МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Галанзовська Кароліна Валентинівна
(прізвище, ім'я, по батькові здобувача освіти)

УДК 004.02

КВАЛІФІКАЦІЙНА РОБОТА

Інформаційна система моніторингу функціонування корпоративної комп'ютерної мережі

122 «Комп'ютерні науки»

Подається на здобуття освітнього ступеня бакалавр

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ К. В. Галанзовська
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи

Черепанська Ірина Юріївна
доктор технічних наук, доцент

Житомир – 2021

Висновок кафедри _____

за результатами попереднього захисту: _____

Протокол засідання кафедри _____

№ ____ від «_____» _____ 20____ р.

Завідувач кафедри _____

_____ _____ _____

(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)

(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____

за шкалою ECTS _____

за національною шкалою _____

Секретар ЕК

_____ _____ _____

(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Галанзовська К.В. Інформаційна система моніторингу функціонування корпоративної комп’ютерної мережі. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 122 – Комп’ютерні науки. – Поліський національний університет, Житомир, 2021.

Проведено аналіз інформаційної системи моніторингу корпоративної комп’ютерної мережі, на підставі чого розроблено інформаційну систему моніторингу корпоративної комп’ютерної мережі з підвищеним забезпеченням безпеки, зокрема, захистом від несанкціонованих доступів, атак, критичних станів та аномалій, та можливістю своєчасного попередження про можливі збої в її роботі.

Визначено функції та проаналізовано задачі моніторингу функціонування корпоративної комп’ютерної мережі. Вивчено структуру системи, обрано на основі аналізу найбільш придатне програмне забезпечення та розроблено алгоритм роботи інформаційної системи моніторингу корпоративної комп’ютерної мережі.

Розроблені вимоги до системи моніторингу на основі наведеного аналізу мережі та систем моніторингу, дозволили обрати найоптимальніше за функціональними вимогами програмне забезпечення, необхідне для закладу освіти в сучасних умовах.

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

SUMMARY

Halanzovska K. Information system for monitoring the functioning of the corporate computer network. - Graduation thesis on the rights of an article.

Graduation thesis for the bachelor's degree in the speciality 122 – Computer science. – Polissia National University, Zhytomyr, 2021.

An analysis of the information monitoring system of the corporate computer network has been carried out, on the basis of which the information monitoring system of the corporate computer network with enhanced security protection has been developed, in particular, protection against unauthorized access, attacks, critical conditions and anomalies, and the possibility of instant notification of possible failures in its functioning.

Functions are identified and tasks for monitoring the functioning of the corporate computer network are analyzed. The system structure is studied, the most appropriate software is selected on the basis of the analysis, and the algorithm of software functioning for monitoring the information system of the corporate computer network is elaborated. Designed requirements for the monitoring system based on the given analysis of the network and monitoring systems can select the most optimal software for functional requirements, which is necessary for educational institutions in modern conditions.

Key words: computer network monitoring, software, server

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 6
ВСТУП..... 7
РОЗДІЛ 1 АНАЛІЗ ЗАДАЧІ МОНІТОРИНГУ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ……...…….....10
1.1 Аналіз проблеми моніторингу функціонування корпоративної комп'ютерної мережі……...…10
1.2 Задачі та функції системи моніторингу функціонування корпоративної комп'ютерної мережі……11
1.3 Аналіз сучасних підходів до проблеми моніторингу функціонування корпоративної комп'ютерної мережі……...12
1.4 Мета та задачі кваліфікаційної роботи …… ……..…18
Висновки до розділу 1 ……19
РОЗДІЛ 2 РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ……...…20
2.1 Структура системи моніторингу функціонування корпоративної комп'ютерної мережі……20
2.2 Аналіз та вибір програмного забезпечення для моніторингу корпоративних інформаційних систем……....24
Висновки до розділу 2 ……29
РОЗДІЛ 3 АЛГОРИТМ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ МОНІТОРИНГУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ …….…….30
3.1 Характеристика інформаційних потоків закладу освіти……...30
3.2 Алгоритм роботи інформаційної системи моніторингу корпоративної комп'ютерної мережі закладу освіти……...32
3.2 Програмне забезпечення інформаційної системи моніторингу корпоративної комп'ютерної мережі закладу освіти ……36
Висновки до розділу 3 ……...……40
ВИСНОВКИ ……..……..……41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……..…....43

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 сучасної корпоративної комп'ютерної мережі – це складний конгломерат різного розміру мереж та систем. З часом кількість обладнання комп'ютерних мереж збільшується, через що стає все важче відслідковувати та підтримувати в робочому, справному стані комп'ютерну мережу. Необхідно не тільки контролювати поточний стан обладнання, але і реагувати на наявність неробочих або пошкоджених вузлів. Із збільшенням клієнтської бази, активного користування мережею, виникає необхідність відслідковувати стан мережі.

В сучасних умовах управління мережами здійснюється шляхом перевірки сервісів та служб вручну. Крім того, доводиться працювати в умовах складного управління працездатністю серверів з використанням стандартних засобів моніторингу. Більшість проблем виявляються вже при виникненні їх у кінцевого користувача. Все це веде до перенавантаження технічного персоналу та системних адміністраторів, постійного погіршення якості послуг. Виходячи із зазначеного, моніторинг мережі є засобом управління та підтримки мережевих операцій та своєчасне реагування на збої та атаки. Таким чином, метою моніторингу мереж є управління мережею, своєчасне виявлення та усунення проблем комп'ютерної мережі. Вказане визначає **актуальність даної роботи**.

Метою кваліфікаційної роботи є розробка інформаційної системи моніторингу корпоративної комп'ютерної мережі з підвищеним забезпеченням безпеки, зокрема, захистом від несанкціонованих доступів, атак, критичних станів та аномалій, та можливістю своєчасного попередження про можливі збої в її роботі.

Для досягнення поставленої мети в роботі необхідно вирішити наступні **задачі**:

– визначити функції та проаналізувати задачі моніторингу функціонування корпоративної комп'ютерної мережі;

– розробити структуру системи моніторингу корпоративної комп'ютерної

мережі;

– на основі аналізу обрати платформу для розробки інформаційної системи та програмне забезпечення;

– розробити алгоритм функціонування інформаційної системи моніторингу корпоративної комп'ютерної мережі.

Об'єктом є процес моніторингу комп'ютерної мережі.

Предметом дослідження є інформаційна система моніторингу корпоративної комп'ютерної мережі.

За темою кваліфікаційної роботи було опубліковано наукові публікації, а саме:

– Галанзовська К. В., Керування інформаційною системою корпоративної комп'ютерної мережі в сучасних умовах. Матеріали І Міжнародної студентської наукової конференції «Пріоритетні напрямки та вектори розвитку світової науки», Миколаїв, травень 21, 2021. Том 2 с. 36;

– Черепанська І. Ю., Галанзовська К. В., Вибір програмного забезпечення для моніторингу корпоративних інформаційних систем. Матеріали Міжнародної наукової конференції «Комп'ютерні технології та сучасна інженерія – 2021», Житомир, 2021.

– Галанзовська К. В., Черепанська І. Ю., Опис функціонування Nagios для моніторингу інформаційної системи корпоративної комп'ютерної мережі. Матеріали Науково-практичної студентської конференції «Фінансове забезпечення економіки», Житомир, 2021.

Досліджено процес моніторингу корпоративної комп'ютерної мережі та проведено аналіз найпопулярнішого на ринку програмного забезпечення з відкритим вихідним кодом для моніторингу корпоративної комп'ютерної мережі на прикладі закладу освіти середнього розміру з урахуванням оснащеності робочих місць. Вивчено особливості корпоративної комп'ютерної мережі, її архітектура, етапи моніторингу та аналізу. Визначено, що відомі системи моніторингу можуть бути з успіхом застосовані у великих організаціях, але є громіздкими для навчального закладу середньої величини з порівняно невеликою

кількістю користувачів. Це обумовлює те, що більшість функцій такого програмного забезпечення залишаться незадіяними. Крім того, на основі наведеного аналізу мережі та систем моніторингу в роботі розроблені вимоги до системи моніторингу. Проте необхідно зауважити, що і обрана платформа не може в повній мірі реалізувати всі поставлені в роботі задачі, адже потребує розробки додаткових додатків та модулів, що вказує на необхідність подальших досліджень.

Кваліфікаційна робота складається зі вступу, трьох розділів, що включають дев’ять підрозділів, висновків, списку використаних джерел.

РОЗДІЛ 1
АНАЛІЗ ЗАДАЧІ МОНІТОРИНГУ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Аналіз проблеми моніторингу функціонування корпоративної комп'ютерної мережі

Несанкціонований доступ до мережної структури сьогодні є однією з основних загроз для мережних комп'ютерних систем, де міститься та передається конфіденційна та службова інформація. Несанкціонований доступ може призвести до витоку, знищення, модифікації важливих даних, в разі несвоєчасного виявлення проблеми та неналежного реагування. Щоб забезпечити безпечну та ефективну роботу мереж та систем, необхідно мати корпоративну платформу для моніторингу мереж з інтегрованими інструментальними функціями.

Слід зазначити, що запровадження карантину внаслідок пандемії коронавірусу COVID-19, привернуло особливу увагу до необхідності дистанційної роботи, яка поширюється на діяльність значної частини працівників для збереження їх здоров'я та забезпечення можливості безперебійної роботи. Адже і вітчизняні, і зарубіжні дослідники відзначають, що більшість опитаних найманих робітників та частина роботодавців і надалі готові працювати в дистанційному або змішаному режимі на регулярній основі або в окремих випадках. Проте перехід на віддалений режим роботи підвищує технологічні ризики несанкціонованого доступу до серверів, доступності систем, щодо витоку конфіденційної інформації та втрати даних.

Моніторинг та управління мережами - це завжди складне завдання для великих організацій зі складною топологією мережі. Мережевим інженерам та адміністраторам трудомістко вручну перевіряти робочий стан сотень або потенційно тисяч пристроїв у топології мережі. Навіть несправність мережі протягом кількох годин може спричинити значні фінансові збитки для організації

разом із втратою задоволеності споживачів. У багатьох організаціях досі існує система оскарження, коли працівник, клієнт реєструє скаргу на підключення до мережі, перш ніж адміністратори мереж почнуть вирішувати проблеми. Повідомлення, виявлення та виправлення несправностей у мережі можуть стати набагато швидшими завдяки розробці автоматизованої інформаційної системи моніторингу та управління мережею.

Актуальність даної теми полягає в складності управління інформаційними системами в сучасних умовах.

1.2 Задачі та функції системи моніторингу функціонування корпоративної комп'ютерної мережі

Для ефективного проведення діагностики, адміністратор має вивчати особливості мережі вже на етапі її проектування та формування, знати схему мережі, докладний опис конфігурації програмного забезпечення та апаратної частини із вказівкою всіх параметрів і інтерфейсів. Для оформлення та зберігання цієї інформації підійдуть спеціальні системи документування мережі у вигляді програмного та апаратного забезпечення. Використовуючи їх, системний адміністратор може заздалегідь знати всі можливі приховані дефекти і тонкі місця системи, щоб у випадку виникнення позаштатної ситуації віднайти, з чим пов'язана проблема – чи з устаткуванням, із програмним забезпеченням, ушкодженням програми або помилковими діями користувача.

Діагностика корпоративної мережі – процес (безперервний) аналізу стану інформаційної мережі. У разі виникнення несправності мережевих пристроїв фіксується факт несправності, визначається її місце і вид та заноситься ця інформація до файлів журналів. Повідомлення про несправності передається, пристрій чи вузол відключається і замінюється резервним або налагоджується. Постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної комп'ютерної мережі, необхідний для підтримки її в працездатному стані [1].

Основними задачами моніторингу комп’ютерних мереж є спостереження, отримання інформації про стан системи, аналіз отриманої інформації, оцінювання критичності стану, виявлення причин збою, прийняття рішень для подолання критичного стану комп’ютерної мережі.

Вирішення задачі моніторингу корпоративних комп’ютерних мереж розглядається як збір, обробка та аналіз інформації для поліпшення процесу працездатності системи та вирішується за рахунок ряду програм мережевого моніторингу [2].

Головною функцією моніторингу комп’ютерних мереж, виходячи із зазначеного, є забезпечення надійного функціонування шляхом своєчасного виявлення погіршень в роботі, аналіз їх та формування звітності для прийняття правильних управлінських рішень.

Функції моніторингу мережі зводяться до:

– перевірки стану всього мережного обладнання, а саме: маршрутизаторів, комутаторів, комп’ютерів користувачів;

– запису та аналізу повідомлень про помилки обладнання та справність усіх пристроїв.

1.3 Аналіз сучасних підходів до проблеми моніторингу функціонування корпоративної комп’ютерної мережі

Дослідження в галузі моніторингу комп’ютерних мереж проводились багатьма як вітчизняними, так і зарубіжними науковцями. Результати їх робіт наведені в літературі.

Так, наприклад, в роботі [3] автором розглядається комп’ютерна мережа, що функціонує в умовах перевантажень та збоїв. Автор встановлює типові причини та наслідки перевантажень комп’ютерних мереж. Ефективність комп’ютерної мережі визначається можливістю її функціонування в умовах перевантажень та збоїв, що є наслідком надлишкової буферизації системи. Одним з ефективних способів зменшення впливу перевантажень на мережу є резервування перепускної

здатності каналів та компенсація її частки в каналах, які піддаються найбільшому впливу. Проте, автор не розкрив питання щодо аналізу динамічних властивостей функціонування комп'ютерної мережі.

Автори [4] представляють ефективну та автоматичну систему моніторингу, яка постійно контролює всю мережу, перемикається та повідомляє адміністратора електронною поштою або sms, коли будь-який мережевий комутатор чи інше обладнання не працює. Ця система також вказує на розташування проблеми в топології мережі та її вплив на решту частин мережі. Система моніторингу мережі використовує розумну взаємодію Request Tracker (RT) та Nagios, програмне забезпечення в середовищі OS Linux. Мережева топологія побудована в Nagios, який постійно контролює всі вузли мережі на основі послуг, визначених для них. Nagios генерує повідомлення, як тільки мережевий вузол відключається і надсилає його до програмного забезпечення RT. Це повідомлення генерує тикет у базу даних RT з інформацією про проблемні вузли та її ефект на решту частин мережі. Програмне забезпечення RT налаштовано на повідомлення електронною поштою та sms адміністратора мережі, як тільки він був згенерований. Ця система моніторингу мережі є повністю автоматичною і адміністратор повинен перевіряти лише свої електронні листи та повідомлення. Представлена система моніторингу мережі є інтелектуальною для швидкого виявлення розташування проблеми в мережі, а також її впливу на решту мережі, що є високоефективним і забезпечує повний контроль над мережею [4].

У статті [5] представлена концепція та опис реалізації системи, призначеної для моніторингу та управління комп'ютерною мережею для великої компанії з гібридною та розподіленою інфраструктурою. Система базується на програмному забезпеченні Nagios, програмному забезпеченні Multi Router Traffic Grapher, NdoUtils, реляційній системі управління базами даних MySQL, системах візуалізації Nagios (NagVis, NagMap) та спеціальному додатку, створеному для системи, що дозволяє презентація відстежуваних ресурсів.

У цій статті [6] розглядаються методи моніторингу на основі маршрутизатора та методи моніторингу, що не базуються на маршрутизаторі.

Надається огляд трьох найпоширеніших доступних інструментів мережевого моніторингу (SNMP, RMON та Cisco Netflow), а також інформація про два новіші методи моніторингу, які використовують комбінацію пасивних та активних методів моніторингу (WREN та SCNM).

Представлена авторами [5] концепція системи моніторингу дозволяє створити ефективний додаток для моніторингу мереж LAN та WAN, використовуючи інструменти, засновані на програмному забезпеченні з відкритим кодом. Запропоновані рішення дозволяють масштабувати таку систему, яка може бути використана на малих, середніх та великих підприємствах. Система не вимагає високих вимог до обладнання. Це дозволяє нам утримувати низькі витрати як на їх створення, так і на впровадження на підприємстві з подальшим тех. обслуговуванням. Описані тут [5] рішення були встановлені, налаштовані та протестовані в лабораторних умовах.

У наш час комп'ютерні мережі великих підприємств та організацій часто є різнорідними мережами. Вони поєднують різні технології, використовуючи пристрої різних виробників, що працюють під різними операційними системами. Крім того, моніторинг та управління мережею не обмежуються одним місцем, але часто вимагають доступу до віддалених місць. У таких випадках один спеціальний інструмент не виконує своїх ролей, або вам потрібно одночасно використовувати кілька різних інструментів, що значно ускладнює адміністрування мережі та збільшує її вартість (придбання декількох інструментів, навчання працівників їх використанню).

Очевидно, що точний і ефективний моніторинг мережі життєво важливий для забезпечення вірності роботи мережі, з можливістю виправлення будь-яких відхилень. Однак поточна практика мережевого моніторингу багато в чому залежить від ручних операцій, і тому підприємства витрачають значну частину своїх бюджетів на персонал, який контролює їх мережі.

Вибираючи конкретний інструмент для моніторингу [6], адміністратор повинен спочатку вирішити, чи хочуть вони використовувати більш перевірену систему або нову систему. Якщо перевірена система - це напрям, який здається

більш зручним, NetFlow є найбільш корисним інструментом, оскільки разом з ним можна використовувати пакет аналізу даних для представлення даних в зручному для користувача середовищі; проте, якщо адміністратор бажає випробувати новішу систему, краще за все буде діяти комбінаційний підхід до моніторингу, такий як WREN або SCNM.

SNMP, RMON і Cisco NetFlow - це деякі з методів, заснованих на маршрутизаторах, які коротко розглянуті. Обговорювалися методи, які базуються на маршрутизаторах, - це інструменти активного, пасивного та комбінованого моніторингу.

Бездротові технології отримали величезний розвиток в останні роки, що дозволяє розробити нову бездротову систему [7]. Важливість передачі в сучасних бездротових мережах привела до розвитку декількох методів моніторингу мережевого трафіку. Термін «моніторинг трафіку» описує метод, за допомогою якого ідентифікуються всі дані, які відправляються і приймаються мережею, виявляються збої і небезпечні події, а хороші пакети даних проходять через мережі. Моніторинг мережевого трафіку є життєво важливою частиною кібербезпеки в наш час через зростаючу складності мереж і загроз, що створюються атаками на мережу, і це перший крок до виявлення атак. Методи моніторингу на основі маршрутизаторів останнім часом викликали великий інтерес через простоту їх використання, застосовність для досліджень і ефективності в моніторингу бездротових мереж. Дослідницька робота спрямована на пропозицію ефективної системи моніторингу мережевого трафіку. Пропонована система працює в два рази краще, ніж існуючі системи.

Точний моніторинг мережевого трафіку [7]є складним процесом через величезну природу Інтернету. Прогнозування нерегулярності відповіді на сервер надзвичайно складне. Аналіз продуктивності мережі можна досягти за допомогою моніторингу трафіку [6]. Відстежуючи трафік, користувач може розпізнати стан цієї мережі. Крім того, він надає повну інформацію про дані, ресурси, які пов'язані з цією мережею. Неаутентифікована служба або підходи до сервера будуть визначатися шляхом регулярного контролю за трафіком. Правила мережі та

статистика про трафік будуть легко відомі, що допоможе усунути несправності в мережі. Події безпеки також будуть досліджені, а вхід користувача буде відповідальним. У мережі не буде жодного маршруту до вузла призначення з вихідного вузла. Вихідний вузол буде транслювати запит маршруту про пакети даних на всі вузли, коли він зможе відправити пакети.

У нинішньому контексті конкуренції не існує управлінського рішення, яке могло б відповідати всім ситуаціям. Наявні відкриті та безкоштовні рішення не охоплюють усіх різних функцій управління, навіть тих, що необхідні для ефективної експлуатації та обслуговування. Нарешті, приймаються патентовані рішення, часто дорогі з обмеженим видом мережевої карти. Обмеження цих патентованих рішень полягає в тому, що вони потребують спеціальної та дорогої підготовки. Щоб подолати цю проблему декількох інструментів управління, розгорнутих в одній кімнаті у випадку підходу централізованого управління, авторами [8] розроблено нову платформу під назвою NB-ITMS (Nagios Based - IT Management System). Nagios - це програмне забезпечення для нагляду з відкритим кодом, яке легко налаштовувати безкоштовно. NB-ITMS має ще дві дуже важливі та критично важливі покращені функції порівняно з Nagios: управління конфігурацією та вдосконалений графічний інтерфейс для експлуатації та обслуговування [8].

Через складність сучасних мереж і недосконалості існуючих функцій програмного забезпечення з відкритим вихідним кодом, мережевим адміністраторам, зазвичай, доводиться інтегрувати кілька інструментів для створення середовищ моніторингу, що відповідають їх вимогам. Nagios - один з тих інструментів, які широко використовуються досвідченими мережевими адміністраторами. Завдяки гнучкій модульній архітектурі Nagios дозволяє користувачам розробляти власні модулі для поліпшення функціональності системи безліччю різних способів. У цій статті пропонується концептуальний дизайн безшовної інтеграції Nagios, як ядра нової багатофункціональної системи моніторингу [9].

У роботі [10] представлена автоматизована система моніторингу та управління мережею, яка полегшує обов'язки адміністраторів мережі з метою підтримання працездатності серверів та пристроїв у режимі 24/7. Вона негайно повідомляє адміністратора мережі електронною поштою, як тільки виникає проблема з мережею. Запропонована система пропонує портативність, динамічну масштабованість мережі та не викликає проблем сумісності та інтеграції між безліччю різнорідних пристроїв різних виробників. Крім того, всі функції моніторингу є безперервними та автоматичними, не вимагаючи певного введення або уваги з боку адміністратора. Крім того, запропонована система забезпечує гнучкість для адміністраторів мережі. Якщо адміністратор зайнятий і не усуває несправність або проблему мережі протягом попередньо визначеного терміну, нове повідомлення електронною поштою надсилається наступній відповідальній особі у списку пріоритетів тощо. Унікальні особливості та їх експериментальна перевірка доводять важливість запропонованої системи моніторингу та управління мережею.

У роботі [10] представлено розробку та впровадження інтелектуальної системи моніторингу та звітності для великих організацій/галузей. Він заснований на програмуванні інструментів з відкритим кодом (таких як Nagios та RT) та розумній інтеграції їх для моніторингу мережевих пристроїв, таких як комутатори та маршрутизатори. Для моніторингу пристроїв кінцевих користувачів у мережі був розроблений пакет програм із використанням технології Universal Plug & Play (UPnP). Автори [10] розглядають систему, яку можна однаково застосовувати для різного роду підприємств та організацій.

Таким чином, можна говорити про те, що відомі системи моніторингу можуть бути застосовані у великих організаціях, але є громіздкими для навчального закладу середньої величини з порівняно невеликою кількістю користувачів. Це обумовлює те, що більшість функцій такого програмного забезпечення залишаться незадіяними, проте досвід їх застосування з успіхом може бути використаний при розробці власного програмного продукту.

1.4 Мета та задачі кваліфікаційної роботи

Для визначення оптимальності роботи комп’ютерної мережі, мережевими адміністраторами використовується програмне забезпечення для моніторингу мережі, завдяки чому можна заздалегідь визначати недоліки мережі, підвищувати та контролювати її працездатність, виявляти критичні стани.

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

Метою кваліфікаційної роботи є розробка інформаційної системи моніторингу корпоративної комп’ютерної мережі з підвищеним забезпеченням безпеки, зокрема, захистом від несанкціонованих доступів, атак, критичних станів та аномалій, та можливістю своєчасного попередження про можливі збої в її роботі.

Для досягнення поставленої мети в роботі необхідно вирішити наступні **задачі**:

– визначити функції та проаналізувати задачі моніторингу функціонування корпоративної комп’ютерної мережі;

– розробити структуру системи моніторингу корпоративної комп’ютерної мережі;

– на основі аналізу обрати платформу для розробки інформаційної системи та програмне забезпечення;

– розробити алгоритм функціонування інформаційної системи моніторингу корпоративної комп’ютерної мережі.

Розроблені вимоги до системи моніторингу на основі наведеного аналізу мережі та систем моніторингу, дозволять обрати найоптимальніше за функціональними вимогами програмне забезпечення, необхідне для закладу освіти в сучасних умовах. Але треба зауважити, що і обраний продукт не може реалізувати в повній мірі всі поставлені задачі, адже потребує розробки додаткових додатків та модулів.

Висновки до розділу 1

Проаналізовано проблеми моніторингу корпоративних комп’ютерних мереж та визначено актуальність даної проблеми, яка полягає в складності управління інформаційними системами в сучасних умовах.

Визначено основні задачі та функції моніторингу корпоративних комп’ютерних мереж. Вирішення задачі моніторингу корпоративних комп’ютерних мереж розглядається як збір, обробка та аналіз інформації для поліпшення процесу працездатності системи та вирішується за рахунок ряду програм мережевого моніторингу [2].

Головною функцією моніторингу комп’ютерних мереж, виходячи із зазначеного, є забезпечення надійного функціонування шляхом своєчасного виявлення погіршень в роботі, аналіз їх та формування звітності для прийняття правильних управлінських рішень.

Проаналізовано дослідження вітчизняних та зарубіжних науковців та сучасні подходи до проблеми моніторингу корпоративних комп’ютерних мереж, результат роботи яких наведений в літературі.

РОЗДІЛ 2
РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Структура системи моніторингу функціонування корпоративної комп'ютерної мережі

Архітектура системи відбиває склад і взаємозв'язок компонентів системи, тобто визначає технологію її функціонування. Архітектура комп'ютерної мережі – це концепція її побудови, яка визначає:

– основні елементи мережі;

– топологію мережі і функції кожного її елементу;

– фізичну і логічну організацію взаємодії елементів мережі [11].

Розуміння структури системи мережевого моніторингу дозволить забезпечити прозорість мережі при необмеженій кількості конфігурацій та у будь-якій ситуації. Існує кілька методів моніторингу мереж на основі маршрутизатора і без нього. SNMP, RMON і Cisco NetFlow - це деякі з методів, заснованих на маршрутизаторах, це інструменти активного, пасивного та комбінованого моніторингу. Існує ряд програм мережевого моніторингу. Так, утиліти ping, ipconfig займається перевіркою якості та цілісності з'єднань в комп'ютерній мережі, сервери SNMP, безліч сучасних програмних продуктів, наприклад, Zabbix, Nagios та інші займаються управлінням обладнанням в комп'ютерних мережах на основі архітектур TCP/IP тощо.

У мережах Ethernet хаби (концентратор, hub) і комутатори (switch) є центральними точками підключення до мережі комп'ютерів або інших мережевих пристроїв. У сукупності ці комп'ютери складають сегмент мережі. В рамках цього сегменту всі комп'ютери можуть «спілкуватися» безпосередньо один з одним [12].

Структура системи управління мережами ілюструє ієрархію, в якій всі

пристрої сполучені в мережу та складається із таких компонентів:

– системи управління мережею (NMS), яка виконує додатки, що відслідковують та контролюють пристрої, що управляються;

– протоколу управління мережею, функцією якого є спрощення обміну інформацією між системою управління мережею та управляючими пристроями;

– управляючих пристроїв, наприклад, маршрутизатор, які управляються системою управління мережею;

– агентів управління, якими є програмне забезпечення на пристроях, що збирає та зберігає інформацію управління;

– інформації управління, дані, які зазвичай зберігаються в базі даних або MIB.

Визначивши компоненти мережевого управління, можна описати, як відбувається управління мережею (рис. 2.1).

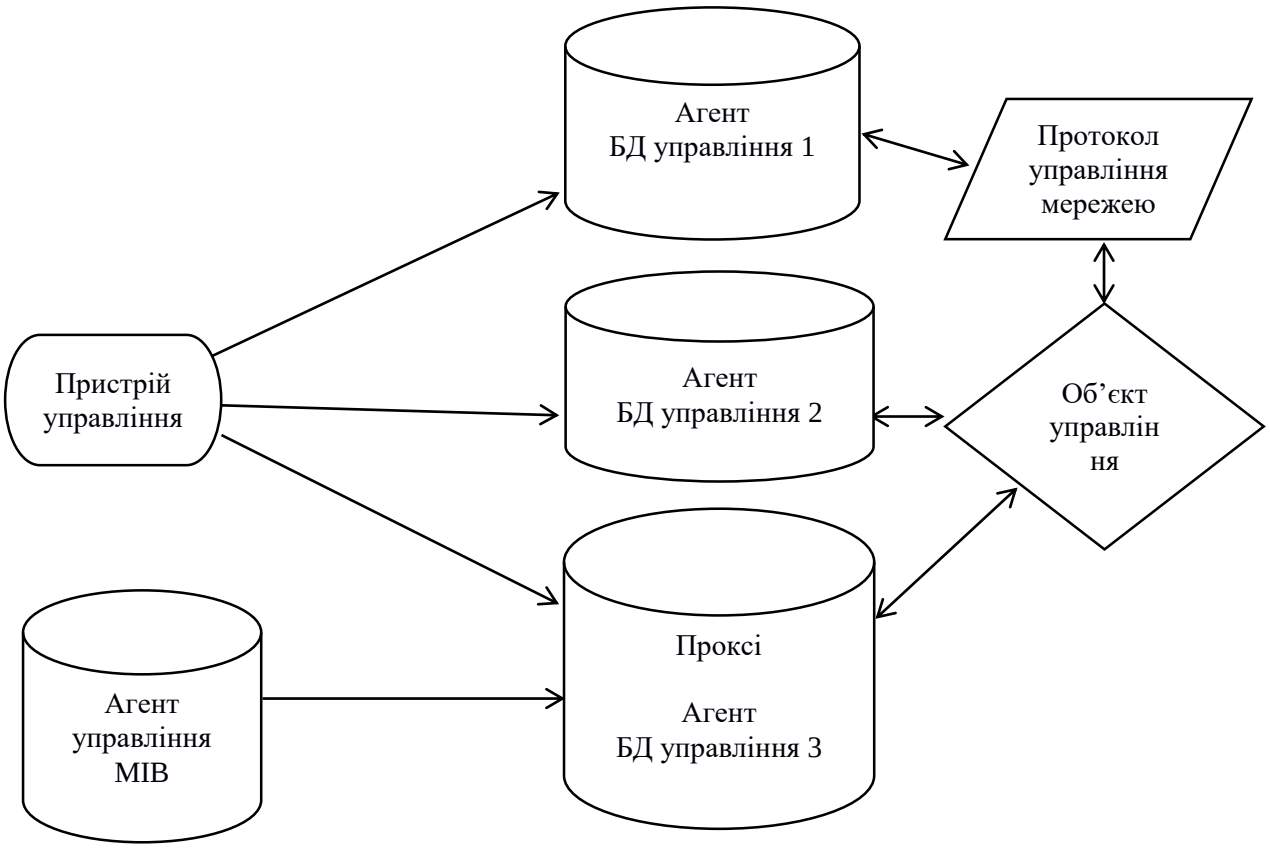


Рисунок 2.1 – Структура системи управління мережею

Під час моніторингу можна користуватись великою кількістю додатків для

управління мережею, вибір яких залежить від мережевої платформи, обладнання або операційної системи. Інформація зберігається на мережевих пристроях, агенти управління, які знаходяться на пристрої, збирають та зберігають інформацію в базах даних (MIB). В архітектурі управління мережею використовується декілька протоколів [13].

MIB – це детальне визначення інформації про мережевий пристрій, доступ до якого можна отримати через протокол управління мережею SNMP. Додаток управління мережею використовує протокол мережевого моніторингу (SNMP) як механізм взаємодії між менеджером та агентами. Агент також виконує функцію управляючого органу, але він не взаємодіє безпосередньо із елементами мережі.

Отримані дані зазвичай обробляються та відображаються за допомогою графічного інтерфейса користувача, який дозволяє оператору використовувати графічне відображення мережі для управління пристроями та програмування додатків для управління мережею. Операція складання звітів ініціюється агентом. Агент повідомляє аномальну дію менеджеру, яке відбулося на стороні агента.

Додаток управління – Менеджер призначений для управління мережею, він періодично опитує агентів SNMP, які знаходяться на пристроях, що управляються на предмет даних, дозволяючи відображати інформацію за допомогою графічного інтерфейсу користувача в системі управління мережею та використовуються для збору та збереження різного роду інформації про пристрій та його роботу.

Існує один суттєвий недолік періодичного опитування SNMP – це можлива затримка між виникненням дії та збором інформації системи управління мережею, виправити це можливо за рахунок частоти опитування та використанням полоси пропускання. SNMP – протокол обміну повідомленнями. Пристрій, що управляється може бути маршрутизатором, який управляється додатком-менеджером.

Агенти управління SNMP знаходяться на пристроях, що управляються MIB, як агент управління збирає дані та зберігає їх локально в базі даних.

Техніка моніторингу мережі включає в себе протокол SNMP та протокол пакетів користувача.

Розглянемо протокол SNMP, який є стандартом управління мережею, адже саме він найчастіше є основою архітектури управління мережею та визначає спосіб обміну управляючою інформацією між додатками управління мережею та агентами управління. SNMP був створений в 1988 році для управління пристроями з інтернет-протоколом IP та являє собою простий набір операцій та інформації про останні, які надають можливості змінювати стан деяких пристроїв на основі SNMP. Зазвичай SNMP зв'язаний із управлінням маршрутизаторами, але можливим є зв'язок із концентраторами, мостами, принтерами, серверами, робочими станціями тощо. SNMP може контролювати такі параметри, як кількість трафіку, вхідного та вихідного інтерфейсу, температура всередині роутера.

SNMP використовує протокол пакетів користувача (UDP) в якості транспортного протоколу для передачі даних між менеджером та агентом. протокол пакетів користувача не встановлює з'єднання між агентом та системою управління мережею при обміні пакетами. SNMP використовує певний порт в конфігурації агента по замовчуванню для отримання пасток від пристроїв, що управляються.

Міжнародна організація по стандартизації ISO розробила еталонну модель взаємодії відкритих систем (Open System Interconnection, OSI). Модель управління мережею відповідно до ISO 10303 (all parts) Industrial automation systems and integration — Product data representation and exchange [14] складається з 5 концептуальних областей, функціональний поділ яких розглянемо детальніше:

– управління ефективністю – вимірювання та забезпечення таких аспектів мережі, як пропускна здатність, час реакції користувачів, коефіцієнт використання лінії, для підтримання мережевої ефективності на достатньому рівні;

– управління конфігурацією, її метою є відслідковування та управління дії на роботу мережі різних апаратних та програмних елементів;

– управління обліком використання ресурсів зводить до мінімуму кількість проблем в мережі та максимізує рівно доступність мережі для всіх користувачів;

– управління несправностями, її метою є виявлення, фіксація, повідомлення про проблеми в мережі.

– управління захистом даних забезпечує контроль доступа до мережевих ресурсів у відповідності із керівницькими принципами, щоб убезпечити несанкціонований доступ до мережі третіх осіб.

Управління мережею або комп'ютерний моніторинг (NM) виконує функції планування, управління, розподілення, координації, управління мережевими ресурсами. Управління мережею включає в себе моніторинг продуктивності мережі, виявлення та усунення несправностей, налаштування мережних ресурсів, ведення бухгалтерської інформації, забезпечення безпеки мережі шляхом контролю доступу до інформаційних потоків мережі.

2.2. Аналіз та вибір програмного забезпечення для моніторингу корпоративних комп'ютерних систем

Відомо, що ПЗ з відкритим вихідним кодом для моніторингу комп'ютерних мереж вигідно відрізняються від інших, зокрема із закритим вихідним кодом, загальною доступністю для широкого кола користувачів та можливістю його використання в загальному випадку без додаткових фінансових витрат.

Множина сучасного ПЗ для моніторингу корпоративних мереж слідкує за приладами, серверами, трафіком, використанням полоси пропуску та повідомляє мережевих адміністраторів про збої в роботі. Проте, з урахуванням того, що у сучасних корпоративних мережах окремі вузли, що беруть участь в обміні інформацією можуть працювати за схемою клієнт-сервер, а окремий вузол може виступати одночасно як клієнтом, так і сервером [15], а їх працездатність та функціональні можливості забезпечується відповідним ПЗ, в тому числі, і ПЗ з відкритим вихідним кодом, воно повинно відповідати вимогам забезпечення якості як деякого комплексного поняття відповідно до міжнародних стандартів, зокрема:

– збережуваності інформації, передачі даних тощо;

– високої ймовірності безвідмовної роботи протягом заявленого терміну експлуатації;

– можливості відслідковувати окремі вузли та програмні додатки, з якими працюють користувачі на предмет ознак низької продуктивності, основними характеристиками якої є час реакції, перепускна здатність, затримка передачі даних;

– оперативного реагування та запобігання несанкціонованим доступам, хакерським атакам, шахрайствам при функціонуванні корпоративної комп'ютерної мережі;

– сумісності з іншими операційними системами вузлів (наприклад, локальних комп'ютерів та серверів) корпоративної комп'ютерної мережі;

– збільшення продуктивності при нарощуванні кількості вузлів в мережі, тобто володіти масштабованістю;

– зручності використання та обслуговування тощо.

Не зважаючи на різноманіття сучасного ПЗ, що може використовуватись для моніторингу комп'ютерних мереж, не все може бути використано для вирішення поставленої задачі та відповідати вказаним вимогам забезпечення якості. Очевидно, що при виборі ПЗ необхідно особливу увагу звертати на низку рішень для моніторингу та оцінювати ключові інструменти, щоб відсіяти ПЗ з непотрібними функціями. Тобто виникає задача багатокритеріального вибору при прийнятті проєктних рішень, що є багатоетапним і трудомістким процесом, який не дає однозначної відповіді, а власне вибір ПЗ для моніторингу корпоративних інформаційних систем є задачею оптимізації, яка передбачає отримання в певному значенні найкращого результату, що повинен задовольняти вище наведеним вимогам забезпечення. Фактично, вибір ПЗ для моніторингу корпоративних мереж можна представити як послідовність певних дій, що виконуються над множиною альтернатив на кожному етапі прийняття рішень в результаті яких отримується підмножина відібраних альтернатив (в даному випадку ПЗ, що може бути використане для вирішення поставленої задачі), що задовольняє певним наперед визначеним умовам. Кінцевим результатом буде

одна альтернатива (в даному випадку певне ПЗ), що є найкращою відповідно до прийнятого сукупного критерію якості. Зазначене вказує на багатоетапність процесу вибору ПЗ для моніторингу комп'ютерних мереж та передбачає застосування певної загальної методики прийнятті проектних рішень [16], що проілюстрована рис. 2.2.

Множина сучасного ПЗ, що може бути застосоване для вирішення поставленої задачі та з використання яких накопичений значний позитивний досвід, а також може виступати в якості альтернатив за методикою (див. рис. 2.2) наведено в табл. 2.1.

На кожному етапі приведеної на рис. 2.2 методики вибору ПЗ для моніторингу корпоративних комп'ютерних мереж здійснюється фактично пошук оптимального. При цьому результати, отримані на кожному з попередніх етапів є вихідними даними для наступного етапу, варіанти, що були відкинуті на попередніх етапах в подальшому не розглядаються.

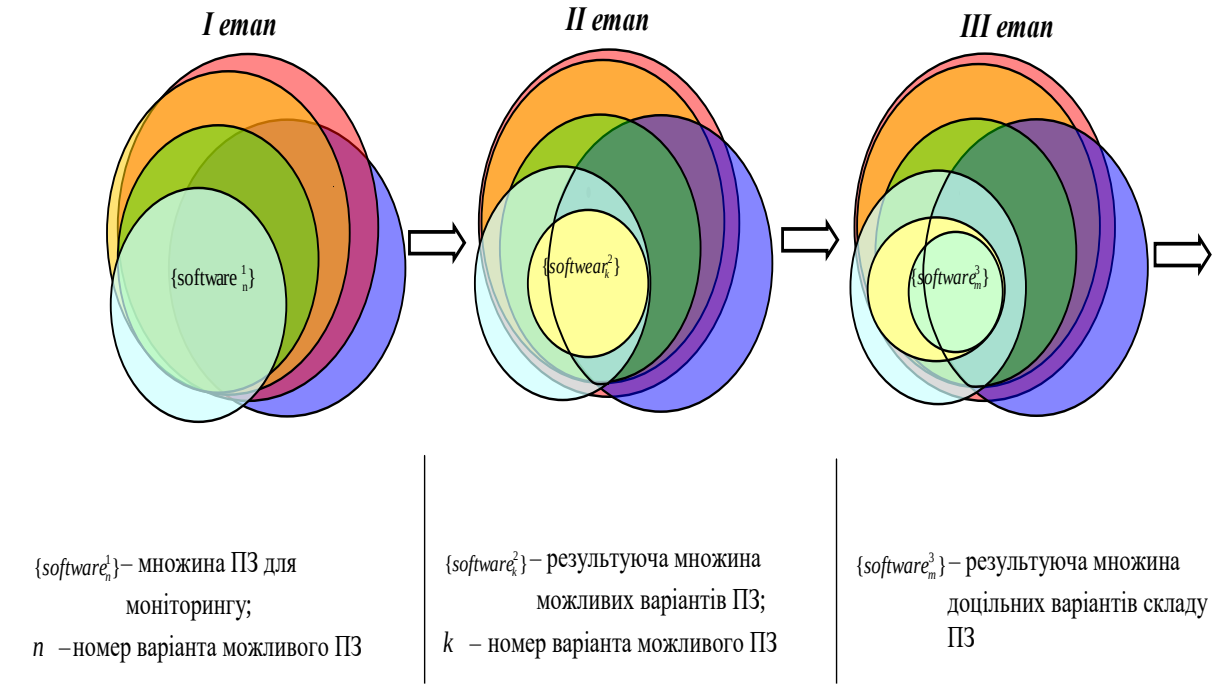


Рисунок 2.2 – Графічна інтерпретація вибору ПЗ для моніторингу комп'ютерних мереж на базі відомої методики автоматизованого вибору складових елементів ГВС [16].

Таблиця 2.1 – Деяке ПЗ, що може 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; - збереження всіх налаштувань в конфігураційному файлі; - налаштування програмної архітектури на основі роботи з плагінами; Переваги: - забезпечує високий рівень продуктивності за рахунок низького використання ресурсів серверу; - інтегрується за допомогою плагінів із майже будь-яким стороннім ПЗ; - має велику кількість користувачів, - легкість налаштування Недоліки: - масштабованість без додаткових плагинів стає дуже складною; - відсутність вбудованих засобів візуалізації; - кожен пагін запускається як окремий процес.	Відслідковує стан серверів, мережевого обладнання та додатків, використовується як для окремого комп'ютера, так і для локальної мережі.	Архітектура клієнт-сервер.
OpenNMS	Підходить для рішень промислового масштабу, особливістю є можливість відслідковувати роботу мережевих топологій на різних рівнях моделі OSI, що дозволяє оптимізувати IT-інфраструктуру. Недоліки: - складний для моніторингу невеликих мереж; - складний web-інтерфейс; Переваги: - написаний на мові Java; - гнучкість; - масштабованість.	Моніторинг мереж корпоративного рівня.	Побудована на подійно-орієнтованій архітектурі.

Продовження таблиці

1	2	3	4
Zabbix	Дозволяє моніторити Java-сервери, функціонал розширюється за допомогою власних скриптів Переваги: - велика кількість типів файлів, що зберігаються; - гарна візуалізація. Недоліки: - відсутність плагінів; - збереження історії та конфігурації в базу даних, що є неефективним та обмежує масштабованість.	Відслідковує багато параметрів мереж, серверів.	Архітектура клієнт-сервер.
Cacti	Збирає опитування мережевого комутатора чи інтерфейса маршрутизатора через протокол SNMP. Використовується в якості зовнішнього додатку інструменту RRDtool. Є інструментом графічного моніторингу мереж. Переваги: - зручний, має сучасний інтерфейс; - чудові інформативні графіки; - має можливість підключення скриптів. Недоліки: - складний в налаштуванні; - використовується тільки для візуалізації.	Використовується для відстеження мережевого трафіку.	Архітектура сервер - клієнт.
Zenoss Core	Включає в себе систему моніторингу за допомогою ICMP pings и SNMP. Переваги: - відстежує мережу від потоку трафіку до HTTP та FTP. Недоліки: - маловідомий; - складний в налаштуванні.	Моніторинг мереж корпоративного рівня.	Побудована на подійно-орієнтованій архітектурі.

Компанії та підприємства намагаються зменшити свої витрати та збалансувати бюджет також і за рахунок використання ПЗ для моніторингу мереж з відкритим вихідним кодом. На основі порівняльного аналізу для створення інформаційної системи обрано ПЗ Nagios Core, яке значно покращує

продуктивність, забезпечує максимальну ефективність та скорочення часу очікуваного вирішення певних завдань та надає можливість підтримувати обладнання в робочому стані та збереження працездатність системи в цілому [17].

Через складність сучасних мереж та неадекватність існуючих функцій програмного забезпечення з відкритим вихідним кодом, мережевим адміністраторам доводиться інтегрувати декілька інструментів для створення середовища моніторингу, що відповідає їх вимогам. Процес моніторингу мережі не є завершеним без допомоги інструментів моніторингу з використанням мінімуму ресурсів та які мають бути більш зручні для забезпечення бажаного результату.

Висновки до розділу 2

Розглянуто та вивчено структуру системи управління корпоративними комп’ютерними мережами. Описано функціональний поділ еталонної мережі ISO. Проведено огляд сучасного стану світового ринку програмного забезпечення (ПЗ) з відкритим вихідним кодом для моніторингу корпоративних комп’ютерних мереж. Проаналізовано найпопулярніше на ринку програмне забезпечення для моніторингу корпоративної комп’ютерної мережі.

До недавнього часу випускались продукти мережного керування обмеженої дії, які неможливо було сумістити з продуктами інших виробників. Нинішня ситуація змінюється на краще – є інструменти, які вважаються універсальними у всіх аспектах керування всією різноманітністю бізнес-інноваційних інформаційних ресурсів, від локальних мереж до ресурсів мережі.

Визначено, що для моніторингу корпоративних комп’ютерних мереж обрано ПЗ Nagios Core, яке значно покращує продуктивність, забезпечує максимальну ефективність та скорочення часу очікуваного вирішення певних завдань та надає можливість підтримувати обладнання в робочому стані та збереження працездатність системи в цілому [17].

РОЗДІЛ 3
АЛГОРИТМ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ МОНІТОРИНГУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Характеристика інформаційних потоків закладу освіти

Корпоративна комп'ютерна мережа управляє інформаційними потоками закладу освіти. В межах мережі заклад має централізований доступ до глобальної мережі Internet, корпоративної електронної пошти, єдиних корпоративних сервісів, має можливість відеозв'язку та доступу до відео конференцій, платформ дистанційного навчання тощо.

У зв'язку із зміною формату вищої освіти, обумовлених пандемією COVID-19, постає питання про переходи на нові стандарти і в області створення нового інформаційного освітнього простору. Інформація виступає рушійною силою діяльності закладу вищої освіти. Інформаційний потік є сукупністю інформації, яка циркулює в певному середовищі, тому обсяг інформації за одиницю часу є певною кількісною характеристикою інформаційного потоку. Створене інформаційне середовище (рис. 3.1) дозволяє вдосконалювати освітній процес, робити його інформаційно насиченим та змістовним, інтегрувати інформаційні технології з науковими.

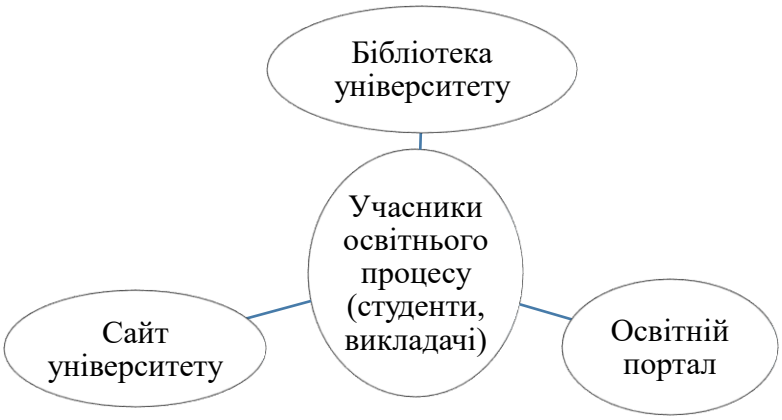
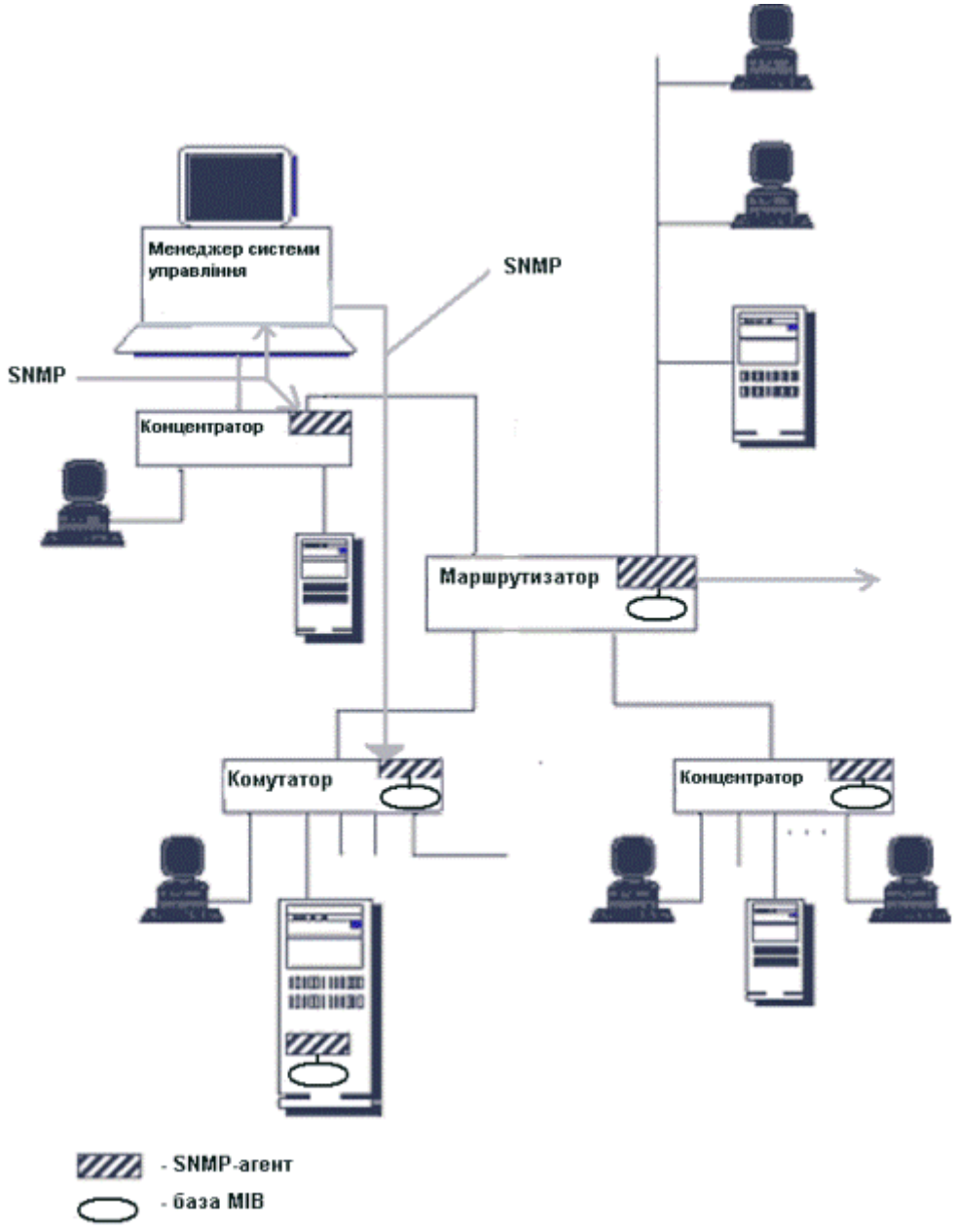


Рисунок 3.1 – Інформаційне освітнє середовище закладу освіти

На тлі пандемії COVID-19 змінюються форми навчання, внаслідок чого збільшуються інформаційні потоки закладів освіти, а це в свою чергу, може збільшувати ураженість комп'ютерної мережі. Постає необхідність в створенні захищеного середовища обробки інформації в корпоративній комп'ютерній мережі. Сутність моніторингу таких мереж полягає у можливості виявлення, повідомлення, реагування шляхом стримання збоїв та атак, які відбуваються в інфраструктурі мережі.



[18]

Рисунок 3.2 – Типова структура системи управління комп'ютерною мережею закладу освіти

Проведено аналіз комп’ютерної мережі, а також, за такими критеріями, як комерційні витрати, системні вимоги, зручний користувацький інтерфейс, швидкість відповіді на аварію або атаку досліджено ринок пропозицій потенційно придатного для моніторингу комп’ютерних мереж програмного забезпечення. Для обрання системи комп’ютерного моніторингу проаналізовано різне, найбільш популярне системне програмне забезпечення, вивчено особливості структури, оцінено складність установки, базову конфігурацію, здатність виявляти вражений вузол, додаткові функції, сумісність з іншими системами тощо. На основі порівняльного аналізу різного, найбільш популярного програмного забезпечення для моніторингу комп’ютерної мережі для закладу освіти в умовах пандемії COVID-19 обрано один із найсучасніших та найпопулярніших інструментів моніторингу з відкритим вихідним кодом Nagios, який працює на ядрі Nagios Core.

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

Під час моніторингу комп’ютерної мережі відбувається процес збору та обробки інформації. Проаналізована інформація систематизується та визначаються проблеми мережі. Для вирішення проблеми, в залежності від її виду, системою застосовуються певні плагіни. По завершенні операції усунення аномалії надсилається звіт з результатами вирішення проблеми (рис. 3.3).

За інформацією розробників [19] задачею Nagios є збір та формування інформації про загальний стан інформаційної системи мережі. Nagios Core об’єднує в собі статичний аналіз системного журналу, журналів контролю мережевих пакетів та встановлені програми, журнали систем виявлення вторгнень тощо, зв’язує їх, порівнює, надає можливість оцінити ризики для інфраструктури мережі, є комплексом інтерактивних функціональних складових, додатків, кожен з яких відповідає за певний етап моніторингу інформаційної системи із застосуванням інструментів для зв’язку, аналізу, порівняння, моделювання та

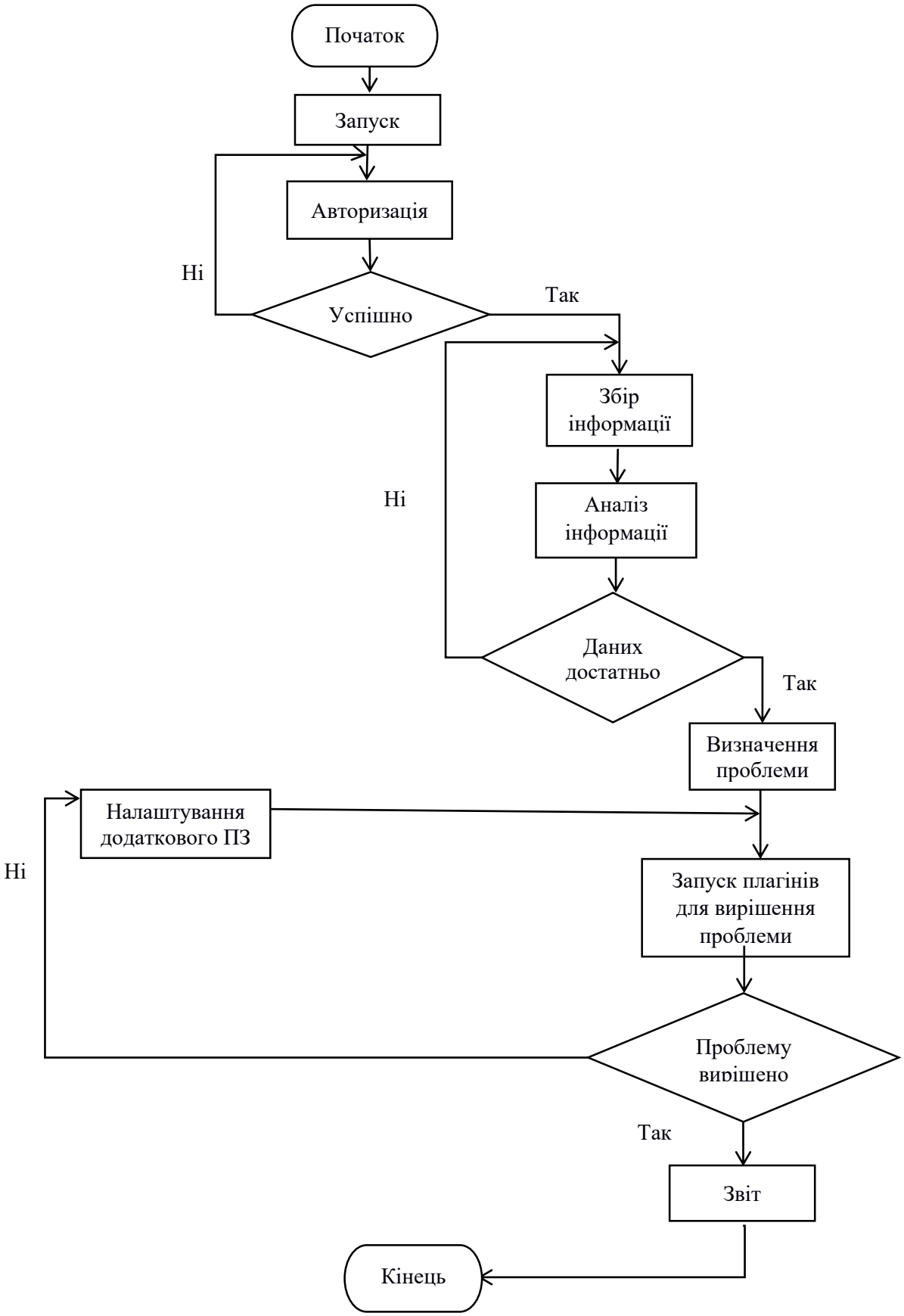


Рисунок 3.3 – Алгоритм роботи інформаційної системи моніторингу корпоративної комп’ютерної мережі закладу освіти

прийняття відповідних рішень, забезпечує безперервний моніторинг системи, додатків, сервісів, процесів в інформаційній системі, дозволяє виявити першопричину проблеми, активно контролює всю інфраструктуру мережі, автоматично усуваючи всі проблеми під час їх виникнення.

У випадку збою програма попереджає системного адміністратора про проблему в мережі, дозволяючи розпочати роботу з виправлення збою ще до того, як він вплине на бізнес-процеси та кінцевих користувачів. Ядро розташоване на сервері як хост та запускає плагіни, які зберігаються на сервері, який в свою чергу, підключений до хоста чи іншого серверу в мережі. Плагіни є скомпільованими модулями або файлами (скрипти, сценарії оболонки тощо), які можуть бути запущені із командної строки для перевірки стану хосту. Програма надсилає сигнал через «планувальник процесів» для запуску плагінів на локальних хостах або серверах. Плагіни збирають дані та відправляють назад до «планувальника». Планувальник являє собою серверну частину Nagios, яка регулярно перевіряє плагіни. Формуються графіки процесу, які відправляють повідомлення адміністратору та поновлюють графічний інтерфейс. Узагальнено процес моніторингу комп’ютерної мережі закладу освіти на прикладі Nagios Core схематично зображено на рис. 3.4.

Nagios Core має в основі архітектуру клієнт-сервер [20]. Додатки або плагіни Nagios працюють окремо від ядра Nagios Core. При цьому ядро представляє API-інтерфейси, що дозволяють легко розширити набір функцій за рахунок додаткових надбудов. Єдиною вимогою для запуску Nagios Core є операційна система Linux з доступом до мережі на комп’ютері та встановленим компілятором C. За бажанням адміністратора використовується CGI, який є складовою Nagios Core, що, за інформацією розробника, вимагає наявності веб-серверу, бажано Apache та Thomas Boutell's gd library ver. 1.6.3 та вище [19].

Існують різні способи моніторингу віддалених серверів Linux. Незважаючи на те, що розглядаємо програмне забезпечення з відкритим вихідним кодом, є можливість використовувати програмні додатки із закритим кодом для розширення можливостей інформаційної системи.

Метод моніторингу віддалених хостів Linux шляхом використання надбудови NRPE дозволяє запускати програмні додатки на віддалених хостах Linux, що є корисним для відслідковування локальних ресурсів, наприклад, використання диску, завантаження ЦП, використання пам’яті тощо.

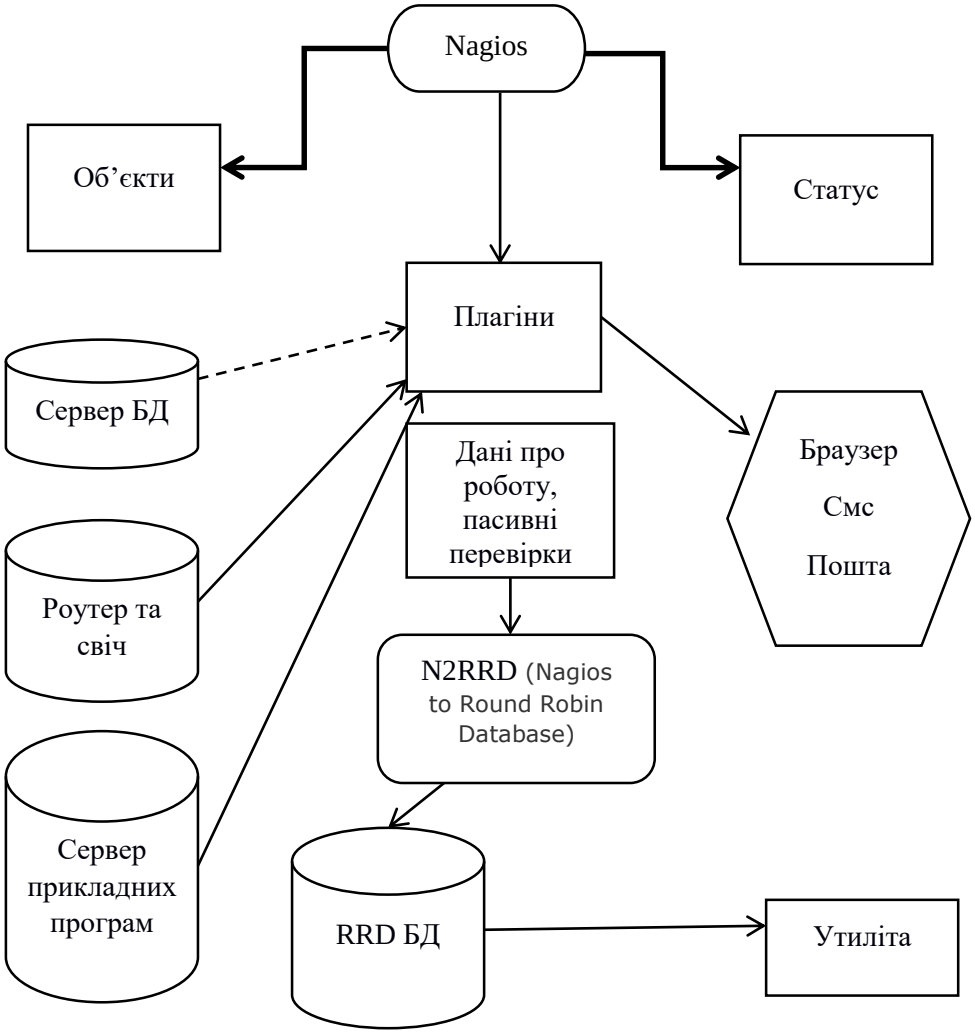


Рисунок 3.4 – Схема моніторингу комп’ютерної мережі на прикладі Nagios

Що стосується використання плагінів для сервісів моніторингу, то вони використовуються для відслідковування конкретних додатків, служб або протоколів. Через існування великої кількості офіційних та додаткових плагінів можливості моніторингу значно розширюються. Якщо немає можливості знайти потрібний плагін, є можливість написати свій власний. Достатньо тільки звернутись до документації з написання плагінів для отримання додаткової інформації.

Кожний сервіс операційної системи можливо відстежити за допомогою додаткових модулів. Спочатку потрібно визначити хост, що зв’язаний з цім сервісом, що відбувається шляхом розміщення хосту в окремому файлі або долучено у вже існуючий файл конфігурації об’єкту. Теж саме робимо з визначенням сервісів, які маємо відслідковувати.

Також Nagios Core дозволяє відслідковувати і веб-сервери. Для цього використовують відповідні програмні додатки. Так, плагін розуміє протокол HTTP та відслідковує час відповіді, коди помилок, сертифікати серверів та багато іншого. За допомогою плагіну check_ftp можна відслідкувати службу FTP-сервера. Плагін check_ssh використовують для моніторингу SSH-серверів. Він контролює SSH-сервер та генерує попередження в разі відсутності відповіді протягом 10 секунд. Подібним чином є можливість контролювати сервери електронних пошт та поштових серверів.

Отже, для кожного виду моніторингу корпоративної комп’ютерної мережі, зокрема, мережі закладу освіти, існує свій програмний додаток, для реалізації функцій якого необхідно долучити нові визначення хостів та служб в файли конфігурації об’єктів, зробити перезапуск програмного продукту і можна починати моніторинг мережі. Якщо під час перевірки з’являються попередження про помилки, необхідно виправити файли конфігурації, після чого процес моніторингу продовжується. Умовою завершення моніторингу є відсутність помилок.

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

Попередніми умовами для налаштування Nagios є обрання дистрибутива. Згідно інформації виробника, Nagios працює на дистрибутивах Linux, UNIX. Саме Linux і будемо використовувати в якості операційної системи. Важливим є засвідчити, що встановлено сервер Apache.

Розглянемо покроково, як відбувається інсталяція обраного для моніторингу

мережі ПЗ та як це виглядає на екрані монітору.

1. Встановлюємо та запускаємо Apache httpd.

2. Встановлюємо PHP.

3. Встановлюємо сервер Nagios, а також основні плагіни для моніторингу самого Nagios Server.

При цьому на моніторі можна побачити командну строку, що представлено на рис. 3.5.

```
# install from EPEL
[root@dlp ~]# yum --enablerepo=epel -y install nagios nagios-plugins-{ping,disk,users,procs,load,swap,ssh,http}
```
[21]

Рисунок 3.5 – Системна консоль, встановлення сервера Nagios

На екрані монітора цей процес має вигляд зображеної командної строки (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
```
[21]

Рисунок 3.6 – Системна консоль, налаштування Nagios

5. Дозволяємо службу HTTP (рис. 3.7).

```
[root@dlp ~]# firewall-cmd --add-service={http,https} --permanent
success
[root@dlp ~]# firewall-cmd --reload
success
```
[21]

Рисунок 3.7 – Системна консоль, налаштування служби HTTP

6. Отримуємо доступ до [http: // (ім’я хосту або IP-адреси сервера Nagios) / nagios /] від клієнта, який знаходиться в мережі, дозволеному сервером Nagios, та

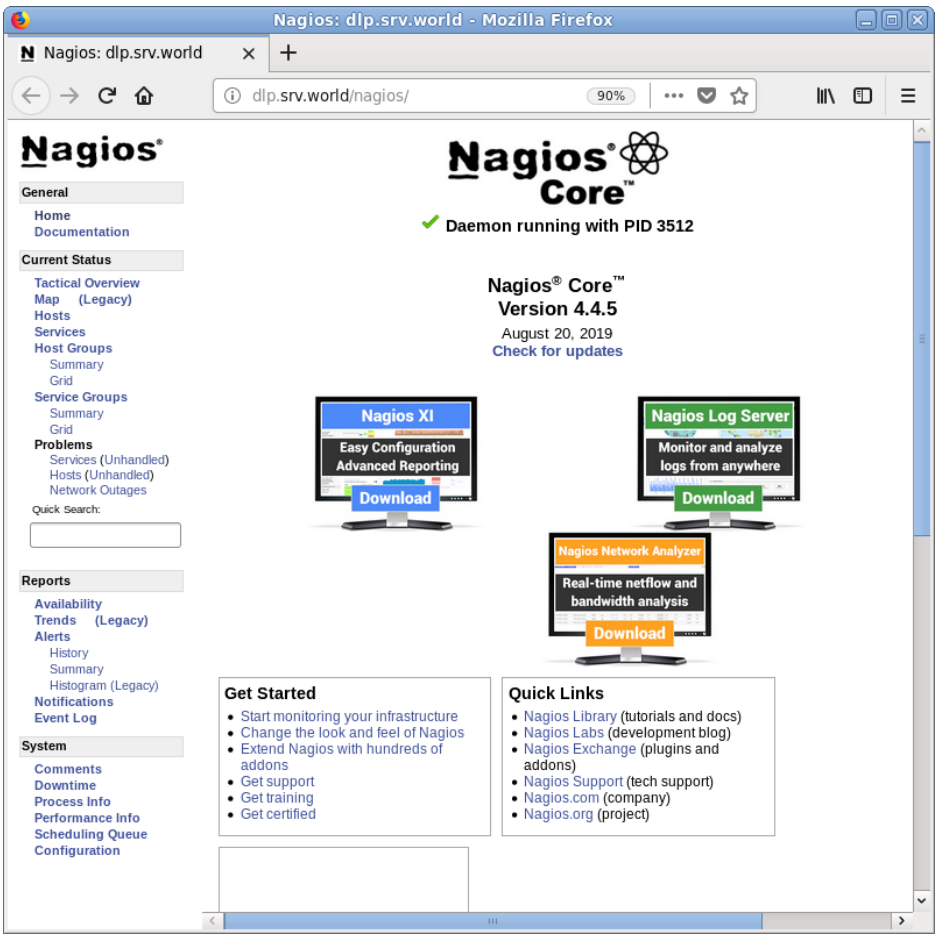
автентифікуємось для входу з користувачем адміністрації Nagios [nagiosadmin], якого додали/ (рис. 3.8).

7. Після успішної автентифікації відображається сайт адміністратора Nagios (рис. 3.9).

8. Можна переглянути стан системи, натиснувши "Тактичний огляд" тощо (рис. 3.10, рис. 3.11).

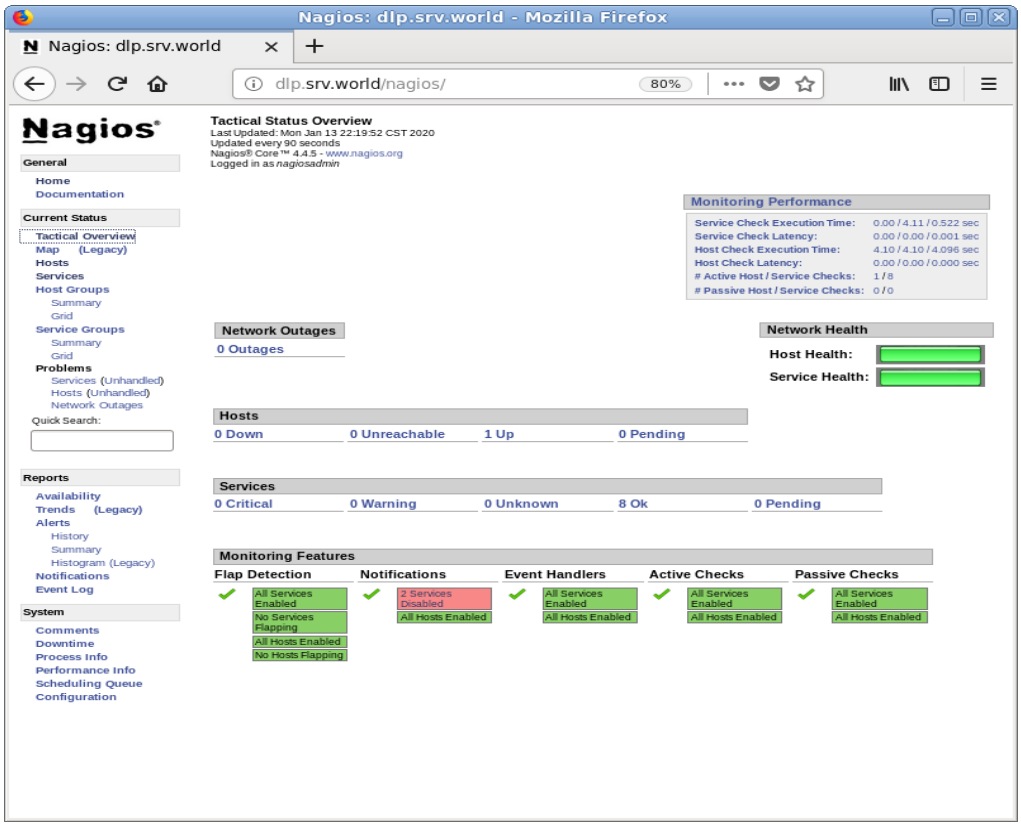
[21]

Рисунок 3.8 – Вікно авторизації



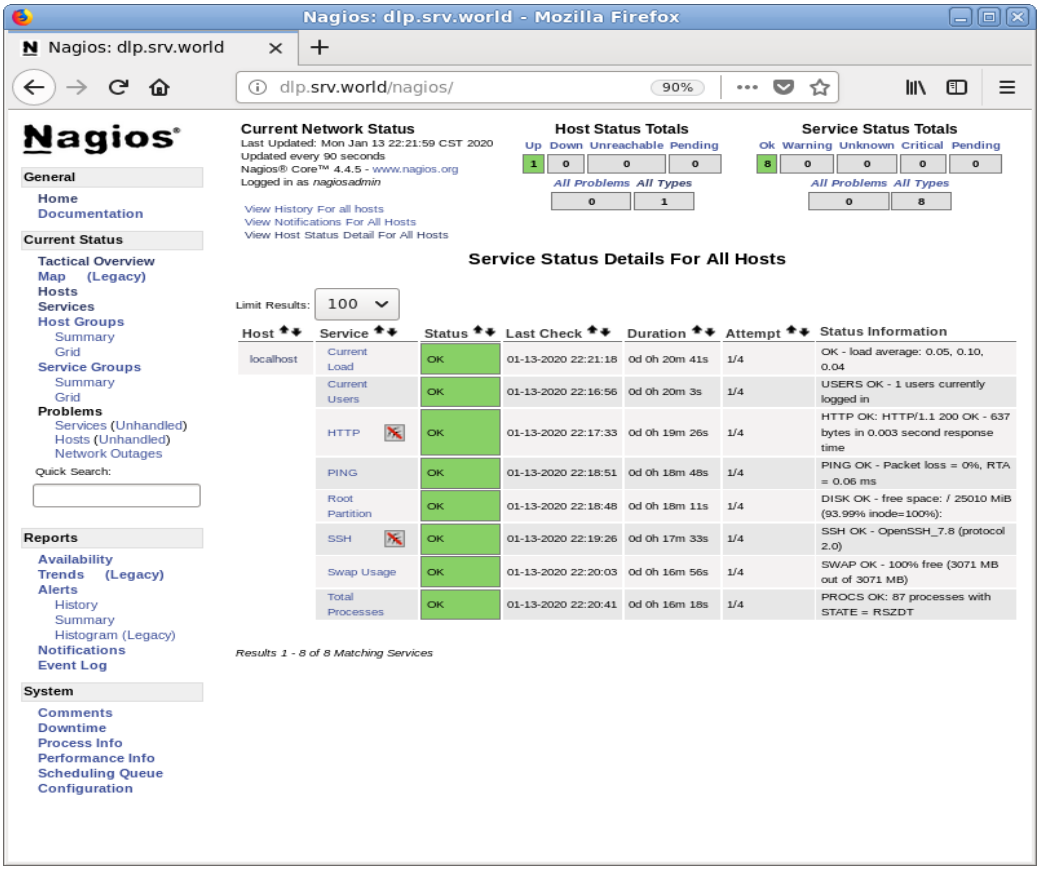
[21]

Рисунок 3.9 – Віконний інтерфейс успішної авторизації



[21]

Рисунок 3.10 – Віконний інтерфейс стану системи



[21]

Рисунок 3.11 – Віконний інтерфейс тактичного огляду системи

Висновки до розділу 3

Розглянуто та проаналізовано інформаційні потоки закладу освіти середньої величини. Представлено алгоритм роботи інформаційної системи корпоративної комп'ютерної мережі, що дає зрозуміти принцип роботи обраного для моніторингу програмного забезпечення. Представлено реалізацію інформаційної системи корпоративної комп'ютерної мережі на прикладі Nagios Core.

Проаналізовано особливості функціонування Nagios для моніторингу інформаційної системи корпоративної комп'ютерної мережі, що працює в умовах перенавантажень та збоїв на платформі OS Linux на прикладі навчального закладу середньої величини.

При формуванні інформаційної системи слід враховувати функціональні можливості та ефективність роботи комп'ютерних мереж в умовах збоїв, перенавантажень та несанкціонованих атак. Враховуючи зазначене, Nagios, як сукупність відповідних блоків та автоматизованих модулів може з успіхом використовуватись для автоматизації процесу сучасного безперервного моніторингу комп'ютерних мереж та є одним із сучасних ефективних способів ефективної роботи обладнання, безперебійної роботи та зменшення впливу на мережу [22].

Визначено, що обране ПЗ є найоптимальнішим за функціональними вимогами для моніторингу комп'ютерної мережі закладу освіти, проте, обране ПЗ не може в повній мірі реалізувати поставлені задачі без розробки додаткових плагінів.

ВИСНОВКИ

В роботі розглянуто та обґрунтовано проблему керування корпоративною комп’ютерною мережею в сучасних умовах.

Для контролю роботи комп’ютерних мереж аналіз та моніторинг є надзвичайно важливими етапами. Аналізатори протоколів, засоби діагностики, експертні та багатофункціональні системи є складовими програмних засобів моніторингу. Розуміння основних принципів мережевого моніторингу дозволить забезпечити прозорість мережі при необмеженій кількості конфігурацій та у будь-якій ситуації. Процес моніторингу мережі не є завершеним без допомоги інструментів моніторингу з використанням мінімуму ресурсів та які мають бути більш зручні для забезпечення бажаного результату.

Проаналізовано проблеми моніторингу корпоративних комп’ютерних мереж та визначено актуальність даної проблеми, яка полягає в складності управління інформаційними системами в сучасних умовах.

Визначено основні задачі та функції моніторингу корпоративних комп’ютерних мереж.

За допомогою інструментів моніторингу мережі можна збирати важливу статистику про мережу, яка допомагає в управлінні та оптимізації пропускної здатності. Деякі інструменти моніторингу обрані з різноманітних наявних на сьогодні інструментів. При виборі враховано такі особливості: доцільність, доступність, легкість, гнучкість, графічна підтримка, збереження даних, зручність для користувачів та насиченість функцій.

Не дивлячись на велику кількість публікацій, глибоке опрацювання теоретично-практичних питань, практичну роботу було зосереджено на подальшому вдосконаленні інформаційної системи моніторингу корпоративної комп’ютерної мережі на прикладі навчального закладу, що збільшує обсяг функціональності системи моніторингу та керування мережею.

Для вдосконалення функцій інформаційної системи обрано на основі аналізу та запропоновано встановити програмне забезпечення для моніторингу компэютерної мережі з відкритим вихідним кодом Nagios, та налаштувати його

для рівномірного розподілу трафіку між підрозділами навчального закладу, що, в свою чергу, дозволить зробити систему моніторингу мережі більш ефективною та досконалою.

Визначено, що обране ПЗ є найоптимальнішим за функціональними вимогами для моніторингу комп’ютерної мережі закладу освіти, проте, обране ПЗ не може в повній мірі реалізувати поставлені задачі без розробки додаткових плагінів.

Список використаних джерел

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. Галанзовська К. В., Керування інформаційною системою корпоративної комп'ютерної мережі в сучасних умовах. Матеріали І Міжнародної студентської наукової конференції «Пріоритетні напрямки та вектори розвитку світової науки», Миколаїв, травень 21, 2021. Том 2 с. 36. – Режим доступу: https://doi.org/10.36074/liga-21.05.2021

3 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_Management_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_merej.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&isAllowed=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_Konspekt_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. Черепанська І. Ю., Галанзовська К. В., Вибір програмного забезпечення для моніторингу корпоративних інформаційних систем. Матеріали Міжнародної наукової конференції «Комп'ютерні технології та сучасна інженерія – 2021», Житомир, 2021.

18. 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%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%D1%83_%D1%82%D0%B0_%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96

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

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

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

22. Галанзовська К. В., Черепанська І. Ю., Опис функціонування Nagios для моніторингу інформаційної системи корпоративної комп'ютерної мережі. Матеріали Науково-практичної студентської конференції «Фінансове забезпечення економіки», Житомир, 2021.