерна мережа займається інформаційним потоком будь-якого навчального закладу. Вона забезпечує внутрішній централізований доступ до глобальної мережі Інтернет, корпоративну електронну пошту, уніфіковані корпоративні сервіси, а також надає можливість відеозв'язку та доступу до відеоконференцій, платформ дистанційного навчання тощо. Зміни формату вищої освіти у зв'язку з війною та наслідками пандемії COVID-19 актуалізують питання переходу до нових стандартів і саме у напрямку створення нового інформаційного освітнього простору. Матеріальна інформація впливає на діяльність вищого навчального закладу. Інформаційний потік - це сукупність інформації, яка циркулює в певному середовищі, тому обсяг інформації за одиницю часу представляє кількісний характер інформаційного потоку. Створене інформаційне середовище дозволяє удосконалити навчальний процес; зробити його насиченим і значущим, інтегрувати інформаційні технології з науковими.

Рисунок 3.1 – Інформаційне освітнє середовище закладу освіти

На тлі війни та пандемії COVID-19 форми навчання змінюються, що збільшує інформаційні потоки навчальних закладів і, отже, підвищує вразливість їх комп’ютерних мереж. Викає потреба в безпечній атмосфері обробки інформації всередині корпоративної комп'ютерної мережі. Сенс спостереження за такими мережами полягає в здатності дізнаватися, повідомляти, реагувати шляхом контролю, а також збоїв і нападів, які відбуваються в мережевій інфраструктурі.

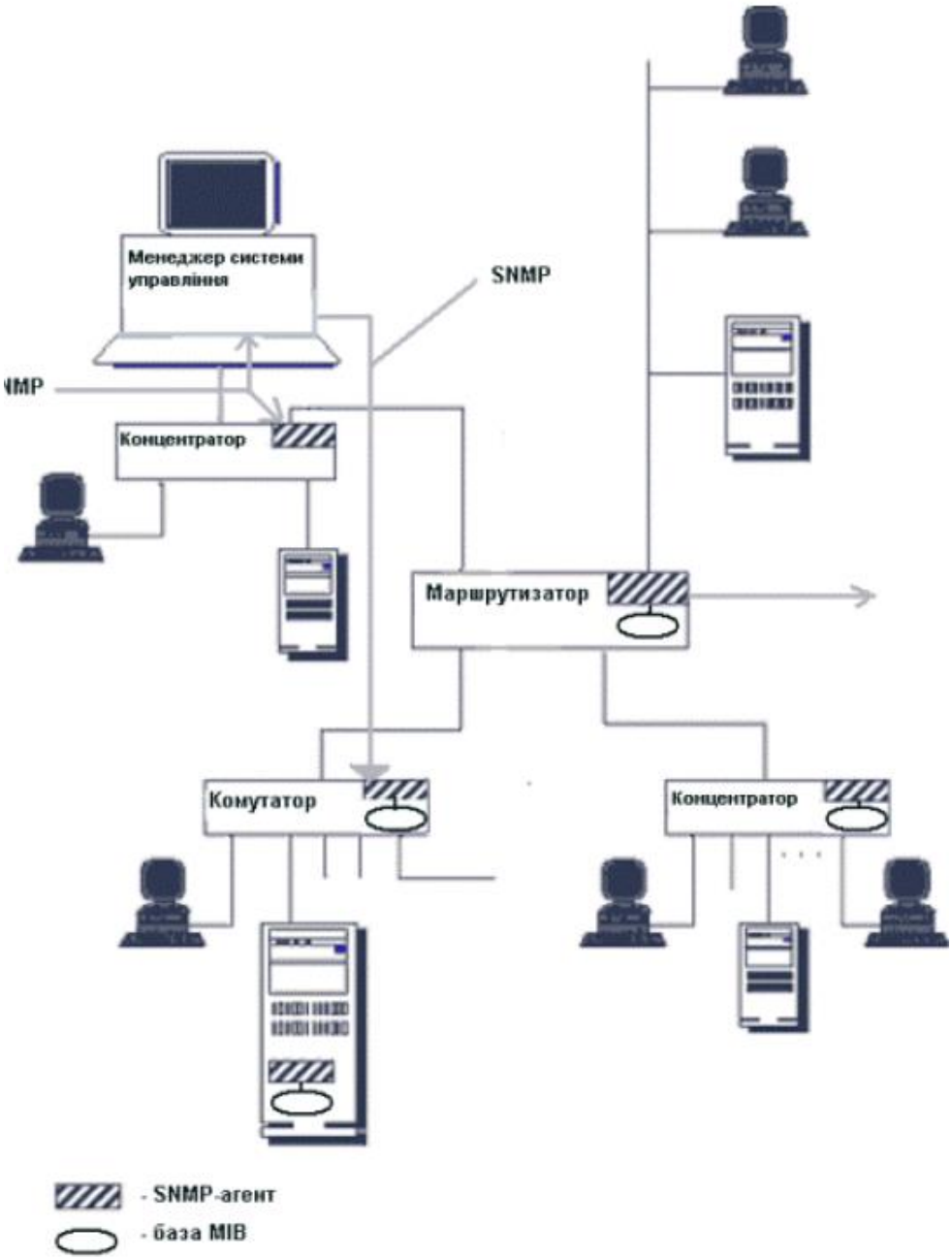


Рисунок 3.2 – Типова структура системи управління комп’ютерною мережею закладу освіти [18]

Оцінка комп’ютерної мережі та потенційних ринків для застосовного програмного забезпечення для моніторингу мережі розглядалася на основі таких факторів, як комерційна вартість, системні вимоги, складність інсталяції та базові налаштування для роботи з скомпрометованим вузлом, а також інші додаткові функції та сумісні системи тощо. Щоб вибрати систему комп’ютерного моніторингу, різне, найбільш популярне системне програмне забезпечення порівнювалося за характеристиками, здатністю виявляти уражений вузол, додатковими функціями, сумісністю з іншими системами тощо. Вибір програмного забезпечення для моніторингу комп’ютерної мережі навчального закладу у військових умовах базувалася на порівняльному аналізі недоліків і переваг різних, найпопулярніших програм моніторингу. У цьому випадку програмне забезпечення є сучасною, широко використовуваною системою моніторингу з відкритим кодом під назвою Nagios, яка працює під керуванням ядра Nagios Core.

3.2 Алгоритм роботи інформаційної системи моніторингу корпоративної комп’ютерної мережі закладу освіти

У ході моніторингу комп'ютерної мережі відбувається збір і обробка інформації. Саме з проаналізованої інформації проводиться систематизація, щоб показати проблеми мережі. З цього випливає, що для вирішення виявленої проблеми система використовує відповідні плагіни для типу проблеми. Після операції усунення аномалії результати надсилаються у звіті, відомому як звіт про вирішення проблеми (рис. 3.3).

Як стверджують розробники [19], завдання Nagios Core полягає в зборі та генеруванні інформації про загальний стан мережевої інформаційної системи, підключення статично проаналізованого системного журналу та журналів встановлення програм керування мережевими пакетами, системних журналів виявлення вторгнень тощо, шляхом порівняння цих положень вимог до оцінки ризиків щодо мережевої інфраструктури та мати інтерактивний набір

функціональних інструментів, додатків, кожен з яких відповідає за певний етап моніторингу інформаційної системи за допомогою інструментів для зв’язку, аналізу, додатки для порівняння, моделювання та прийняття рішень для роботи та забезпечення безперервного моніторингу системи, додатків, послуг і процесів в інформаційній системі, а також пошуку першопричини проблеми, активного спостереження за всією мережевою інфраструктурою та автоматичного усунення всіх проблем у міру їх виникнення.

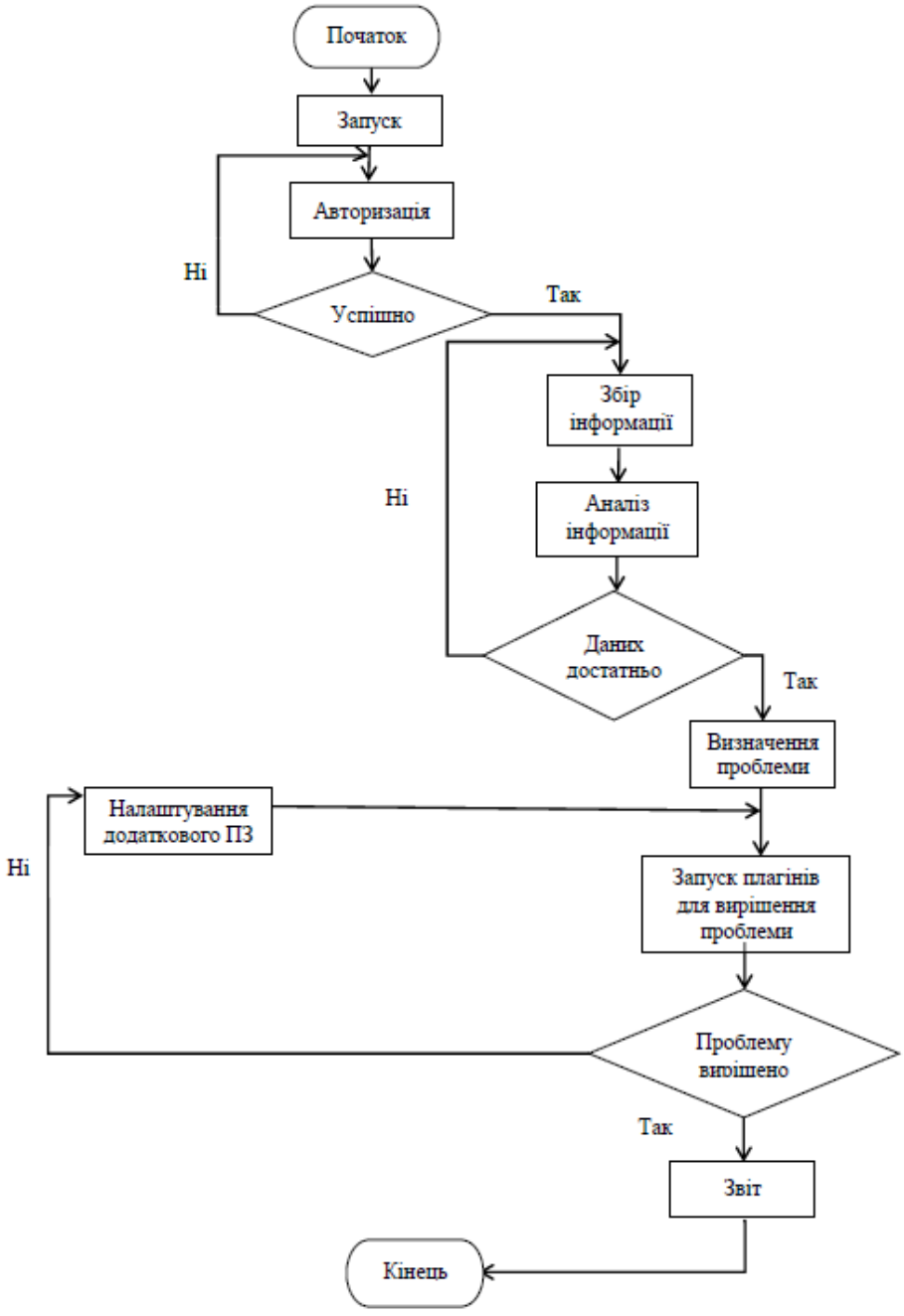


Рисунок 3.3 – Алгоритм роботи інформаційної системи моніторингу корпоративної комп’ютерної мережі

У разі збою в мережі мережевий хост, який має можливість обробляти значну кількість процесів завдяки підтримці багатьох ядер, надсилає попередження системному адміністратору про виниклу проблему. Це дозволяє оперативно розпочати усунення несправностей ще до того, як вони вплинуть на бізнес-процеси або кінцевих користувачів.

Ядро системи моніторингу розміщується на сервері, де також встановлено відповідні плагіни. Плагіни — це скомпільовані модулі або скрипти (наприклад, сценарії на мові оболонки), які виконуються з командного рядка для перевірки стану хоста. Запуск плагінів ініціюється за допомогою так званого "планувальника процесів", який входить до складу серверної частини Nagios Core. Цей планувальник виконує плагіни на локальному сервері або віддалених хостах, збирає результати виконання й передає їх на подальшу обробку. Зібрані дані використовуються для створення звітів, які виводяться в графічному вигляді через веб-інтерфейс, що дозволяє системному адміністратору оперативно реагувати на інциденти.

На рисунку 3.4 подано схематичне зображення процесу моніторингу в комп’ютерній мережі навчального закладу з використанням Nagios Core, який базується на архітектурі клієнт-сервер [20]. Основна програма Nagios (ядро) функціонує незалежно від плагінів, водночас надаючи інтерфейси API для їх інтеграції. Це дозволяє значно розширювати функціональність системи за допомогою додаткових надбудов.

Для запуску Nagios Core необхідна операційна система на базі Linux, мережевий інтерфейс та встановлений компілятор мови C. Для візуалізації результатів моніторингу використовуються CGI-модулі, які адміністратор може активувати за потреби. Згідно з документацією, для їх коректної роботи необхідна наявність веб-сервера, бажано Apache, а також бібліотеки gd версії 1.6.3 або вище (розроблена Томасом Бутеллом) [19].

Система Nagios підтримує декілька способів моніторингу віддалених серверів. Одним з найпоширеніших є використання плагіна NRPE (Nagios

Remote Plugin Executor), який дозволяє запускати плагіни безпосередньо на віддалених хостах Linux. Цей підхід особливо корисний для перевірки локальних параметрів, таких як використання дискового простору, завантаження процесора, обсяг доступної пам’яті тощо.

Хоча у даному випадку розглядається використання програмного забезпечення з відкритим кодом, можливе також поєднання з комерційними рішеннями або надбудовами з обмеженим доступом, що дозволяє розширити функціональність інформаційної системи відповідно до потреб конкретної організації.

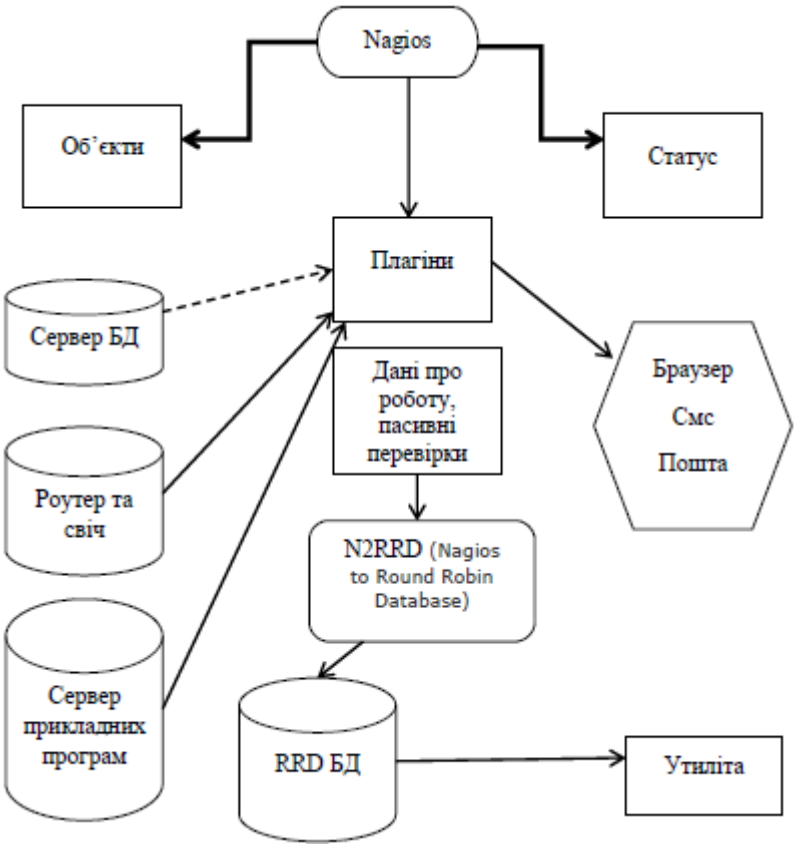


Рисунок 3.4 – Схема моніторингу комп’ютерної мережі з використанням Nagios

Плагіни для моніторингу служб застосовуються для контролю стану конкретних програм, служб або мережевих протоколів. Існує велика кількість як офіційних, так і сторонніх (додаткових) плагінів, що значно розширюють

можливості системи моніторингу. У разі відсутності необхідного плагіна користувач має змогу створити власний, скориставшись офіційною документацією з написання плагінів.

Моніторинг будь-якої служби операційної системи можна реалізувати через відповідні конфігураційні модулі. Передусім потрібно визначити хост, який відповідає за цю службу, створивши окремий конфігураційний файл або додавши відповідне визначення до існуючого файлу об’єктів. Аналогічно виконується конфігурування служб, які підлягають перевірці.

Nagios Core підтримує моніторинг широкого спектру служб, зокрема веб-серверів. Для цього використовуються спеціалізовані плагіни, наприклад, плагін check_http здійснює перевірку доступності веб-сервера за протоколом HTTP, а також контролює час відповіді, коди помилок, термін дії SSL-сертифікатів тощо. Для моніторингу FTP-серверів застосовується плагін check_ftp, а для SSH-серверів — check_ssh, який перевіряє доступність SSH-служби та в разі відсутності відповіді протягом встановленого часу (наприклад, 10 секунд) генерує відповідне попередження.

Аналогічним чином здійснюється моніторинг поштових серверів, серверів баз даних та інших критично важливих служб. Для кожного з таких типів моніторингу, особливо у контексті мережі навчального закладу, слід чітко визначити необхідні об’єкти спостереження. Реалізація цієї процедури передбачає внесення нових записів про хости та сервіси у відповідні конфігураційні файли об’єктів, після чого систему необхідно перезапустити.

У разі виникнення помилок під час перевірки конфігурації, слід негайно усунути неточності у відповідних файлах. Лише за відсутності помилок конфігурації процес моніторингу можна вважати коректним, і він може бути безперервно виконуваним у продуктивному середовищі.

3.3 Налаштування програмного забезпечення інформаційної системи моніторингу корпоративної комп’ютерної мережі закладу освіти

Необхідними умовами для налаштування Nagios є вибір дистрибутива. За словами виробника, Nagios працює на дистрибутивах Linux і UNIX. Ми будемо використовувати Linux. Перевірте, чи встановлено сервер Apache.

Розглянемо поетапно, як встановлюється програмне забезпечення, вибране для моніторингу мережі, і як воно виглядає на екрані монітора.

1. Встановлюємо і запускаємо веб-сервер Apache httpd.

2. Встановлюємо дистрибутив PHP.

3. Налаштовуємо сервер Nagios і ключові плагіни для моніторингу сервера Nagios.

Одночасно переглянемо командний рядок на моніторі, як показано на рис. 3.5., де бачмо наступне:

```
# install from EPEL
[root@dlp ~]# yum --enablerepo=epel -y install nagios nagios-plugins-{ping,disk,users,procs,load,swap,ssh,http}
```

Рисунок 3.5 – Системна консоль процесу встановлення сервера Nagios [21]

На екрані монітора цей процес відображається у командному рядку з переліком команд інсталяції та налаштування (рис. 3.6).

```
[root@dlp ~]# vi /etc/httpd/conf.d/nagios.conf

# line 24-26, change settings to set access permissionlike follows ( set for line 54-56, too )
# Require all granted
# Require local
Require ip 127.0.0.1 10.0.0.0/24

# add nagios admin user
[root@dlp ~]# htpasswd /etc/nagios/passwd nagiosadmin
New password:     # set any password
Re-type new password:
Adding password for user nagiosadmin

[root@dlp ~]# systemctl start nagios
[root@dlp ~]# systemctl enable nagios
[root@dlp ~]# systemctl restart httpd
```

Рисунок 3.6 – Системна консоль, налаштування сервера Nagios

Далі для безпечної роботи сервісу необхідно створити спеціального користувача та групу:

sudo useradd nagios

sudo groupadd nagcmd

sudo usermod -a -G nagcmd nagios

sudo usermod -a -G nagcmd www-data # для доступу до веб-інтерфейсу

4. Дозволяємо запуск служби за протоколом HTTP (рис. 3.7).

```
[root@dlp ~]# firewall-cmd --add-service={http,https} --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
```

Рисунок 3.7 – Системна консоль, налаштування служби HTTP[21].

Веб-інтерфейс Nagios потребує створення користувача з паролем для доступу до моніторингу:

sudo htpasswd -c /etc/nagios4/htpasswd.users nagiosadmin

Після цього переконуємося, що веб-сервер Apache налаштований правильно: у конфігурації веб-сервера прописується шлях до CGI-скриптів Nagios. Потім запускаємо або перезапускаємо Apache, використовуючи команду:

sudo systemctl restart apache2

Всі параметри моніторингу задаються у конфігураційних файлах, наприклад у файлі hosts:

sudo nano /etc/nagios4/conf.d/hosts.cfg

У цьому файлі додаються хости (сервери, маршрутизатори, робочі станції):

```
define host {
    use             linux-server
    host_name       server1
    alias           Основний сервер
    address         192.168.1.10
}
```

У файл services.cfg додаються сервіси, які потрібно моніторити (наприклад, ping, HTTP, SSH):

```
define service {
   use                  generic-service
   host_name            server1
   service_description  PING
   check_command        check_ping!100.0,20%!500.0,60%
}
```

5. Встановлення та налаштування NRPE на віддалених хостах

На віддалених машинах, які потрібно моніторити, встановлюється NRPE (Nagios Remote Plugin Executor):

```
sudo apt install nagios-nrpe-server nagios-plugins
```

Далі у конфігураційному файлі /etc/nagios/nrpe.cfg вказується IP-адреса сервера Nagios, якому дозволено виконувати перевірки:

```
allowed_hosts=127.0.0.1,192.168.1.5
```

Після цього перезапускається служба NRPE:

```
sudo systemctl restart nagios-nrpe-server
```

6. Перевірка конфігурації та запуск Nagios

Після внесення змін до конфігураційних файлів необхідно перевірити правильність налаштувань:

```
sudo nagios4 -v /etc/nagios4/nagios.cfg
```

Якщо все налаштовано правильно, сервіс Nagios перезапускається:

```
sudo systemctl restart nagios4
```

7. Далі отримуємо доступ до порталу [http: // (ім’я хосту або IP-адреси сервера Nagios) / nagios /] від клієнта, який знаходиться в мережі, яка дозволена сервером Nagios, та автентифікуємось для входу з користувачем з правами адміністратора Nagios [nagiosadmin], якого ми додали під час попереднього налаштування (рис. 3.8).

Рисунок 3.8 – Вікно авторизації в сервер Nagios

8. Після успішної автентифікації відображається сайт адміністратора Nagios (рис. 3.9). Там можна переглянути стан системи, натиснувши "Тактичний огляд" тощо (рис. 3.10, рис. 3.11).

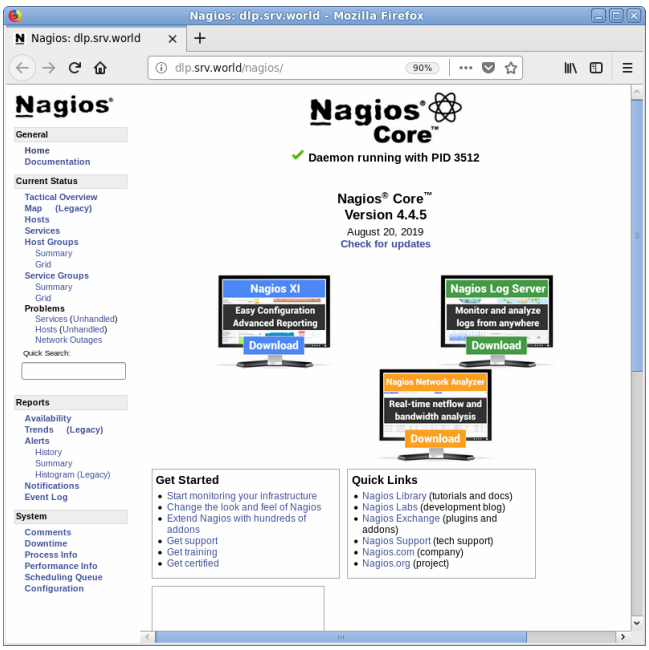


Рисунок 3.9 – веб-інтерфейс системи адміністрування після успішної авторизації[21]

Після основного налалаштування додаються нові шаблони, налаштовуються email-повідомлення, інтегрується з SMTP або іншими інструментами сповіщень. Також можлива інтеграція з іншими системами, як-от Prometheus, Zabbix або Elasticsearch.

Кожен із описаних вище етапів може бути автоматизований за допомогою скриптів (наприклад, Bash або Ansible) для швидкого розгортання системи моніторингу на великій кількості серверів.

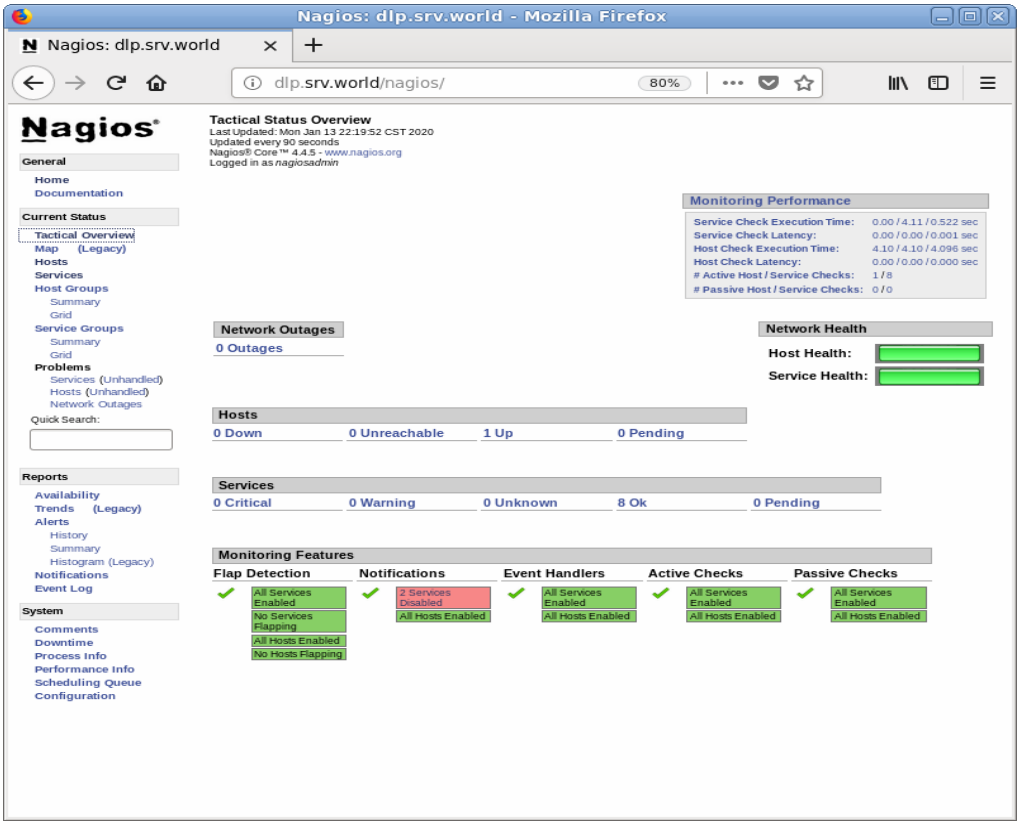


Рисунок 3.10 – веб-інтерфейс стану системи

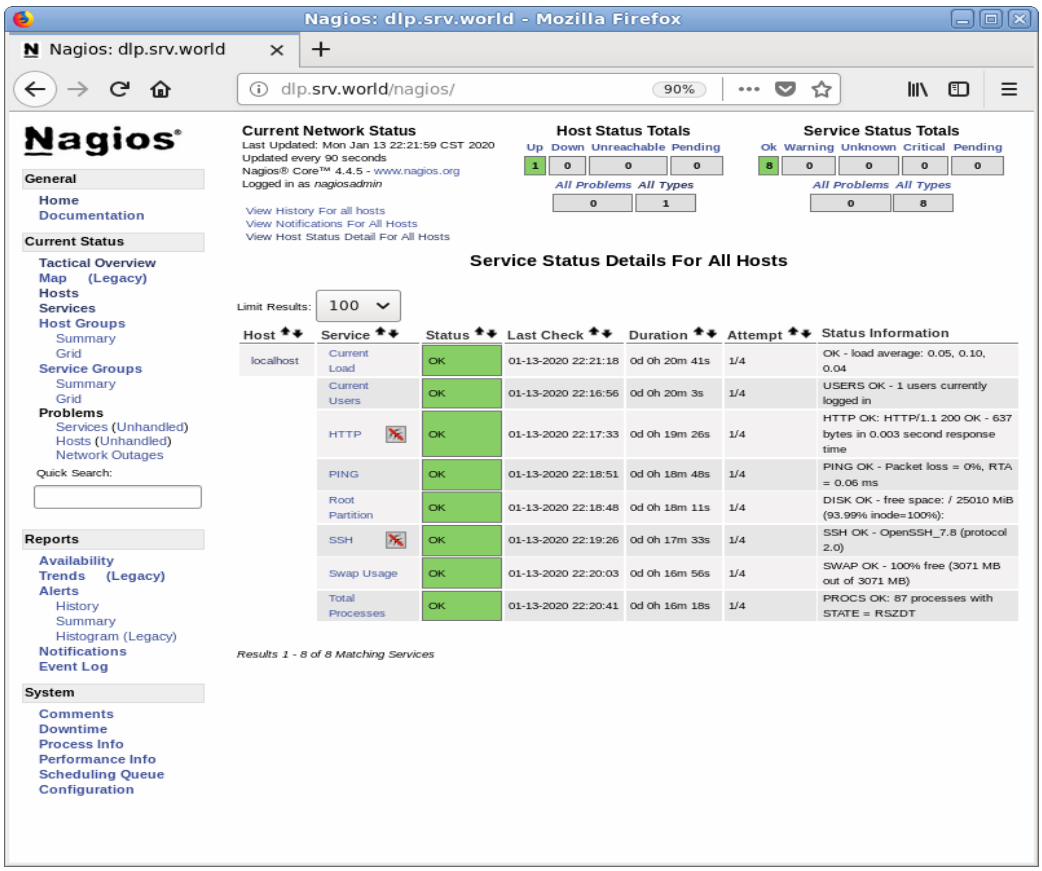


Рисунок 3.11 – веб- інтерфейс тактичного огляду системи

У результаті проведеного поетапного налаштування системи Nagios Core було розгорнуто повноцінне середовище для моніторингу стану корпоративної комп’ютерної мережі, що базується на відкритому програмному забезпеченні. Детально розглянуто інсталяцію серверної частини, налаштування користувачів та прав доступу, конфігурування основних параметрів моніторингу, зокрема хостів і сервісів, а також інтеграцію плагінів для перевірки різних типів мережевих служб.

Особливу увагу приділено налаштуванню віддаленого моніторингу за допомогою NRPE, що дозволяє отримувати інформацію про критичні системні ресурси на віддалених вузлах. Також розглянуто способи інтеграції Nagios із веб-інтерфейсом Apache, забезпечення автентифікації адміністратора та запуску системи моніторингу у продуктивному середовищі.

Усі налаштування виконані відповідно до вимог безпеки, а конфігураційні файли організовані з дотриманням структурованого підходу.

Запропонована методика може бути легко масштабована та автоматизована для великої кількості вузлів за допомогою сценаріїв автоматичного розгортання (наприклад, за допомогою Bash або Ansible).

Загалом, система Nagios Core є ефективним і гнучким інструментом для моніторингу мережі навчального закладу або корпоративного середовища, що дозволяє своєчасно реагувати на збої, підтримувати стабільність інфраструктури та забезпечувати її безперебійну роботу.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Структурно-функціональний аналіз виробничого процесу та розроблення моделі травмонебезпечних ситуацій

У зображеннях процесів формування, виникнення аварій та виробничих травм усі випадкові події, що утворюють конкретну аварійну ситуацію, пов'язані між собою причинно-наслідковими зв'язками.

Метод логічного моделювання потенційних аварій, травм та катастроф відкриває можливість розробити досконалу систему управління ОП виробництва, яка базується на оперативному пошуку виробничих небезпек, їх глибокому аналізі й терміновому прийнятті заходів для усунення потенційних небезпек ще до виникнення травмонебезпечних та катастрофічних ситуацій. Деякі небезпечні ситуації в табл. 4.1.

Працівники, що обслуговують електрообладнання вениляційної системи, зобов'язані знати Правила безпечної експлуатації електроустановок споживачів відповідно до займаної посади або роботи, як вони виконують, і мати відповідну групу з електробезпеки [21,22].

Працівники, що порушили вимоги Правил безпечної експлуатації електроустановок, усуваються від роботи і несуть відповідальність (дисциплінарну, адміністративну, кримінальну) згідно з чинним законодавством. Такі працівники не допускаються до робіт в електроустановках без позачергової перевірки знань вимог правил безпечної експлуатації електроустановок.

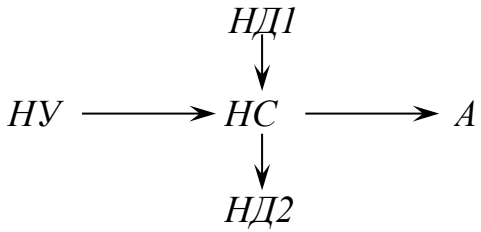
Забороняється допускати до роботи в електроустановках осіб, які не пройшли навчання і перевірку знань Правил безпечної експлуатації електроустановок.

Працівнику, який пройшов перевірку знань Правил безпечної експлуатації електроустановок, видається посвідчення встановленої форми.

Таблиця 4.1. Моделювання процесів формування та виникнення травмонебезпечних і аварійних ситуацій

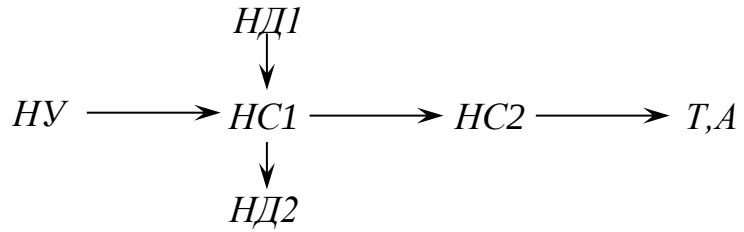
Вид робіт	Виробнича небезпека			Можливі наслідки	Заходи запобігання небезпечним ситуаціям
	Небезпечна умова (НУ)	Небезпечна дія (НД)	Небезпечна ситуація (НС)		
Використання механічної вентиляції	Оператор не перевірив обладнання НУ	Пошкоджений трубопровід мережі НД1 Закупорений трубопровід шланга НД2	Відмова вентиляційної системи (двигуна) НС	Аварія	Розвісити плакати, провести інструктажі із експлуатації обладнання системи

Модель процесу:



Використання електронних пристроїв регулювання	Пошкоджена ізоляція провідників з’єднання НУ	Пробій на корпус НД1 Коротке замикання НД2	Ураження людини електричним струмом НС1 Виведення обладнання із ладу НС2	Травма Аварія	Заміна провідників, установлення захисного обладнання (запобіжників, захист від ураження людини струмом) тощо

Модель процесу:



Посвідчення про перевірку знань працівника є документом, який засвідчує право на самостійну роботу в електроустановках на зазначеній посаді за фахом.

4.2. Вимоги техніки безпеки під час роботи обладнання та протипожежні заходи

Вимоги правил техніки безпеки перед початком роботи. Для початку роботи пов'язаної з вентиляцією вимикають рубильники або автоматичні вимикачі щита низької напруги, запирають шафу і вивішують попереджувальні плакати. Також повинні бути основні захисні засоби до яких належать такі, ізоляція яких надійно захищає від робочої напруги мережі і за допомогою яких можна дотикатися до струмопровідних частин, що перебувають під напругою, без небезпеки ураження електричним струмом (інструмент з ізольованими ручками, ізолюючі струмовимірювальні кліщі, діелектричні рукавиці).

Вимоги правил техніки безпеки під час роботи. Виконавши ці операції, надівають діелектричні рукавиці і за допомогою покажчика напруги перевіряють відсутність напруги на всіх фазах. Потім, приєднавши один кінець переносного заземлення до заземлюючого пристрою, накладають його на струмоведучі частини. Після цього остаточно приступають до роботи.

Вимоги правил техніки після закінчення роботи. Після закінчення роботи системи перед її вимиканням необхідно виконати такі технічні операції: перевірити надійність кріплення, зняти переносні тимчасові заземлення, відімкнути щит низької напруги і зняти плакати з техніки безпеки; якщо тимчасове переносне заземлення встановлене на лінії, його також треба зняти тощо [21].

Протипожежні заходи на об'єкті. Для запобігання пожеж на об'єкті розроблено організаційні, експлуатаційні, технічні режимного характеру, пожежно-евакуаційні, профілактичні заходи. До організаційних заходів відносяться правила розміщення машин, що обслуговують приміщення,

обладнання, матеріалів з дотримання певних проходів, не допускається захаращення приміщень, проходів і т.д.

4.3. Розрахунок штучного заземлення

Вибір штучного заземлення проводиться в залежності від характеру ґрунту і способу забивання стержнів [21]. Розраховуємо заземлюючий контур підстанції напругою 10/0,4 кВ з глухозаземленою нейтраллю. Характер ґрунту – чорнозем з $\rho=2\cdot10^4$ Ом·см. Кліматична зона – IV (K_c – 1,2, K_n – 1,5). Струм замикання на землю в мережі становить 50 А.

В відповідності з діючими правилами, опір заземлюючого пристрою повинен становити

$$R=\frac{125}{I_з}=\frac{125}{50}=2,5Ом, \qquad (4.1)$$

де $I_з$ – струм замикання на землю, А.

Приймаємо 3 Ом. Контур заземлення розміщуємо в ряд з а = 5 м, l = 2,5 м. В якості стержневого заземлювача приймаємо кутникові сталь 50х50х5 мм, а протяжного – пластинчасту сталь 40х4 мм.

Опір одиночного стержня становить:

$$R_o=0.00318\rho\cdot K_c, Ом \qquad (4.2)$$

де K_c – коефіцієнт сезонності для стержневого заземлювача (K_c – 1,2).

$$R_o=0.00318\cdot 2\cdot 10^4\cdot 1.2=76.32Ом.$$

Число стержнів приймаємо 15. При цьому коефіцієнт використання стержневих заземлювачів становить η_c = 0,7. Опір всіх стержнів розтікання струму становить:

$$R_c=\frac{R_o}{n\cdot\eta_c}, Ом, \qquad (4.3)$$

де n – число стержнів, шт.

$$Rc = \frac{76.32}{15 \cdot 0.7} = 7.3 Ом .$$

Довжина протяжного заземлювача становить l = 35 м (3500 см); приймаємо t = 50 см, b = 0,4 см. Опір протяжного заземлювача становить:

$$R_{пр} = \frac{0,366}{l} \cdot \rho \cdot 2 \cdot \lg \frac{2 \cdot l^2}{t \cdot b}, Ом \qquad (4.4)$$

$$R_{пр} = \frac{0,366}{3500} \cdot 1,2 \cdot 10^4 \cdot 2 \cdot \lg \frac{2 \cdot 3500^2}{0,4 \cdot 50} = 3,2 Ом$$

Коефіцієнт використання протяжного заземлювача η_n = 0,71. Дійсний опір протяжного заземлення становить:

$$R_n = \frac{R_{пр}}{\eta_n} = \frac{3,2}{0,71} = 4,5 Ом \qquad (4.5)$$

Опір всього заземлюю чого пристрою становить:

$$R_u = \frac{R_c \cdot R_n}{R_c + R_n} = \frac{4.5 \cdot 7.3}{4.5 + 7.3} 2.78 < 3 Ом \qquad (4.6)$$

Отже, число стержнів вибрано вірно.

4.4. Захист цивільного населення

Забезпечення захисту населення і території у разі загрози та виникнення надзвичайних ситуацій є одним з найважливіших завдань не лише підприємства, але й цілої держави. Актуальність проблеми забезпечення природо-техногенної безпеки населення і території зумовлена тенденціями зростання втрат людей і шкоди територіям, що спричиняються небезпечними природними явищами, промисловими аваріями і катастрофами.

Інженерний захист проводиться з метою виконання вимог ІТЗ із питань забудови міст, розміщення ПНО, будівлі будинків, інженерних споруд та інше.

Медичний захист проводиться для зменшення ступеня ураження людей, своєчасного надання допомоги постраждалим та їх лікування, забезпечення епідеміологічного благополуччя в районах надзвичайних ситуацій.

Біологічний захист включає своєчасне виявлення чинників біологічного зараження, їх характеру і масштабів, проведення комплексу адміністративно-господарських, режимно-обмежувальних і спеціальних протиепідемічних та медичних заходів.

Радіаційний і хімічний захист включає заходи щодо виявлення і оцінки радіаційної та хімічної обстановки, організацію і здійснення дозиметричного та хімічного контролю, розроблення типових режимів радіаційного захисту, забезпечення засобами індивідуального захисту, організацію і проведення спеціальної обробки.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У даній кваліфікаційній роботі розглянуто актуальну проблему управління корпоративною комп'ютерною мережею та обґрунтовано її значущість у сучасних умовах функціонування інформаційних систем. Особливу увагу приділено етапам аналізу та моніторингу, які є ключовими для забезпечення стабільної та безпечної роботи мережевої інфраструктури.

Зазначено, що ефективне управління мережею неможливе без використання спеціалізованих інструментів моніторингу, до яких належать аналізатори протоколів, діагностичні засоби, експертні системи та багатофункціональні комплекси. Знання базових принципів моніторингу та гнучка підтримка різноманітних конфігурацій є основою для створення прозорої та контрольованої мережі.

У ході дослідження було проаналізовано сучасні підходи до моніторингу корпоративних комп'ютерних мереж, виявлено їхню складність, яка зумовлена зростанням обсягів даних, кількості вузлів і жорсткими вимогами до безпеки. Визначено ключові функціональні вимоги до систем спостереження, серед яких — збирання статистичних даних, контроль пропускної здатності, оптимізація трафіку та оперативне реагування на збої.

На основі порівняльного аналізу обрано набір програмних інструментів моніторингу, які відповідають вимогам практичності, доступності, простоти у використанні, гнучкості, наявності графічного інтерфейсу, функціонального наповнення та підтримки збереження даних.

Значна частина теоретичних і практичних досліджень була спрямована на вдосконалення інформаційної системи моніторингу комп'ютерної мережі навчального закладу, зокрема на підвищення її функціональності, масштабованості та зручності адміністрування. У результаті проведеного аналізу було запропоновано впровадити програмне забезпечення з відкритим кодом — Nagios Core, яке дозволяє організувати ефективний процес контролю та управління мережею, а також забезпечити рівномірний розподіл трафіку між

відділами закладу освіти.

Вибране програмне забезпечення продемонструвало відповідність більшості поставлених завдань і стало основою для створення гнучкої системи спостереження. Водночас встановлено, що для повноцінного покриття усіх потреб мережі необхідне подальше розширення системи за рахунок розробки та впровадження додаткових надбудов і плагінів, які дозволять автоматизувати ключові процеси, інтегрувати сповіщення, покращити інтерфейс та розширити функціонал збору метрик.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пастернак І. І., Інформаційні системи, мережі та технології.– Національний університет «Львівська політехніка», 2017 – Режим доступу: http://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/12996/ilovepdfcom-3-9.pdf

2. Кучеров Д.П. Керування перевантаженням комп'ютерної мережі. – Навчально-науковий інститут Комп'ютерних інформаційних технологій Національного авіаційного університету, Київ, Україна – Режим доступу: http://ceur-ws.org/Vol-2067/paper10.pdf

4. Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Muhammad Inayatullah Babar. An Efficient Network Monitoring and Management System. – International Journal of Information and Electronics Engineering, Vol. 3, No. 1, January 2013 – Режим доступу: https://core.ac.uk/download/pdf/207663439.pdf.

5. D.Doliwa, M.Frydrych, W.Horzelski, Network Monitoring and Management for Company with Hybrid and Distributed Infrastructure, Information Systems in Management, 2016, tom 5, nr 3, 326-335

6. Alisha Cecil, «A Summary of Network Traffic Monitoring and Analysis Techniques» Comput. Syst. Anal. (2006), pp. 4-7 – Режим доступу: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html.

7. M.Uma and G.Padmavathi. Article: An Efficient Network Traffic Monitoring for Wireless Networks. – International Journal of Computer Applications 53(9):51-59, September 2012. Режим доступу: https://www.researchgate.net/publication/258652349_An_Efficient_Network_Traffic_Monitoring_for_Wireless_Networks

8. Ahmed Dooguy Kora, Moussa Moindze Soidridine, Nagios Based Enhanced IT Management System. CoRR abs/1206.1611 (2012). – Режим доступу: https://www.researchgate.net/publication/225284738_Nagios_Based_Enhanced_IT_Ma nagement_System

9. C. Issariyapat, P. Pongpaibool, S. Mongkolluksame, K. Meesublak, Using Nagios as a Groundwork for Developing a Better Network Monitoring System, in: 2012

Proceedings of PICMET 2012: Technology Management for Emerging Technologies, 2012.– Режим доступу: https://www.researchgate.net/publication/261281885_Using_Nagios_as_a_groundwork for_developing_a_better_network_monitoring_system

10. Rafiullah Khan, Sarmad Ullah Khan. Design and Implementation of an Automated Network Monitoring and Reporting Back System, November 2017, Journal of Industrial Information Integration. – Режим доступу: https://www.researchgate.net/publication/321224252_Design_and_Implementation_of_ an_Automated_Network_Monitoring_and_Reporting_Back_System

11. Тарнавський Ю. А., Кузьменко І. М. Організація комп'ютерних мереж, Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_me rej.pdf

12. Гузій М. М., Станіславова О. В., Кадет М.В. Аналіз технологій моніторингу комп'ютерних мереж. – Режим доступу: http://jrnl.nau.edu.ua/index.php/SBT/article/download/5091/5353

13. Afeez Yusuff, Network monitoring : Using Nagios as an Example Tool. Bachelor's thesis Central Ostrobothnia University of Applied Sciences Degree Programme in Information Technology, May 2012. – Режим доступу: https://www.theseus.fi/bitstream/handle/10024/48457/Yusuff_Afeez.pdf?sequence=1&i sAllowed=y

14. ISO. Online browsing platform [Електронний ресурс]: – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

15. Організація комп'ютерних мереж: конспект лекцій [Електронний ресурс]: Л.М. Олещенко; КПІ ім. Ігоря Сікорського, 2018.–225 с. – [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/22890/1/Organizacia_komputernyh_merezh_Ko nspekt_lekciy.pdf

16. Черепанська І. Ю. Автоматизація процесів керування вибором пристроїв орієнтування при проектуванні гнучких інтегрованих систем: дис. Канд. Техн. Наук: 05.13.07 "Автоматизація процесів керування" / Ірина Юріївна

Черепанська. – Київ, 2008. – 380 с.17.

17. Вікі ЦДПУ. Засоби моніторингу та аналізу мережі. – [Електронний ресурс]. – Режим доступу: https://wiki.cuspu.edu.ua/index.php/%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%BC%D0%BE

18. Nagios.The Industry Standard In IT Infrastructure Monitoring.– [Електронний ресурс]. – Режим доступу: https://www.nagios.org/

19. Edureca! Nagios Tutorial – Continuous Monitoring With Nagioshttps [Електронний ресурс]. – Режим доступу: https://www.edureka.co/blog/nagios-tutorial/

20. Nagios 4: Install. – [Електронний ресурс]. – Режим доступу: https://www.server-world.info/en/note?os=CentOS_8&p=nagios&f=1

21. Пістун І. П., Тимочко В.О., Городецький І. М.. Березовецький А. П. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. ІІ. Львів: Тріада плюс, 2011. 224 с.

22. Пістун І. П., Тимочко В.О., Городецький І. М.. Березовецький А. П. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. ІІ. Львів: Тріада плюс, 2011. 224 с.